eNetwork Communications Server
Versión 6.0
para Windows NT

Guía de Administración de la Red

Versión 6.0

SC10-3108-00

eNetwork Communications Server
Versión 6.0
para Windows NT

Guía de Administración de la Red

Versión 6.0

SC10-3108-00

Nota: Antes de utilizar esta información y el producto al que da soporte, lea la información contenida en el apartado Apéndice B, “Avisos” en la página 221.

Primera edición (Julio de 1998)

Esta edición se aplica a la Versión 6.0 de IBM eNetwork Communications Server para Windows NT y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

© Copyright International Business Machines Corporation 1989, 1996. Reservados todos los derechos.

Contenido

© Copyright IBM Corp. 1989, 1996

Figuras

© Copyright IBM Corp. 1989, 1996

Tablas

© Copyright IBM Corp. 1989, 1996

Acerca de este manual

IBM eNetwork Communications Server para Windows NT (*Communications Server* en este manual) es una plataforma de servicios de comunicaciones. Esta plataforma proporciona una amplia gama de servicios para las estaciones de trabajo Windows NT que se comunican con sistemas principales y con otras estaciones de trabajo. Los usuarios de Communications Server puede elegir entre una variedad de opciones de conectividad remota.

La publicación *Guía de Administración de la Red* se proporciona como fuente de información para la planificación y administración para la persona que utiliza o que piensa utilizar Communications Server. Este manual puede servir de ayuda al personal de administración, al personal de soporte técnico y de servicio, a los coordinadores de servicios y al personal de IBM, así como a cualquier persona que tenga que tomar decisiones con respecto a los sistemas de información. Este manual proporciona una visión general de las funciones de Communications Server y los pasos necesarios para crear las configuraciones de Communications Server para las estaciones de trabajo que el usuario soporta.

Se supone que está utilizando Windows NT 4.0 Server como el sistema operativo base.

Cómo utilizar este manual

Guía de Administración de la Red le permite realizar la planificación necesaria para instalar y configurar una red de estaciones de trabajo. Este manual le ayuda a:

- Planificar la red
- Elegir las herramientas de configuración e instalación
- Crear un archivo de configuración modelo
- Implantar la planificación de la red
- Mantener la red

La configuración de una red de estaciones de trabajo necesita una planificación cuidadosa y completa. Cuando se crea una red, es necesario conocer la siguiente información:

- Los nombres de las estaciones de trabajo, los nombres de los perfiles, los nombres del archivo de configuración y otros nombres existentes en la red
- Dónde está el punto focal para enviar alertas
- Las estaciones de trabajo que tiene que puede continuar utilizando y cuántas estaciones nuevas necesita
- La función que desea que realice cada estación de trabajo en la red
- El paquete que se ha de instalar en cada estación de trabajo para que pueda cumplir la función que le ha asignado
- Los recursos de hardware y de software que ya tiene que desea conservar o actualizar
- Los nuevos recursos de hardware y de software que necesita para poder implantar la planificación de la red

© Copyright IBM Corp. 1989, 1996

- El método para mantener la red y sus recursos
- El número y tipo de conexiones del sistema principal y las estaciones de trabajo que se han de conectar a los sistemas principales mediante la pasarela y la definición de la pasarela

Los pasos del apartado “Implantación de las configuraciones de Communications Server” en la página 181 proporcionan un procedimiento para determinar esta información para la red. Si ya tiene un procedimiento que funciona, puede utilizarlo en su lugar, pero debe revisar el procedimiento del capítulo antes de tomar esa decisión.

Convenios utilizados en este manual

En este manual se utilizan los siguientes convenios.

Convenios para el texto

Negrita	El texto en negrita indica lo siguiente: • Verbos, funciones, palabras clave y parámetros que puede utilizar en un programa o en un indicador de mandatos. Estos valores son sensibles a las mayúsculas y minúsculas y deben entrarse exactamente igual a como aparecen en el texto. • Los nombres de controles de ventana como, por ejemplo, listas, recuadros de selección, campos de entrada, pulsadores y opciones de menú.
Cursiva	El texto en cursiva indica lo siguiente: • Una variable para la que el usuario suministra un valor. • Títulos de manuales. • Una letra que se utiliza como letra o una palabra como palabra. **Ejemplo**: Cuando aparece un *un*, asegúrese de que no tiene que ser un *uno*.
Cursiva negrita	El texto en cursiva negrita se utiliza para enfatizar una palabra.
MAYÚSCULAS	Las mayúsculas indican constantes, nombres de archivos y opciones que puede utilizar en un programa o en un indicador de mandatos. Puede entrar estos valores en mayúsculas o en minúsculas.
Comillas dobles	Las comillas dobles indican mensajes que se pueden ver en una ventana. Por ejemplo, los mensajes que aparecen en el área de información del operador (OIA) de una sesión de emulador.
`Tipo de letra de ejemplos`	El tipo de letra de ejemplos indica la información que debe escribir en un indicador de mandatos o en una ventana.

Convenios sobre los números

Números binarios	Representados como B'xxxx xxxx' o B'x' excepto en algunos casos en que se representan con texto (“Un valor de xxxx xxxx binario es...”).
Posiciones de bit	Empiezan por 0 en la posición más a la derecha (bit menos significativo).
Números decimales	Los números decimales de más de 4 dígitos se representan en estilo métrico. Se utiliza un espacio en lugar de un punto para separar los grupos de 3 dígitos. Por ejemplo, dieciséis mil ciento cuarenta y siete se escribe 16 147.
Números hexadecimales	Representados en texto como xxxx hex o X'xxxx' (“La dirección del nodo adyacente es 5D hex, que se especifica como X'5D'.”)

Dónde encontrar más información

Para obtener más información, consulte el manual *Quick Beginnings* que contiene una descripción completa de la biblioteca de Communications Server y las publicaciones relacionadas.

La página de presentación de Communications Server en Internet contiene información general del producto, así como información de servicio acerca de los APAR y arreglos. Hay dos maneras de llegar a la página de presentación:

1. En Communications Server, seleccione el icono **Acceso a página de presentación**
2. Utilizando un navegador de Internet, vaya a la siguiente URL:

   http://www.software.ibm.com/enetwork/commserver/about/csnt.html

Visión general y conceptos

© Copyright IBM Corp. 1989, 1996

Presentación de las funciones de Communications Server

Este capítulo proporciona una visión general de las funciones de comunicaciones soportadas por Communications Server y de los métodos que puede utilizar para configurar los sistemas para que realicen estas funciones. Capítulos posteriores de este manual describen las funciones y los métodos de configuración con más detalle.

Funciones soportadas

Esta sección describe las siguientes funciones de Communications Server:

- Soporte de comunicación SNA
- Comunicaciones avanzadas programa a programa (APPC), que incluye Red avanzada de igual a igual (APPN)
- Interfaces de programación de aplicaciones (API) de 32 bits
- Direccionamiento de alto rendimiento (HPR)
- Compresión de datos SNA
- Descubrimiento de proveedores de servicios
- Aplicación de LU (LUA) convencional
- Peticionario de unidades lógicas dependientes (DLUR)
- Pasarela SNA
- Soporte AnyNet
  - AnyNet SNA sobre TCP/IP (nodo de acceso y pasarela)
  - AnyNet Sockets sobre SNA (nodo de acceso y pasarela)
- Servidor TN3270E
- Servidor TN5250
- Acceso de datos de legado
  - Proveedor de AS/400 OLE DB
  - Editor del sistema principal
  - Servidor de carpetas compartidas AS/400
- Soporte de cliente API SNA
- Soporte de cliente Novell IntranetWare para SAA
- Soporte de configuración y administración
- Equilibrio de la carga
- Seguridad de datos
- Soporte de adaptadores
- Soporte de Control de enlace de datos (DLC)
- Soporte APPN MIB
- Espera en caliente

© Copyright IBM Corp. 1989, 1996

- Funciones de emulador de nivel de entrada

Soporte de comunicaciones SNA

Communications Server puede actuar como un nodo Systems Network Architecture (SNA) de tipo 2.0 y un nodo SNA de tipo 2.1. Este soporte le permite escribir programas para comunicarse con muchos otros productos IBM SNA.

APPC/APPN

Communications Server proporciona el soporte de nodos finales y de red de la Red avanzada de igual a igual (APPN) para las estaciones de trabajo, permitiéndoles comunicarse con más flexibilidad con otros sistemas de la red. Además, la función de red derivada le permite aislar las bifurcaciones para evitar el tráfico CP-CP no necesario.

Communications Server proporciona las comunicaciones avanzadas programa a programa (APPC) para dar soporte a las comunicaciones entre programas de proceso distribuido denominados programas de transacción (TP). Los TP se pueden localizar en cualquier nodo de la red que proporcione APPC. APPC utiliza el protocolo LU 6.2 para intercambiar datos entre los programas ubicados en distintas unidades lógicas (LU). Además, APPC da soporte a múltiples enlaces simultáneos y sesiones paralelas. También se da soporte a la seguridad de conversación o de sesión entre los programas en comunicación a través de APPC.

Communications Server proporciona la productividad APPC en entornos de la LAN de rendimiento crítico. Communications Server da soporte a las conectividades siguientes:

Tabla 1. Conexiones APPC soportadas

Protocolos	Conexión	Tipo de conexión
Canal	• CDLC (OEM) • MPC	
LAN (802.2)	• Red en anillo • Ethernet • Frame Relay • Emulación de Lan ATM	
SDLC	• Síncrona • Autosíncrona • Módems	• Automarcado, DTR marcado, Permanente • Automarcado • Automarcado, Permanente • Automarcado
X.25	• Síncrona • Hayes** AutoSync • Red X.25	• Automarcado, Semipermanente • Automarcado, Permanente • Automarcado
IP	SNA sobre IP	Conexiones proporcionadas por IP
IP	HPR sobre IP	Conexiones proporcionadas por IP

Nota: APPC/APPN también tiene la posibilidad de compresión de datos. Consulte el apartado “Compresión de datos” en la página 58 para obtener más información sobre la compresión de datos. Consulte también el apartado “Cifrado a nivel de sesión SNA” en la página 61 para obtener información sobre el cifrado.

Soporte de SNA LU Tipo 6.2

LU 6.2 es una arquitectura para las comunicaciones programa a programa. Communications Server da soporte a la siguientes características opcionales de SNA LU 6.2:

- Conversaciones básicas y correlacionadas
- Nivel de sincronización de confirmación
- Soporte de seguridad a niveles de sesión y de conversación
- Múltiples LU
- Sesiones paralelas, incluyendo la posibilidad de utilizar un sistema remoto para cambiar el número de sesiones
- Transacciones en modalidad de una dirección o de dos direcciones simultáneas
- Múltiples enlaces simultáneos con sesiones SSCP-PU, cada uno de los cuales puede conectarse a una red de subárea

Consulte el manual *Communications Server Programming Guide and Reference* para ver una lista completa de características.

Mejoras de la configuración APPC

La configuración básica del nodo final sólo necesita cuatro parámetros: ID de red, nombre de nodo local, tipo de enlace y dirección de destino. La definición del sistema se reduce mediante:

- Modalidades suministradas por IBM
- Creación implícita de las definiciones de LU asociada y de modalidad cuando se asigna una conversación
- Inicialización implícita de los límites de la sesión (función CNOS), que elimina el requisito de inicializar explícitamente los límites de la sesión antes de poder asignar conversaciones
- Eliminación de los límites de la sesión para las LU local y asociada, lo que permite una mayor libertad al configurar e inicializar los límites de sesiones de modalidad
- Valores por omisión para los nombres del programa de transacción, el funcionamiento y el tipo, que eliminan el requisito de configurar las definiciones del programa de transacción para los programas aplicables
- Actualizaciones dinámicas de la configuración
- Definiciones implícitas de estación de trabajo de pasarela SNA
- Posibilidad de editar un archivo .ACG que contenga los parámetros de configuración
- Posibilidad de buscar información de definición del sistema con Discovery

Puesto que la configuración SNA se almacena como un archivo de texto, puede modificar rápida y fácilmente el archivo utilizando un editor o un programa escrito por un usuario. Después, puede verificar y actualizar dinámicamente una configuración activa (sin detener Communications Server).

Ahora, puede configurar conexiones para múltiples sistemas principales y puede haber múltiples conexiones del sistema principal que estén activas a la vez. Se puede definir las conexiones para que se inicien bajo petición, o como resultado de una anomalía de la espera en caliente.

El soporte que Communications Server da a Discovery permite que un nodo encuentre dinámicamente el nombre de punto de control, la dirección de control de acceso al medio (MAC) y la dirección del punto de acceso de servicio (SAP) de otro servidor de nodos de red de Communications Server en una LAN de red en anillo o Ethernet. Esto significa que el usuario no tiene que conocer el nombre del punto de control ni la dirección de MAC ni de SAP de una máquina asociada para poder definir una conexión con la ella. Actualmente, los usuarios de Client Access/400 y Personal Communications pueden utilizar este recurso.

Conceptos de APPC fundamentales

Esta sección presenta los conceptos y términos de APPC.

Programas de transacción: Un *programa de transacción* (TP) es un programa, o parte de un programa de aplicación, que utiliza las funciones de comunicaciones APPC. Los programas de aplicación utilizan estas funciones para comunicarse con los programas de aplicación de otros sistemas que dan soporte a APPC.

Communications Server proporciona la API APPC y da soporte a las llamadas que la Interfaz común de programación (CPI-C) de IBM Systems Application Architecture (SAA) realiza a programas de transacción.

Los programas de transacción emiten parámetros APPC para invocar funciones APPC. Un ***parámetro*** es una petición formateada que un programa de transacción emite y que APPC ejecuta. Un programa utiliza secuencias de parámetros APPC para comunicarse con otro programa. Dos programas que se comunican entre sí pueden estar ubicados en distintos sistemas o en el mismo sistema. La API APPC es la misma en ambos casos.

Cuando un programa de transacción intercambia datos con otro programa de transacción, el otro programa se denomina el programa de transacción ***asociado***.

Los programas de transacción pueden emitir llamadas CPI-C. Estas llamadas permiten a los programas de aplicación aprovechar las ventajas de la coherencia que SAA proporciona.

Unidades lógicas: Cada programa de transacción consigue el acceso a una red SNA a través de una ***unidad lógica*** (LU). Una LU es el software SNA que acepta los parámetros de los programas y realiza acciones a partir de esos parámetros. Un programa de transacción emite parámetros APPC a su LU. Esos parámetros hacen que los mandatos y datos fluyan a través de la red a una LU asociada. La LU también actúa como intermediario entre los programas de transacción y la red para gestionar el intercambio de datos entre programas de transacción. Una sola LU puede proporcionar servicios para múltiples programas de transacción. Pueden estar activas simultáneamente múltiples LU en el nodo.

Tipos de LU: Communications Server da soporte a las LU de tipo 0, 1, 2, 3 y 6.2. Las LU de tipo 0, 1, 2 y 3 dan soporte a la comunicación entre los programas de aplicación del sistema principal y diferentes clases de dispositivos como, por ejemplo, terminales e impresoras.

LU 6.2 da soporte a las comunicaciones entre dos programas ubicados en los nodos de subárea de tipo 5, nodos periféricos de tipo 2.1, o en ambos, y entre programas y dispositivos. APPC es una implantación de la arquitectura LU 6.2.

Sesiones LU: Para que los programas de transacción puedan comunicarse entre sí, sus LU deben estar conectadas en una relación mutua denominada ***sesión***. Una sesión conecta dos LU, por lo que se llama una sesión ***LU-LU***. La Figura 1 ilustra esta relación de comunicación.

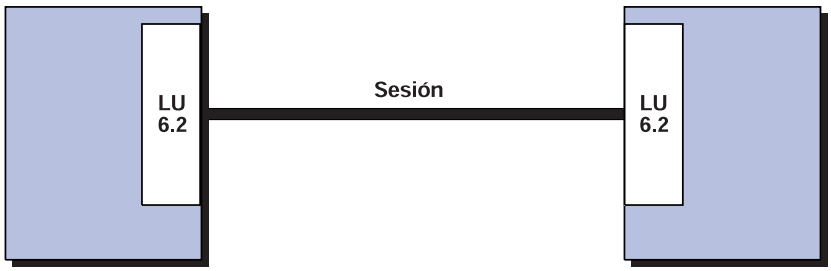


Figura 1. Una sesión entre dos LU (LU-LU)

Las sesiones actúan como conductos que gestionan el movimiento de datos entre un par de LU en una red SNA. Específicamente, las sesiones tratan con elementos como, por ejemplo, la cantidad de datos transmitidos, la seguridad de los datos, el direccionamiento de la red y la congestión de tráfico.

Las LU mantienen las sesiones. Normalmente, los programas de transacción no funcionan con las características de la sesión. Las características de la sesión se definen cuando:

- Se configura el sistema
- Se utiliza **Operaciones de nodos SNA**
- Se utilizan los parámetros de gestión

Conversaciones del programa de transacción: La comunicación entre los programas de transacción se denomina una ***conversación***. Como en una conversación telefónica, un programa de transacción llama a otro y “conversan”, los programas de transacción hablan por turnos, hasta que uno de ellos finaliza la conversación. Una conversación se inicia cuando un programa de transacción emite un parámetro APPC o una llamada CPI-C que asigna una conversación. Las conversaciones se realizan a través sesiones LU-LU.

La asignación de una conversación a una sesión establece una relación de envío-recepción entre los programas de transacción conectados a la conversación. Un programa de transacción emite parámetros para enviar datos. El otro programa de transacción emite parámetros para recibir datos. Cuando el programa de transacción emisor termina de enviar datos, puede transferir el control de envío de la conversación al programa de transacción receptor. Las conversaciones pueden intercambiar información de control y datos.

La Figura 2 muestra una conversación entre dos programas de transacción que se lleva a cabo en una sesión.

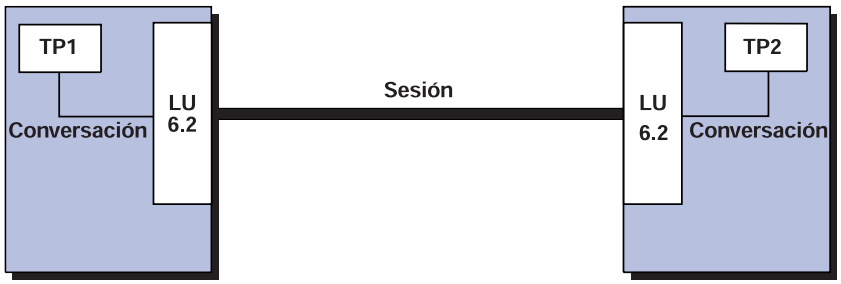


Figura 2. Conversación entre programas de transacción en una sesión

Una sesión sólo puede dar soporte a una conversación cada vez, pero una sesión puede dar soporte a muchas conversaciones en secuencia. Debido a que varias conversaciones pueden volver a usar las sesiones, una sesión es una conexión de larga duración a comparación de una conversación. Cuando un programa asigna una conversación y se están utilizando todas las sesiones aplicables, la LU pone la conexión de entrada (petición de asignación) en una cola. Completa la asignación cuando hay una sesión disponible.

Dos LU también pueden establecer sesiones paralelas entre sí para dar soporte a múltiples conversaciones simultáneas. Una sesión paralela se produce cuando el programa de transacción asigna una conversación y existe una sesión, pero una conversación la está utilizando. La LU puede pedir una nueva sesión para satisfacer la asignación.

La Figura 3 muestra tres sesiones paralelas entre dos LU; cada sesión transporta una conversación.

Figura 3. Sesiones paralelas entre LU

Red avanzada de igual a igual (APPN)

La Red avanzada de igual a igual (APPN) es un conjunto de funciones, formatos y protocolos que amplía en gran manera la gestión de una red SNA y la utilización de las aplicaciones APPC que se ejecutan en la red. APPN lo lleva a cabo a través de unos cuantos requisitos de configuración, búsquedas dinámicas en el directorio, posibilidades de cálculo de la ruta y direccionamiento de sesiones intermedias.

Con APPN, puede escribir programas sin conocer los detalles de la red básica. Todo lo que necesita saber es el nombre de la LU asociada; no necesita conocer su ubicación. SNA determina la ubicación de la LU asociada y la mejor vía de acceso para direccionar los datos. Un cambio en la red básica como, por ejemplo,

un cambio en una dirección física, la adición de un nuevo adaptador o la reubicación de una máquina no afecta a los programas APPC.

Communications Server proporciona el soporte de nodo final APPN y de nodo de red para las estaciones de trabajo, permitiéndoles comunicarse con más flexibilidad con otros sistemas de la red. Además, la función de red derivada le permite aislar las redes derivadas para evitar el tráfico CP-CP no necesario.

- La posibilidad de nodo final proporciona los servicios siguientes:
  - La conexión del nodo local con un nodo de red de servicio para los servicios del directorio y de direccionamiento
  - La reactivación automática de sesiones CP-CP cuando un nodo final pierde su servidor de nodos de red.
- La posibilidad de nodo de red proporciona los servicios siguientes:
  - Servicios de selección de rutas que calculan la ruta mejor para una sesión a través de una red APPN
  - El direccionamiento de sesiones intermedias que permite que dos LU de nodos no adyacentes mantengan una sesión entre ellas, cuando la sesión atraviesa uno o más nodos intermedios
  - Los servicios del directorio que proporcionan la posibilidad de conocer dinámicamente las ubicaciones de las LU asociadas
  - Los servicios de red de conexión para la LAN que proporcionan la posibilidad de conocer las direcciones de destino de la LA sin tener que configurarlas

    Esta posibilidad permite que un nodo establezca una conexión de enlace directamente con otro nodo sin tener configurada ninguna dirección de destino de la LAN.
  - El soporte de red derivada le permite interconectar eficazmente una sucursal que contiene redes LAN, nodos finales y nodos de red de extremo inferior con LU dependientes e independientes y con PU como, por ejemplo, cajeros automáticos, a una o varias WAN. Esto permite que más nodos de red funcionen como pasarelas para las sucursales. Se puede configurar una LAN en cada sucursal como una red de conexión.

Interfaces de programación

Communications Server da soporte a una amplia gama de interfaces de programación de aplicaciones (API) de 32 bits en el servidor, para el desarrollador de programas de aplicación. Estas API proporcionan los procedimientos adecuados para que los programas de aplicación accedan a las funciones de Communications Server y permiten que las aplicaciones dirijan las necesidades de comunicación de las conexiones a sistemas IBM y a otros sistemas. Además, las interfaces proporcionadas dan soporte a los protocolos SNA, de modo que la estandarización está asegurada.

Las API soportadas son:

- Comunicaciones avanzadas programa a programa (APPC)
- Interfaz común de programación para comunicaciones (CPI-C)
- RUI y SLI de Interfaz de aplicación de LU (LUA) convencional
- Bibliotecas de clases de accesos de sistema principal (HACL)

- Java CPI-C (JCPI-C)
- WinSock (conjuntamente con AnyNet Sockets sobre SNA)
- Recurso del operador de red
- Servicios de gestión
- Servicios comunes

En los clientes, también se proporciona la API APPC ampliada (EHNAPPC).

Los desarrolladores de aplicaciones también pueden utilizar el Kit de herramientas para los desarrolladores de software de Communications Server (que se puede instalar independientemente desde el CD-ROM de Communications Server). Este kit de herramientas contiene ejemplos, archivos de cabecera, archivos de bibliotecas y manuales en línea para cada una de las API.

Para obtener información sobre las interfaces de programación de Communications Server, consulte las publicaciones *Client/Server Communications Programming* y *System Management Programming*

Direccionamiento de alto rendimiento

El Direccionamiento de alto rendimiento (HPR) es una mejora de APPN que aumenta el rendimiento y fiabilidad del direccionamiento de datos y establece un enlace virtual entre los nodos de protocolo de transporte rápido (RTP). HPR sustituye el direccionamiento de sesiones intermedias, que es la técnica de direccionamiento utilizada en APPN.

HPR proporciona una transmisión más rápida en los nodos intermedios, redirecciona, sin interrumpir, las sesiones rodeando los nodos y enlaces que han fallado y regula el flujo del tráfico previendo y reduciendo la congestión en la red.

Communications Server da soporte a conexiones HPR en Enterprise Extender (IP), control síncrono de enlace de datos (SDLC), LAN, WAN, canal, Canal de múltiples vías (MPC) y conexiones X.25.

Compresión de datos SNA

La compresión de datos a nivel de sesión aumenta la productividad para grandes cantidades de datos a través de enlaces de comunicaciones, dando como resultado los siguientes beneficios:

- Productividad de datos mejorada en líneas de baja velocidad
- Costes reducidos en líneas de alto coste
- Tiempos de respuesta más rápidos, dando como resultado mejoras en la productividad

La compresión de datos SNA es compatible con las implantaciones de S/390 y AS/400 y puede utilizarse con todos los tipos de LU.

Discovery de proveedores de servicio

Discovery es un protocolo de resolución de direcciones de la LAN que un nodo puede utilizar para buscar otro nodo que coincida con los criterios de búsqueda dados. Mediante el ajuste del parámetro de búsqueda, un nodo puede buscar nodos de red APPN, nodos que proporcionan la función de límite SNA, AS/400, pasarelas SNA o clases de servidor definidas por el usuario. Un servidor Communications Server para Windows NT puede responder a las peticiones de

clientes como un servidor de nodos de red, una pasarela PU 2.0 o como una clase de servidor definido por el usuario. Communications Server también puede utilizar discovery para buscar nodos APPN y pasarelas SNA.

Peticionario de LU dependientes (DLUR)

Communications Server proporciona soporte de nodo final y de nodo de red del peticionario de LU dependientes (DLUR) para estaciones de trabajo, permitiéndoles aprovechar las ventajas del soporte de punto de control de servicios del sistema (SSCP) mejorado proporcionado por un servidor de LU dependientes (DLUS). DLUS está soportado por VTAM V4R2 y posteriores. Con este soporte, las LU SNA dependientes tradicionales como, por ejemplo, emuladores e incluso impresoras, pueden obtener ventajas de una red APPN.

Algunos de estos beneficios son:

- Permitir que las LU dependientes residan en nodos que no son adyacentes al sistema principal
- Utilizar la lógica de búsqueda APPN para proporcionar la mejor vía de acceso para sesiones LU-LU

Consulte el apartado “Soporte del peticionario de la unidad lógica dependiente” en la página 55 para obtener más información acerca de DLUR.

Pasarela SNA

Una pasarela permite la comunicación entre sistemas principales que dan soporte a estaciones de trabajo PU 2.0 y estaciones de trabajo que utilizan tipos de DLC diferentes. Una pasarela SNA puede realizar las siguientes acciones:

- Permitir que las estaciones de trabajo compartan el mismo enlace con el sistema principal
- Proporcionar conectividad de múltiples sistemas principales a las estaciones de trabajo que no tienen la posibilidad de múltiples PU
- Actuar como una agrupación de PU para las estaciones de trabajo en sentido descendente de PU dedicadas
- Actuar como conversor de protocolo entre estaciones de trabajo que utilizan en sus enlaces unos DLC que son diferentes del DLC que se utiliza en el enlace con el sistema principal
- Reducir la cantidad de definición del sistema en el sistema principal y estaciones de trabajo
- Permitir al usuario cambiar dinámicamente las definiciones de red y añadir estaciones de trabajo
- Reducir recursos del sistema principal y reducir el número de conexiones del sistema principal mediante la utilización de LU agrupadas y por la desconexión automática de las sesiones que no se utilizan durante el período de tiempo especificado por el usuario.
- Mejorar la fiabilidad proporcionando un enlace de reserva del sistema principal

La pasarela SNA permite que un sistema principal de la familia S/390 de soporte a las estaciones de trabajo que implantan LU 0, 1, 2, 3 o LU 6.2 dependiente (APPC). La pasarela SNA también da soporte a LU 0, 1, 2 ó 3 para un sistema

principal AS/400. El sistema principal AS/400 pasa los datos a través de un sistema principal de la familia S/390.

Cada sistema principal ve la pasarela SNA como un nodo PU 2.0 SNA, que da soporte a una o varias LU por estación de trabajo. En lo relativo al sistema principal, todas las LU pertenecen a la PU de pasarela SNA. La pasarela SNA puede tener múltiples conexiones del sistema principal simultáneamente y direccionar diferentes sesiones de estación de trabajo a sistemas principales especificados. Sin embargo, sólo un sistema principal (y debe estar en un enlace con una PU CP) puede actuar como punto focal y el nombre de punto de control se añade a todos los transportes de vectores de la gestión de red (NMVT) direccionados a través de la pasarela.

Para las estaciones de trabajo soportadas, la pasarela SNA se parece a un controlador de comunicaciones PU 4 SNA y reenvía mensajes del sistema principal, como BIND y UNBIND. Las LU de red no conocen la pasarela SNA. Sin embargo, la pasarela SNA, conoce todas las LU de las estaciones de trabajo.

En realidad, la pasarela SNA es un tipo especial de PU 2.0. Mientras una estación de trabajo dependiente está inactiva, la pasarela SNA implanta las funciones de LU para la estación de trabajo, igual que lo haría una PU 2.0 real. Sin embargo, en cuanto la estación de trabajo está en línea con el sistema principal, la pasarela SNA permite a la estación de trabajo implantar las funciones de LU y solamente pasa datos entre las estaciones de trabajo y el sistema principal.

Una pasarela SNA habilita las aplicaciones de estación de trabajo soportadas para acceder a las aplicaciones remotas soportadas de una red de subárea sin necesidad de una conexión directa separada con cada sistema principal en cada estación de trabajo. Desde el punto de vista de un sistema principal, el sistema principal tiene una sola conexión con la pasarela.

Consulte el apartado “Planificación de la pasarela SNA” en la página 115 para obtener más información sobre la utilización de la pasarela SNA.

La Figura 4 muestra un ejemplo de una conexión utilizando una pasarela SNA.

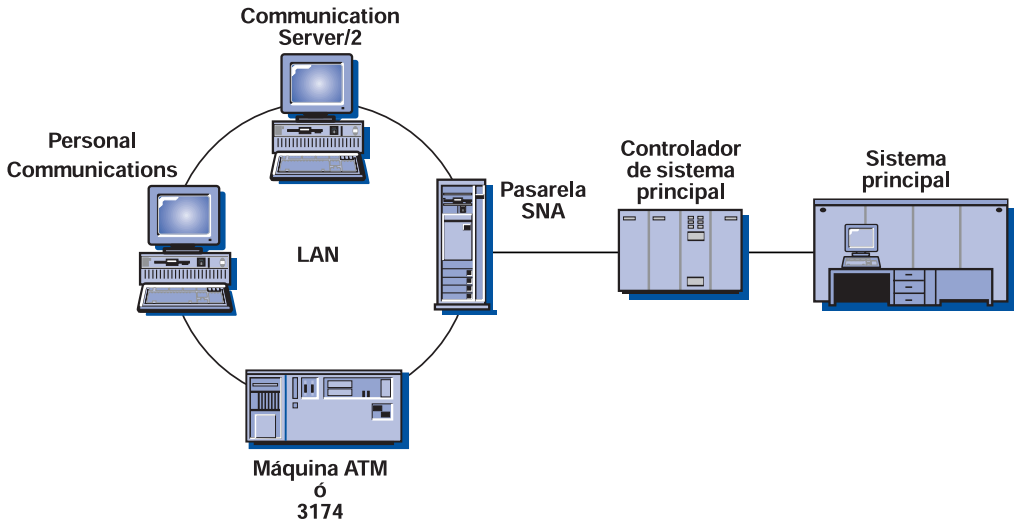


Figura 4. Ejemplo de conexiones de pasarela SNA

Soporte AnyNet

Communications Server incorpora las funciones de SNA sobre TCP/IP y Sockets sobre SNA de la familia de productos AnyNet. Este soporte le permite ampliar y simplificar la red permitiendo que las aplicaciones SNA se comuniquen a través de una red TCP/IP y que las aplicaciones Sockets se comuniquen a través de la red SNA sin realizar cambios en las aplicaciones.

SNA sobre TCP/IP

La función de nodo de acceso SNA sobre TCP/IP permite que las las aplicaciones SNA que residen en una red IP se comuniquen. Esta función da soporte a la LU6.2 independiente y las LU 0, 1, 2, 3 ó 6.2 dependientes con o sin el peticionario de LU dependientes (DLUR). Además, el nodo de acceso SNA sobre TCP/IP puede utilizarse conjuntamente con la pasarela SNA para permitir sesiones de pasarela SNA sobre TCP/IP.

La función de pasarela SNA sobre TCP/IP amplía el alcance de las aplicaciones SNA permitiendo que las aplicaciones SNA de una red SNA se comuniquen con aplicaciones SNA de una red IP. La pasarela SNA sobre TCP/IP da soporte a sesiones LU 6.2 independientes.

La Figura 5 muestra aplicaciones SNA en comunicación por medio de la pasarela SNA sobre TCP/IP a través de redes IP y SNA.

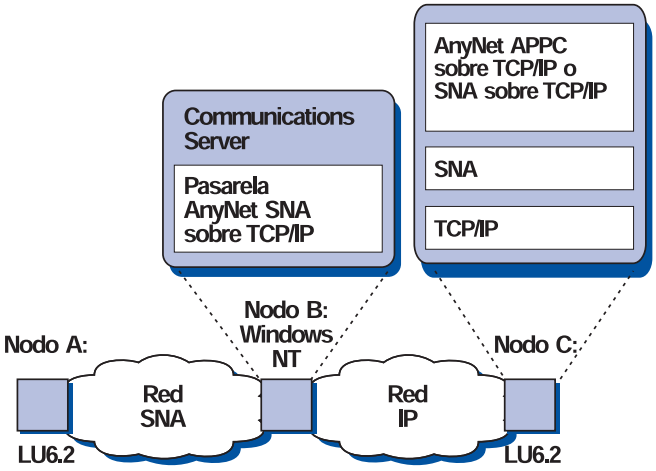


Figura 5. Pasarela SNA sobre TCP/IP

Sockets sobre SNA

La función de nodo de acceso Sockets sobre SNA permite que los programas de aplicación TCP/IP que utilizan las interfaces de socket WinSock 1.1 y WinSock 2.0 se comuniquen en una red SNA.

La función de pasarela Sockets sobre SNA permite que las aplicaciones sockets de las redes SNA y TCP/IP se comuniquen. Con frecuencia, las pasarelas Sockets sobre SNA se utilizan para conectar redes TCP/IP aisladas utilizando una red principal SNA.

La Figura 6 en la página 14 muestra aplicaciones Socket en comunicación mediante una pasarela Sockets sobre SNA a través de redes IP y SNA.

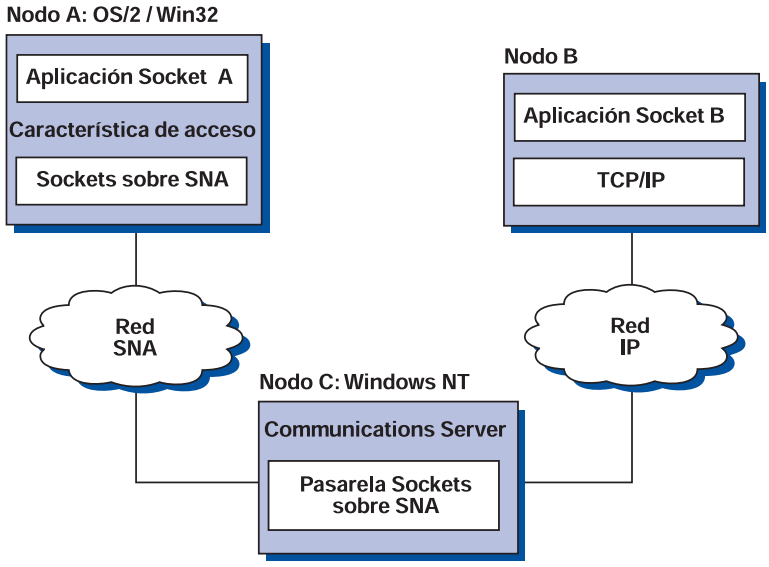


Figura 6. Pasarela Sockets sobre SNA

Servidor TN3270E

La función del servidor TN3270E permite que los usuarios TCP/IP accedan a aplicaciones que se encuentran en una máquina de sistema principal de una red SNA. Cualquier estación de trabajo cliente TN3270 o TN3270E estándar de la industria puede conectarse con el servidor TN3270E para acceder a las redes SNA. El servidor TN3270E da soporte al manejo de teclas ATTN y SYSREQ y permite que los usuarios impriman desde las aplicaciones del sistema principal en las impresoras conectadas a su estación de trabajo. Estas impresoras pueden estar conectadas localmente o conectadas a la red.

Communications Server da soporte al equilibrio de la carga para conexiones cliente de un servidor TN3270E que se conecta a los mismos recursos del sistema principal, si el cliente tiene habilitado el equilibrio de la carga.

El servidor TN3270E da soporte al filtro de IP y de nombres de sistema principal que permite el acceso controlado a las LU sin modificar las configuraciones del cliente.

El servidor TN3270E también da soporte a la autentificación y cifrado de la Capa de sockets segura (SSL), proporcionando un acceso seguro en la red TCP/IP. Si especifica la seguridad, el servidor debe tener una certificación autentificada proporcionada por una autorización certificada como, por ejemplo, Verisign. Communications Server proporciona un programa de utilidad que genera y gestiona las claves y certificaciones utilizados por SSL Versión 3.

La Figura 7 muestra un ejemplo de conexiones del servidor TN3270E.

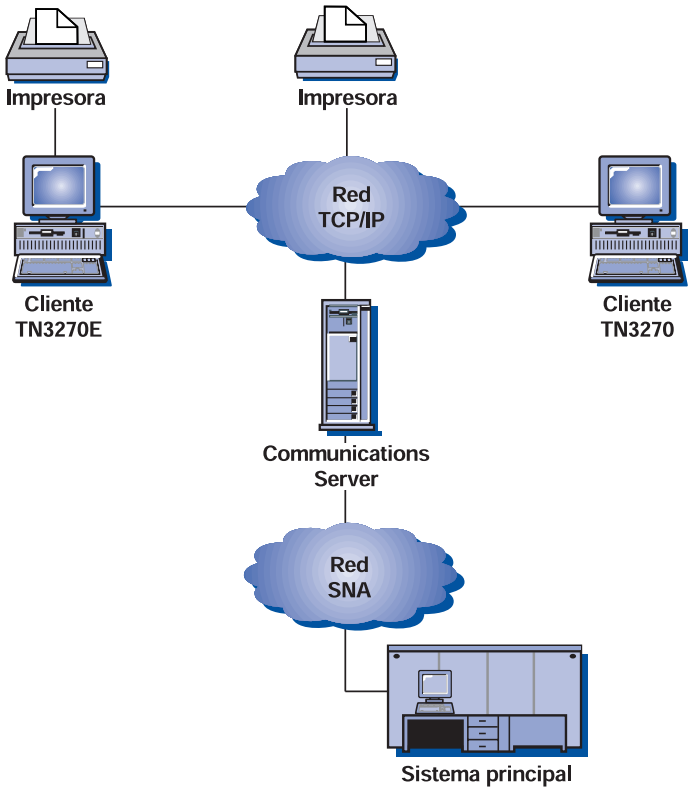


Figura 7. Conexiones del servidor TN3270E

Servidor TN5250

La función del servidor TN5250 permite que los usuarios TCP/IP accedan a aplicaciones que se encuentran en un AS/400 de una red SNA. Cualquier estación de trabajo cliente TN5250 estándar de la industria puede conectarse con el servidor TN5250 para acceder a las redes SNA.

Communications Server da soporte al equilibrio de la carga para conexiones cliente de los servidores TN5250 que se conectan a los mismos AS/400, si tienen habilitado el equilibrio de la carga.

El servidor TN5250 da soporte al filtro del nombres de sistema principal y de IP que permite la administración central del acceso de clientes al servidor, así como el direccionamiento de clientes a AS/400 específicos.

El servidor TN5250 también da soporte a la autentificación y cifrado de la Capa de sockets segura (SSL), proporcionando un acceso seguro en la red TCP/IP. Si especifica la seguridad, el servidor debe tener una certificación autentificada proporcionada por una autorización certificada como, por ejemplo, Verisign. Communications Server proporciona un programa de utilidad que genera y gestiona las claves y certificaciones utilizados por SSL Versión 3.

La Figura 8 muestra un ejemplo de conexiones del servidor TN5250.

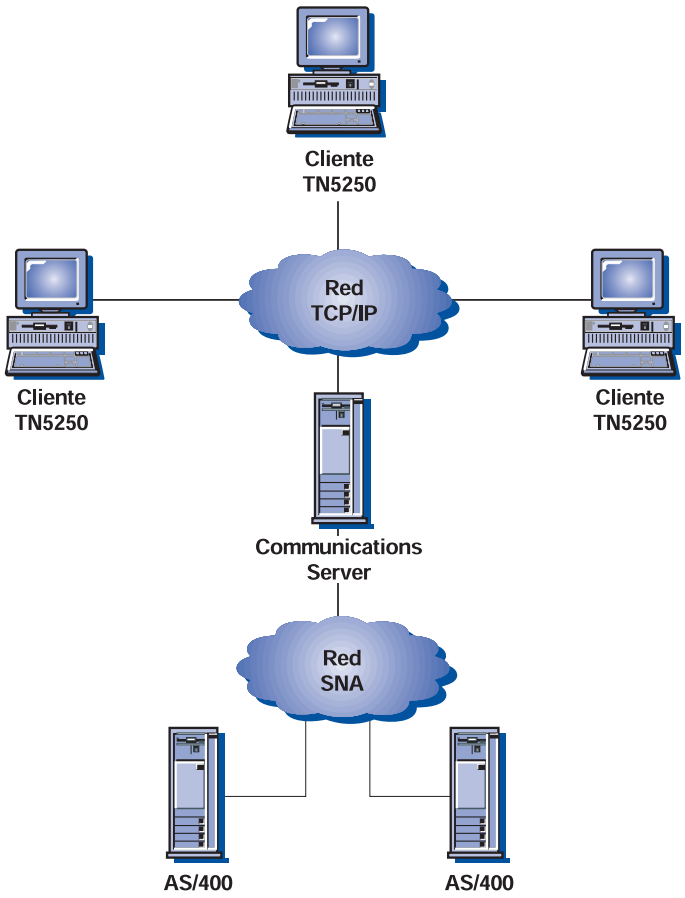


Figura 8. Conexiones del servidor TN5250

Acceso de datos de legado

Communications Server proporciona acceso a los datos de máquinas de sistema principal, AS/400 y estaciones de trabajo en redes SNA mediante las funciones siguientes:

- Proveedor de AS/400 OLE DB
- Editor del sistema principal
- Servidor de carpetas compartidas AS/400

Proveedor de AS/400 OLE DB

Las aplicaciones que utilizan OLE DB o ActiveX pueden comunicarse mediante Communications Server para acceder a nivel de registro a los archivos de un AS/400. La documentación de esta función, así como la información acerca del desarrollo de estas aplicaciones utilizando el Client Access, se proporciona en el directorio `csnt\sdk\as400_oledb`.

Editor del sistema principal

El Editor del sistema principal proporciona el acceso en la Web para los sitios de la Web de gran volumen con contenido dinámico. Puede utilizar el Editor del sistema principal para acceder a los datos de los sistemas principales S/390 o AS/400 y para publicarlos en las páginas de la Web creadas dinámicamente a partir de su propio diseño.

Servidor de carpetas compartidas AS/400

El sistema AS/400 utiliza una estructura llamada carpeta para almacenar y organizar los documentos, el correo y otros objetos relacionados. Communications Server le permite crear dispositivos de disco en el servidor que se comunican con las carpetas AS/400 a través del sistema de archivos integrado (IFS) de AS/400. Además, si el servidor comparte estos dispositivos de disco, los clientes pueden emitir NET USE para los mismos. Se pueden conectar múltiples clientes a las carpetas del sistema AS/400 como si fueran unidades de sus estaciones de trabajo.

Puede utilizar las carpetas compartidas para:

- Utilizar la seguridad del AS/400 para limitar el acceso a los archivos de la estación de trabajo
- Compartir los datos con múltiples usuarios a la vez
- Hacer copias de seguridad de los archivos de la estación de trabajo en una carpeta AS/400

Soporte de cliente de Communications Server

Communications Server proporciona soporte para los clientes API SNA (disponibles en CD-ROM,) y para clientes Novell IntranetWare para SAA.

Soporte de clientes API SNA

El soporte de cliente API SNA de Communications Server permite que los clientes conectados por TCP/IP e IPX accedan a las API SNA sin necesitar protocolos SNA para el flujo entre los clientes y el servidor. Esto permite que la mayor parte de la configuración SNA se realice en el servidor central.

Communications Server da soporte a clientes API SNA en Windows 95, Windows NT, Windows 3.1 y OS/2.

Los clientes SNA proporcionan soporte para las interfaces API CPI-C, APPC, EHNAPPC, LUA RUI, JCPI-C y HACL, a la vez que proporcionan el proceso SNA real en el servidor. Estos clientes se suministran como parte del servidor pero, en realidad, se instalan y configuran en el cliente.

Los clientes Windows de 32 bits y OS/2 tienen mejoras adicionales:

- Cifrado entre cliente y servidor
- Formato de rastreo más detallado que sirve de ayuda para depurar los problemas más rápidamente
- Posibilidad de iniciar y detener el rastreo mientras el cliente está en ejecución
- Posibilidad de volver a instalar el cliente sin desinstalarlo

Los clientes Windows NT y Windows 95 se ejecutan desde el mismo ejecutable. Este ejecutable se puede instalar en una unidad compartida; cualquier arreglo se aplica a ambos clientes. El nuevo cliente Windows de 32 bits puede comunicarse con los servidores Communications Servers o Novell IntranetWare o NetWare para SAA.

Para obtener más información acerca de los clientes API en Communications Server, consulte el apartado “Planificación de la comunicación cliente/servidor” en la página 95.

Soporte de cliente Novell IntranetWare para SAA

Communications Server da soporte a clientes conectados por IPX o TCP/IP que ejecutan paquetes de software emulador que implanta la arquitectura Queue Element/Message Unit (QEL/MU) de Novell para la emulación 3270, permitiendo que los clientes accedan a los datos del sistema principal. Esto incluye el soporte de características de clientes conocidas, incluyendo las categorías de LU dedicadas, agrupadas y públicas (a las que algunas veces se hace referencia como tipos de recurso).

Communications Server da soporte a clientes Novell IntranetWare para SAA en Windows 95, Windows NT, Windows 3.1 y OS/2.

Consulte el manual *Novell NetWare for SAA 3270 Client Interface Guide and Reference* P/N 100–002018–001 para obtener más información acerca del desarrollo de estos clientes.

Equilibrio de la carga

Ahora, Communications Server da soporte al equilibrio de la carga para todos los tipos de cliente. El equilibrio de la carga le permite distribuir las sesiones LU 0 a 3 y LU 6.2 entre los servidores Communications Server e IntranetWare para SAA. El servidor anuncia los servicios incluyendo los factores de carga, que los clientes o servidores pueden reunir y organizar para seleccionar un servidor.

Explotación de directorio

Puede configurar múltiples clientes desde una ubicación central utilizando el protocolo Lightweight Directory Access Protocol (LDAP) para simplificar el proceso de configuración.

Para obtener información acerca de la utilización de la explotación de directorio, consulte el apartado “Planificación de la comunicación cliente/servidor” en la página 95.

Soporte de configuración y administración

Communications Server proporciona servicios para configurar y administrar los recursos.

Configuración de Communications Server

Esta sección proporciona una visión general de los componentes de la configuración de Communications Server y los métodos utilizados para crearlos o cambiarlos. La configuración está compuesta de un solo archivo (ACG) almacenado en el subdirectorio PRIVATE del directorio donde ha instalado el producto (por ejemplo, C:\IBMCS\PRIVATE). El archivo ACG puede crearse o configurarse mediante **Configuración de nodos** o utilizando un editor ASCII. Está disponible un programa de verificación para comprobar la validez del archivo ACG antes de utilizarlo.

Puede utilizar los siguientes métodos para crear o cambiar una configuración de Communications Server:

- **Configuración de nodos**
- Configuración del archivo de respuesta

Configuración de nodos: Communications Server proporciona la aplicación **Configuración de nodos** (PCSCFG) que le permite configurar las funciones de Communications Server utilizando una interfaz gráfica y suministra los valores por omisión para que pueda configurarlas fácilmente utilizando una cantidad mínima de parámetros. Cuando se realiza una configuración, un paso de verificación automática examina la configuración que ha creado y, si no existen conflictos, crea los archivos de configuración necesarios. Si existen conflictos, se informan para que pueda corregirlos en la configuración.

Se da soporte a la configuración local a nivel de cliente y de servidor. Se da soporte a la configuración remota del servidor en clientes Windows NT y Windows 95.

La mayoría de configuraciones pueden crearse utilizando **Configuración de nodos**. Sin embargo, hay unas cuantas palabras clave y algunos parámetros de palabras clave a los que **Configuración de nodos** no da soporte.

Configuración del archivo de respuesta: La configuración del archivo de respuesta le permite personalizar un modelo de archivo de configuración para satisfacer las necesidades de usuarios específicos. Para obtener más información sobre la utilización de archivos de respuesta para la configuración, consulte el apartado “Configuración con archivos modelo y de respuesta” en la página 192.

Operaciones de nodos SNA: **Operaciones de nodos SNA** proporciona la posibilidad de crear y modificar los recursos seleccionados.

Administración de Communications Server

Communications Server proporciona los siguientes servicios para la administración de recursos.

- **Operaciones de nodos SNA**
- Programas de utilidad de la línea de mandatos
- Administración basada en la web
- Módulo Tivoli Plus

Para obtener más información sobre las posibilidades de estos recursos, consulte el apartado “Recursos de gestión de sistemas” en la página 205.

Equilibrio de la carga

El equilibrio de la carga es una función de Communications Server que equilibra dinámicamente las sesiones de LU dependiente (sistema principal a estación de trabajo) y sesiones de LU 6.2 independiente distribuyéndolas al servidor de comunicaciones que tenga menor carga. Communications Server realiza el equilibrio de la carga para los programas API de Communications Server y emuladores 3270 que se conectan mediante protocolos TCP/IP o emuladores TN3270 y TN5250 de otros fabricantes. Los recursos entre los que se produce el equilibrio de la carga dependen del tipo de sesión:

- En el caso de sesiones LU dependientes, la carga se distribuye entre servidores de una agrupación de LU nombrada y un ámbito nombrado.
- En el caso de sesiones LU 6.2, la carga se distribuye entre todos los servidores disponibles de un ámbito nombrado o entre los servidores seleccionados de una lista de servidores nombrados.

Las posibilidades del equilibrio de la carga de Communications Server se crean en las API de cliente SNA. El equilibrio de la carga para los clientes se configura utilizando **Configuración de cliente SNA**.

En el caso de sesiones LU dependientes, los emuladores que utilizan las API de cliente SNA pueden participar en el equilibrio de la carga. De lo contrario, es necesario adquirir el software de emulador 3270, TN3270 o TN5250 que de soporte al equilibrio de la carga.

En las sesiones LU 6.2, la conexión inicial establecida por un cliente API SNA determina el servidor que gestionará todas las sesiones LU 6.2 posteriores.

Para obtener más información sobre el equilibrio de la carga, consulte el apartado “Planificación del equilibrio de la carga” en la página 145.

Seguridad de datos

Communications Server proporciona el soporte de seguridad básica y mejorada a niveles de sesión y de conversación. Existe seguridad en la limitación de los usuarios Windows NT que pueden acceder a recursos SNA a través de clientes API SNA. La seguridad de conversación incluye el soporte para la sustitución de contraseñas. También está la seguridad LU-LU mejorada.

Communications Server proporciona soporte para la seguridad basada en la Capa de sockets segura (SSL) en las conexiones entre clientes TN y el servidor TN3270E o el servidor TN5250. Esta seguridad utiliza SSL Versión 3 para proporcionar el cifrado de datos y la autentificación utilizando certificaciones firmadas.

Soporte de adaptadores

Communications Server proporciona una interfaz abierta para que los fabricantes de adaptadores creen soluciones de conectividad. Se proporciona una interfaz de adaptador superficial (no programable) para que los fabricantes de adaptadores trabajen con el SDLC de Communications Server y la pila de protocolo X.25. Se proporciona una interfaz de adaptador profunda (programable) para que los fabricantes de adaptadores creen soluciones de conectividad utilizando los controles de enlaces de datos suministrados por el fabricante.

Soporte de Control de enlace de datos (DLC)

Communications Server permite las comunicaciones en los siguientes DLC:

- AnyNet (SNA sobre TCP/IP)
- Twinaxial (sólo en sentido ascendente)
- LAN (cualquier adaptador de red que se ajuste a NDIS**)
- SDLC X.25 (síncrono, asíncrono y AutoSync)
- OEM (soporte de adaptador de otros fabricantes)
- Canal (sólo en sentido ascendente)
- Canal de múltiples vías (sólo HPR)
- Ampliación de empresa

DCL AnyNet (SNA sobre TCP/IP)

Para obtener más información acerca del DLC de AnyNet SNA sobre TCP/IP, consulte el apartado “SNA sobre TCP/IP” en la página 13.

DLC de canal de múltiples vías IBM

El DLC de Canal de múltiples vías (MPC) proporciona conexiones de fibra de alta capacidad y de alta disponibilidad con uno o más sistemas principales con posibilidad de MPC S/390 mediante la tarjeta adaptadora de canal ESCON (P/N 9663 001). Las conexiones MPC proporcionan altas velocidades de transmisión de datos con copia de seguridad transparente cuando las conexiones físicas se interrumpen o no están disponibles temporalmente. Esta conexión de canal a canal le permite proporcionar a los clientes de la LAN un acceso preparado para los recursos y servicios S/390.

DLC de ampliación de empresa

Ahora, Communications Server proporciona conexiones HPR en redes IP, utilizando paquetes UDP/IP. Para la red HPR, la red principal IP parece como si fuera un enlace lógico. Para la red IP, el tráfico SNA parece como datagramas UDP. Estos datagramas se direccionan sin cambios a la red principal IP. Puesto que no se efectúa ninguna transformación de protocolo y como el empaquetamiento se lleva a cabo en la capa de direccionamiento sin la actividad de capas de transporte adicionales, da como resultado una utilización eficaz de la infraestructura de intranet para los clientes IP que acceden a los datos basados en SNA (clientes TN3270 o navegadores de la Web que utilizan IBM Host on Demand, por ejemplo), así como para clientes SNA.

Soporte MIB APPN

Communications Server da soporte a las peticiones del protocolo simple de gestión de red (SNMP) para la información de gestión APPN de cualquier sistema de gestión SNMP.

Espera en caliente

En Communications Server, puede configurar ciertos enlaces del sistema principal para que se activen automáticamente si falla un servidor crítico especificado. Las conexiones configuradas en un sistema principal pueden continuar funcionando mediante la activación de conexiones alternativas en un servidor de reserva. Esta función se conoce como espera en caliente.

Las conexiones nombradas en la configuración de un servidor crítico del servidor de reserva se activan cuando el servidor de reserva detecta una pérdida de contacto con el servidor crítico y los cargos de licencias para el servidor crítico se gestionan en el servidor de reserva.

Nota: La característica de espera en caliente sólo activa las conexiones del sistema principal en un servidor de reserva y depende de la utilización del software emulador que da soporte al direccionamiento alternativo al servidor de reserva cuando un servidor crítico queda inactivo.

Para obtener más información sobre la utilización de la espera en caliente para las conexiones de reserva, consulte el apartado “Planificación de las conexiones del sistema principal de reserva” en la página 149.

Funciones del emulador de nivel de entrada

Communications Server incluye una versión a nivel de entrada del conocido emulador Personal Communications 3270 y 5250 con fines administrativos. Este emulador proporciona un soporte básico de 5250 y 3270 en el servidor que incluye un subconjunto de las características y funciones que están en la familia de emuladores de IBM Personal Communications de funciones completas.

Las funciones de emulación de nivel de entrada proporcionadas son:

- Correlación de color
- Transferencia de línea de mandatos (sólo 3270)
- Juego de fonts completo
- Modalidad de tamaños de pantalla 2-5
- Dos sesiones

Aunque no se de soporte a volver a correlacionar el teclado gráfico para el emulador de nivel de entrada, puede utilizar los archivos de volver a correlacionar generados por el emulador de funciones completas.

Communications Server y SNA

Este capítulo explica las funciones de red SNA proporcionadas por Communications Server e incluye los temas siguientes:

- Visión general de las funciones SNA
- Definiciones de Control de enlace de datos (DLC)
- Red avanzada de igual a igual (APPN)
- Direccionamiento de alto rendimiento (HPR)
- soporte de LU
- Compresión de datos
- Cifrado
- Servicios de gestión (MS)
- Control de flujo
- Soporte de pasarela SNA

Visión general de las funciones SNA

Esta sección proporciona una visión general de cómo Communications Server implanta SNA en una estación de trabajo. No es una explicación exhaustiva de las funciones SNA. Para obtener información más detallada acerca de SNA, consulte los manuales siguientes:

- *Systems Network Architecture Concepts and Products*
- *Systems Network Architecture Technical Overview*
- *Systems Network Architecture Network Product Formats* (disponible en línea en la lista de documentación de Communications Server)
- *Systems Network Architecture Format and Protocol Reference Manual: Architecture Logic for LU Type 6.2*

SNA define los estándares, protocolos y funciones utilizados por los dispositivos de la red (desde sistemas principales a terminales) para comunicarse entre sí. Esta comunicación permite que estos dispositivos compartan información transparentemente y procesen recursos. En otras palabras, un usuario de una estación de trabajo no tiene que conocer lo que ocurre en el segundo plano para acceder a la información de un sistema principal o para comunicarse con otro usuario.

Una red SNA está organizada como un sistema de nodos y enlaces. Es importante recordar que esta organización es lógica. SNA clasifica los nodos de acuerdo a sus posibilidades y el grado de control que tienen sobre otros nodos de la red. El tipo de nodo no está asociado necesariamente con un tipo específico de hardware. Las posibilidades de un nodo pueden realizarse por distintos dispositivos. Una estación de trabajo que actúa como pasarela puede realizar las mismas funciones que un controlador de comunicaciones. Incluso es posible que un solo dispositivo contenga más de un nodo.

La red SNA es responsable de mover los datos entre dos usuarios finales de una manera eficaz, ordenada y fiable. Por ejemplo, cuando un usuario de una estación

© Copyright IBM Corp. 1989, 1996

de trabajo envía un mensaje a otra estación de trabajo, SNA lleva a cabo las siguientes acciones:

- Empaqueta el mensaje en un formato que pueda utilizarse en el tipo de enlace
- Direcciona el paquete
- Selecciona una ruta para el mensaje
- Supervisa la comunicación para asegurarse de que el mensaje llega a su destino
- Convierte el mensaje de nuevo a un formato que pueda utilizarse en el destino

Estas tareas se definen en SNA como capas funcionales separadas. Estas capas no forman parte de la explicación que se ofrece aquí, pero es importante recordar que todas las capas SNA forman parte de un enlace lógico.

Tal como se ha mencionado anteriormente, los nodos SNA se clasifican de acuerdo a sus posibilidades de comunicaciones y el grado de control que el nodo tiene sobre otros nodos de la red. Los nodos SNA se clasifican de manera amplia como nodos de subárea y nodos periféricos. Los nodos de subárea son como ejes y pueden comunicarse con los nodos periféricos y con otros nodos de subárea. Los nodos de subárea activan y controlan los recursos de los nodos periféricos. Los nodos de subárea también se clasifican como nodos de tipo 4 o de tipo 5. Los nodos de tipo 5 contienen un punto de control de servicio del sistema (SSCP) que proporciona un punto de control central para los nodos de tipo 4 que están conectados a ellos. A veces se hace referencia al nodo de tipo 5 como nodo de sistema principal. Un nodo periférico sólo puede comunicarse directamente con el nodo de subárea al que está conectado. Sin embargo, los nodos periféricos pueden controlar los dispositivos a los que están conectados. Por ejemplo, un controlador de cluster que actúa como nodo periférico puede dar soporte a terminales que están conectados al mismo. También se hace referencia a los nodos periféricos como nodos de tipo 2 o de tipo 2.1.

Cada nodo contiene unidades accesibles de red (NAU) que efectúan las funciones de control y comunicación. Una de estas NAU es una unidad física (PU). La PU gestiona los recursos físicos del nodo. Otras NAU llamadas unidades lógicas (LU) proporcionan puntos de acceso lógico a la red que permiten la comunicación entre los usuarios y las aplicaciones de cada nodo. Se hace referencia a la comunicación entre unidades lógicas como sesión. Las sesiones no sólo dan soporte a la comunicación entre usuarios y aplicaciones, sino que también dan soporte a la comunicación entre aplicaciones para que compartan el proceso de recursos. La comunicación entre aplicaciones se conoce como comunicación avanzada programa a programa (APPC). APPC es un conjunto de convenios y protocolos de programación que implantan la LU 6.2. (APPC es el nombre que se da a la posibilidad LU 6.2 en los productos que implantan este tipo de LU.)

Perfiles de control de enlace de datos

El control de enlace de datos (DLC) permite el intercambio ordenado de datos entre dos nodos a través de un enlace lógico. El DLC proporciona los protocolos necesarios para el suministro fiable de las unidad básica de transmisión (BTU) entre un par de nodos de la red SNA. Debe configurar los perfiles adecuados de DLC de Communications Server para que una estación de trabajo acceda a una red SNA.

Consulte la *Guía de aprendizaje* en línea para obtener más información sobre la configuración de los perfiles DLC adecuados.

Red avanzada de igual a igual

Red avanzada de igual a igual (APPN) es una extensión de SNA que añade funciones de comunicaciones adicionales a las descritas en las secciones anteriores. Sus componentes básicos son:

- Tipos de nodo APPN
- Puntos de control
- Red derivada
- Control de enlace de datos
- Enlaces lógicos
- Servicios del directorio
- Topología y servicios de selección de rutas

Tipos de nodo APPN

Esta sección explica los tres tipos de nodos implantados por Communications Server que pueden participar en una red APPN:

- Nodo de red
- Nodo final
- Nodo de Red de entrada limitada (LEN)

Además, la red derivada es una extensión de un nodo de red. Aunque proporciona servicios para los nodos finales como un nodo de red, aparece en la red como si fuese un nodo final conectado a otros nodos de red.

Cada nodo se distingue de los demás nodos de la red por un nombre exclusivo que consta de dos partes—un ID de red y un nombre de nodo local (conocido también como nombre de punto de control [CP]). El nombre identifica cada nodo para todos los demás nodos de la red. También, el nodo puede tener múltiples nombres de PU para el acceso simultáneo a múltiples sistemas principales PU T4/5.

Un nodo puede configurarse para ser un nodo final o un nodo de red, pero cuando un nodo final no tiene sesiones CP-CP (consulte el apartado “Sesiones CP-CP” en la página 28) para un nodo de red APPN, actúa como un nodo LEN. Un nodo LEN no da soporte a funciones APPN.

Los tipos de nodo se describen con más detalle en las secciones siguientes. La Figura 9 en la página 26 ilustra un ejemplo de red APPN que incluye todos estos tipos de nodo.

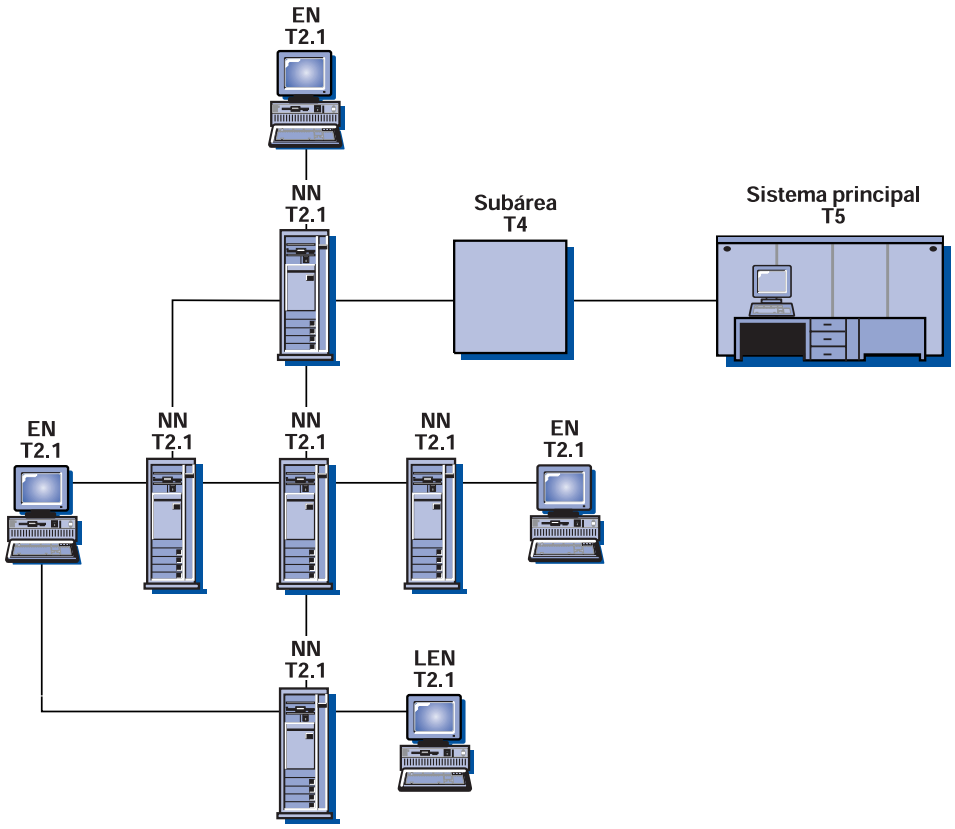


Figura 9. Parte de una red APPN de ejemplo. Esta vista de la topología de red muestra cinco nodos de red (NN). Están conectados tres nodos finales (EN), así como un nodo LEN y una subárea. Los programas de aplicación APPC escritos para cualquier nodo de esta red pueden comunicarse con cualquier otro.

Nodo de red

Un nodo de red da soporte a sus propios usuarios finales; proporciona los servicios del directorio, de selección de ruta y de gestión para los nodos finales; y realiza el direccionamiento intermedio de datos en las sesiones que lo atraviesan. El nodo de red lleva a cabo búsquedas distribuidas de la red para localizar las LU asociadas y calcula la mejor ruta desde el nodo de origen al nodo de destino basándose en el criterio especificado por el usuario.

Un servidor de nodos de red hace referencia a la función de un nodo de red cuando actúa como punto de entrada de la red para los nodos finales específicos que tiene conectados. Estos nodos finales están definidos como que están en su dominio. Por ejemplo, todas las peticiones de directorio en relación a los recursos (por ejemplo, las LU) de estos nodos finales (así como sus propios recursos) pasan a través de los servicios del directorio del servidor de nodos de red. Los nodos de red pueden reunir y controlar la información de directorio que pasa en la red APPN.

Un nodo de red proporciona lo siguiente:

- Servicios de sesión LU-LU para sus LU residentes localmente
- Direccionamiento de sesiones intermedias

- Funciones de servidor de red (para realizar búsquedas de directorio de red y selección de ruta) para los nodos finales conectados o los nodos LEN (así como sus propias LU residentes localmente)
- La posibilidad de direccionamiento de los Servicios de gestión (MS) para reenviar datos de servicios de gestión (alertas, por ejemplo) entre un nodo final servido y un punto focal (FP) de servicios de gestión.

Nodo final

Un nodo final funciona en un entorno similar para sesiones LU-LU (que utilizan protocolos LU 6.2) a la vez que proporciona funciones APPN adicionales. Un nodo final proporciona funciones APPN como, por ejemplo, servicios del directorio y servicios de selección de ruta para los usuarios finales en su propio nodo. Puede participar en la red APPN utilizando los servicios de un servidor de nodo de red conectado para las peticiones de sesión que implican nodos no conectados directamente; hace esto intercambiando peticiones y repuestas para los servicios del directorio con un nodo de red adyacente (su servidor) utilizando sesiones CP-CP.

Los nodos finales APPN pueden registrar sus LU locales en su servidor de nodos de red. Mediante el registro de los nodos finales, el operador de la red del servidor de nodos de red no necesita predefinir los nombres de LU para las LU de todos los nodos finales conectados para los cuales el nodo de red proporciona servicios.

Un nodo final APPN puede estar conectado a múltiples nodos de red, pero sólo puede tener sesiones CP-CP activas con un nodo de red cada vez—su servidor de nodo de red. Los demás nodos de red pueden utilizarse para proporcionar el direccionamiento de sesiones intermedias para el nodo final o como sustitutos del servidor de nodos de red si el servidor de nodos de red principal no se puede utilizar. Nunca se establecen sesiones CP-CP entre dos nodos finales.

Nodo LEN

Un nodo LEN es un nodo que implanta los protocolos T2.1 básicos sin las mejoras APPN. En un nodo LEN, todas las conexiones posibles con las LU asociadas están predefinidas antes de iniciar sesiones con ellas. Un nodo LEN, conectado a un nodo de red APPN adyacente, utiliza las funciones avanzadas de APPN predefiniendo las posibles conexiones con las LU asociadas como si existiesen en ese nodo de red. El nodo de red, a su vez, puede actuar automáticamente como servidor de nodos de red del nodo LEN y localizar el destino real de la LU asociada y seleccionar la mejor ruta a la misma. Pasando por un nodo de red, el nodo LEN puede participar en una red APPN sin necesidad de conexiones directas con todos los nodos.

Puntos de control

El punto de control (CP) es responsable de gestionar el nodo y sus recursos. Para obtener los servicios de red APPN, el punto de control de un nodo final APPN debe comunicarse con el punto de control de un nodo de red adyacente. También, para gestionar la red, el punto de control de un nodo de red APPN debe comunicarse con los puntos de control de los nodos de red adyacentes. El punto de control dirige las funciones como, por ejemplo, la activación y desactivación del adaptador y la activación y desactivación del enlace y ayuda a las LU en la iniciación y terminación de la sesión.

Cuando se configura una estación de trabajo, debe definirse el nombre de punto de control (conocido también como nombre de nodo local). El punto de control

también es una LU y se puede elegir que la LU de punto de control sea la única LU definida en la estación de trabajo.

Sesiones CP-CP

Para realizar los servicios del directorio y topología y los servicios de selección de ruta, los nodos adyacentes de la red APPN utilizan un par de sesiones CP-CP paralelas para intercambiar la información de red. Los nodos de red utilizan sesiones CP-CP para supervisar los nodos de un enlace de red, así como para hacer un seguimiento de los servicios del directorio y de sesión. Un nodo de red establece dos sesiones paralelas con cada nodo de red adyacente y con cada nodo final servido. Un nodo final APPN establece dos sesiones paralelas con un solo nodo de red adyacente actuando como su servidor actual. Los nodos LEN no dan soporte a sesiones CP-CP.

Una vez establecida una conexión, los nodos intercambian información de identificación de intercambio (XID). Después, se inician las sesiones CP-CP entre los puntos de control de los nodos conectados directamente. Las sesiones CP-CP utilizan los protocolos LU 6.2 y las dos sesiones de un par deben estar activadas para que los puntos de control asociados empiecen y sostengan sus interacciones. Todas las sesiones CP-CP se utilizan para conducir búsquedas de directorio.

Una vez establecidas las sesiones CP-CP, los dos nodos intercambian mensajes de posibilidad de punto de control que informan a cada nodo de las posibilidades del otro. Cuando ambos nodos son nodos de red, intercambian mensajes de actualización de base de datos de topología (TDU). Los mensajes TDU contienen la información de identificación, las características del nodo y del enlace y los números de secuencia de los recursos para identificar las actualizaciones más recientes para cada uno de los recursos descritos en la TDU.

Activación de la conexión CP-CP

Cuando se inicia Communications Server, primero intenta activar la conexión del servidor NN preferido. Communications Server intenta activar todas las demás conexiones definidas como ***activar en el arranque***. Si existe un enlace paralelo alternativo para la conexión de servidor NN preferido, en lugar de esperar los resultados del intento de activación de la conexión del servidor NN preferido antes de intentar el enlace alternativo, Communications Server intenta activar las sesiones CP-CP del enlace alternativo.

Nota: Si la conexión se ha desactivado por petición del operador desde el nodo local, las sesiones CP-CP no se vuelven a conducir. Si la conexión se ha desactivado por petición del operador desde el nodo remoto, las sesiones CP-CP se vuelven a conducir en el nodo local. Para los enlaces entre nodos NN, sólo se activan los enlaces activados bajo petición (enlaces con el nombre de CP adyacente especificado y no definidos como ***activar en el arranque***).

Reactivación de conexión CP-CP

Communications Server proporciona soporte para la reactivación de la conexión CP-CP. La pérdida de sesiones CP-CP entre un nodo final y su servidor de nodos de red y entre los nodos de red adyacentes puede interferir en el funcionamiento de una red APPN. El soporte de reactivación de conexión CP-CP mejora la fiabilidad de una red APPN restableciendo las sesiones importantes cuando terminan debido a una anomalía o a una desactivación de la de la conexión.

El intento de reactivación de conexión CP-CP se inicia por la activación de enlace CP-CP, la anomalía de una sesión CP-CP o por la caducidad del temporizador de reintentos CP-CP. Communications Server inicia las sesiones CP-CP con el primero de los siguientes:

1. El CP-CP del servidor preferido (si no se ha intentado previamente).
2. Si está configurado el DLUR, utilice un CP adyacente que de soporte al registro de DLUR.
3. La última activación (más reciente) de NN que no se haya intentado, para la que existe una conexión activa.
4. El primero de cualquier otro NN de nivel superior de la red derivada.

Nota: Si las conexiones CP-CP se han terminado debido a una anomalía de un enlace, Communications Server no reactiva el enlace. Puede configurar una conexión como ***reactivar automáticamente*** (reintentos infinitos) para mantener activadas las conexiones importantes.

Red derivada

La red derivada es un subconjunto de nodos marco que está diseñada para interconectar una red derivada con una red principal WAN APPN. Las redes interconectadas pueden ser nativas (es decir, tener el mismo ID de red) o no nativas. Un nodo que soporta la red derivada es un nodo de red derivada que normalmente tiene interfaces LAN y WAN y que también incluye DLUR y HPR.

Los enlaces con un nodo que da soporte a una red derivada se definen como ***enlaces superiores de red derivada*** o ***enlaces inferiores de red derivada***. La Figura 10 proporciona un ejemplo de la manera en que funciona un nodo de red derivada en la red. En esta figura, el nodo del centro es un nodo de red derivada. Normalmente, el CP adyacente (nodo de enlace superior de red derivada) será el servidor de nodos de red (NNS) para el nodo de red derivada, el cual se parece a un nodo final para el nodo de enlace superior de red derivada.

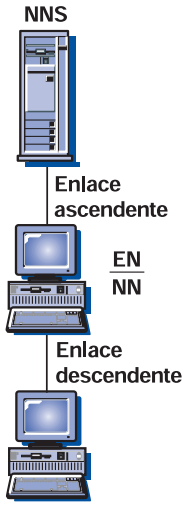


Figura 10. Visión general conceptual de enlaces superiores e inferiores de red derivada

Los enlaces superiores de derivación se definen en el nodo de red derivada como de sentido ascendente para la red principal. Puede considerarse que un nodo con un enlace superior está conectado periféricamente a la red principal.

Los enlaces inferiores de red derivada se definen desde el nodo de red derivada como de sentido descendente. El nodo ve los enlaces inferiores como conexiones con los nodos finales (puntos de control) del dominio. Normalmente, los enlaces inferiores de red derivada son enlaces de la LAN (pero no es necesario que lo sean). Puede considerarse que los nodos finales conectados a través de enlaces inferiores de red derivada son recursos locales. El nodo de red derivada es el servidor de nodos de red para estos nodos finales. En los enlaces inferiores de red derivada, proporciona los servicios de nodos de red para los nodos finales del dominio, los nodos finales LEN, los nodos T2.0 dependientes y nodos T2.1 y las LU y PU locales.

Un nodo de red derivada funciona como un servidor de nodos de red. Mantiene la información topológica acerca de todos sus nodos de enlace inferior de red derivada, pero no mantiene la información completa acerca de toda la red de enlaces superiores. Si la información que tiene el nodo no es suficiente, pasa as peticiones LOCATE a su servidor de nodos de red de enlace superior, que puede ser otro nodo de red derivada o un nodo de red APPN.

La red derivada optimiza el entorno de comunicación de igual a igual para los administradores que desean conectar redes derivadas basadas en la LAN a una gran WAN basada principalmente en una red conmutada. La red derivada mejora el rendimiento en las redes APPN grandes. Específicamente:

- Reduce el número de nodos de red en grandes redes APPN, permitiendo la adición de redes derivadas adicionales
- Oculta la información de topología de la red derivada
- Habilita la comunicación de igual a igual entre redes derivadas conectadas a la misma red de conexión APPN
- Permite la coexistencia con servidores de pasarela PU
- Reduce el tráfico de sesiones CP-CP de enlace superior (tráfico WAN)
- Aísla la red derivada de la actividad del tráfico WAN de la red principal

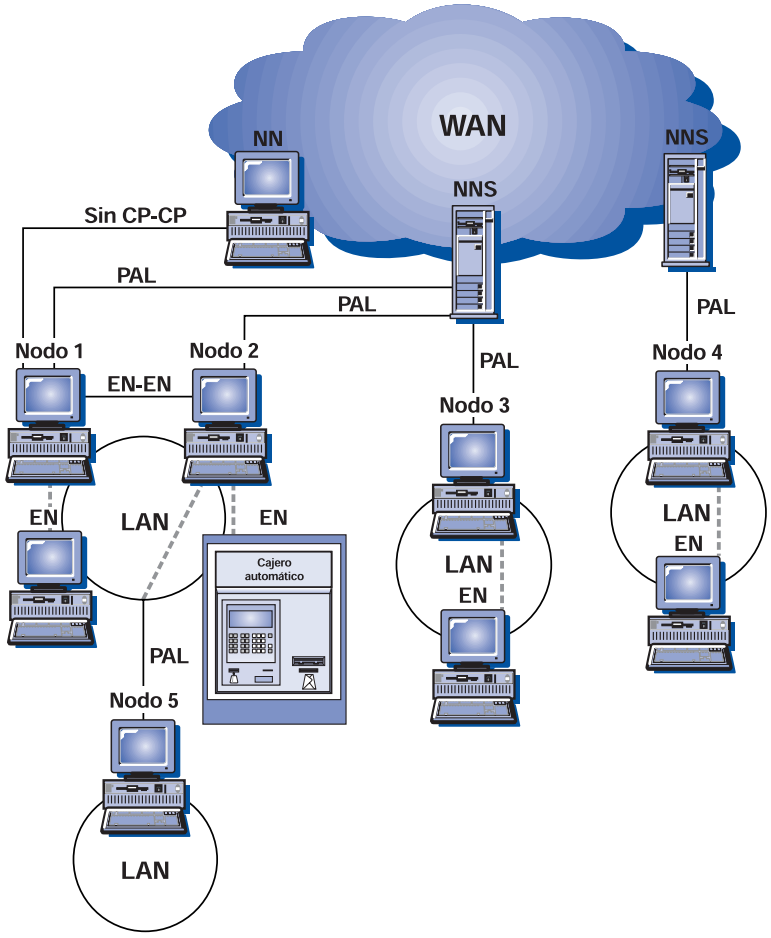


Figura 11. La red derivada en una red

La Figura 11 muestra cómo funcionan los nodos de red derivada en una red. Las líneas de guiones representan los enlaces lógicos. En la figura, los nodos 1, 2, 3 y 4 están configurados para dar soporte a la red derivada y funcionar como nodos finales y nodos de red. Ocultan su topología de enlace inferior a la red WAN (es decir, aparecen como nodos finales para los servidores de nodos de red en sentido ascendente). Para los nodos del sentido descendente de las LAN, los nodos funcionan como servidores de nodos de red. El Nodo 5 aparece como un nodo final para el Nodo 2, pero es un servidor de nodos de red (NNS) para otros nodos finales de su LAN. Para el NNS, el Nodo 5 aparece como una LU del Nodo 2.

Cuando un nodo final servido por el Nodo 1 intenta establecer una sesión con un nodo final a través de la WAN, el Nodo 1 puede enviar una petición Localizar (Enviar) en su enlace de red derivada a su servidor de nodos de red. Si se encuentra el CP de destino, el servidor de nodos de red determina una ruta desde el Nodo 1 al CP de destino. El Nodo 1 modificará la ruta antes de devolverlo al nodo final de origen. El nodo final de origen utiliza esta ruta para su sesión.

Restricciones de la red derivada

Las siguientes restricciones se aplican a las redes configuradas para utilizar la red derivada:

- Un nodo de red derivada sólo se puede conectar a un nodo de red mediante un enlace superior de red derivada.
- Para evitar una repetición en bucle de la búsqueda, los nodos finales de enlace inferior deben ser nodos finales reales, no nodos que presentan una imagen de nodo final.
- Un nodo no puede tener sesiones CP-CP con el nodo de red derivada a través de enlaces superiores de red derivada y enlaces inferiores de red derivada simultáneamente.
- El nodo de red derivada sólo puede tener sesiones CP-CP en un enlace superior de red derivada cada vez; es decir, puede tener sesiones CP-CP con un servidor de nodo de red como máximo.
- La red derivada no proporciona el soporte twinaxial.
- Un nodo de red derivada no puede tener sesiones DLUR en sentido descendente.

Configuración de la red derivada

Para configurar la red derivada, primero debe configurar un nodo de red derivada. Después debe configurar un DLC (para un enlace implícito) o un nodo de red derivada. Un enlace configurado para dar soporte a la red derivada es un enlace superior de red derivada. En un nodo de red derivada, cualquier enlace que no esté configurado para dar soporte a la característica es un enlace inferior de red derivada.

Si los nodos de red derivada tienen enlaces definidos entre ellos, deben estar definidos como conexiones ***similares***, que les dan un tipo de enlace de **LEARN** en el archivo ACG. Alternativamente, puede definirse el enlace como **ACTIVATE_AT_STARTUP=1** para que el enlace esté siempre activo. Cuando los nodos de red derivada se conectan entre sí, se producen bucles en la topología. Esto es aceptable mientras los enlaces estén siempre activados o que se conozcan los enlaces a medida que se activen. Si se definen los enlaces entre los nodos de red derivada como enlaces **END_NODE** o **NETWORK_NODE**, la topología informada en sentido ascendente puede interpretar los enlaces incorrectamente y provocar anomalías de asignación.

También puede utilizar un archivo ACG para configurar la red derivada.

Administración de la red derivada

Las siguientes secciones describen la forma de verificar una configuración y las restricciones de cómo configurar la red.

Verificación de la configuración: Puede utilizar **Operaciones de nodos SNA** en un nodo que da soporte a las redes derivadas para determinar si se ha configurado satisfactoriamente una red derivada local. En tiempo de ejecución, la visualización de la topología del nodo no debe tener nunca más de dos nodos de red, el mismo y el servidor de nodos de red de enlace superior.

Nota: Sólo está disponible un enlace superior para CP-CP. Cada estación de trabajo debe estar configurada como un nodo final con el nodo de red derivada definido como su servidor de nodos de red preferido.

Puede utilizar **Operaciones de nodos SNA** para verificar si el DLC o el enlace se ha configurado para dar soporte correctamente a la red derivada. También puede utilizar **Operaciones de nodos SNA** para determinar si un enlace activo es un enlace superior de red derivada o un enlace inferior de red derivada. Los nodos finales en sentido descendente registrados utilizando AnyNet no registrarán sus recursos.

Funciones soportadas

Communications Server da soporte a todas las funciones básicas de APPN Versión 2 (tanto nodo final como nodo de red). Además, se da soporte a las siguientes opciones:

- Nodo final

Función establecida	Opción
162	MS_CAPS Ser esfera de control (SOC) EN
171	Datos de diagnóstico de problemas en alerta
177	Alerta de LAN
178	Alerta de LLC SDLC/LAN
181	Alerta de X.25
182	Alerta retenida para CPMS
1002	Nombre de estación de enlace adyacente
1007	TG paralelos
1011	Múltiples LU independientes locales
1012	CP=LU
1018	Suprimir recursos EN antes de registro
1067	Peticionario de LU dependientes
1070	Criptografía de sesión
1107	Registro de recurso central (de LU)
1116	Registro de LU servidas por DLUS
1200	Poner en antememoria árbol y TG
1400	HPR base (ANR)
1401	Protocolo de transporte rápido
1402	Flujos de control sobre RTP
1520	Servicios de operaciones comunes

- Nodo de red

Función establecida	Opción
164	MS_CAPS Tener un punto focal de subárea
171	Datos de diagnóstico de problemas en alerta

177	Alerta de LAN
178	Alerta de LLC SDLC/LAN
181	Alerta de X.25
182	Alerta retenida para CPMS
1002	Nombre de estación de enlace adyacente
1007	TG paralelos
1011	Múltiples LU independientes locales
1012	CP=LU
1018	Suprimir recursos EN antes de registro
1067	Peticionario de LU dependientes
1070	Criptografía de sesión
1100	Almacenamiento protegido de antememoria de directorio
1101	Precarga de antememoria de directorio
1107	Registro de recurso central (de LU)
1116	Registro de LU servidas por DLUS
1118	Registro de vectores TG EN
1121	Función de red derivada
1200	Poner en antememoria árbol y TG
1203	Detección y eliminación de guerras de TDU
1301	Tráfico de sesión intermedia sin ritmo
1400	HPR base (ANR)
1401	Protocolo de transporte rápido
1402	Flujos de control sobre RTP
1520	Servicios de operaciones comunes

Control de enlace de datos (DLC)

El DLC proporciona los protocolos necesarios para la entrega fiable de las unidades de transmisión básicas (BTU) entre un par de nodos en la red APPN y el mantenimiento de las conexiones lógicas entre nodos.

Conexiones

Una conexión enlaza un par de nodos adyacentes a través del DLC básico.

Enlaces paralelos

El nodo local puede tener múltiples enlaces con un nodo adyacente. Se hace referencia a esta asociación como ***enlaces paralelos***. Se asigna un número exclusivo (número de grupo de transmisión) a cada enlace paralelo y pueden tener asignadas diferentes características de enlace. Para tener dos enlaces paralelos entre dos nodos, las estaciones de enlace para los enlaces pueden estar en un solo adaptador de un nodo pero deben estar en adaptadores separados en el otro

nodo; es decir, la combinación de número de adaptador y dirección de estación de enlace adyacente (o destino) debe ser exclusiva para cada enlace.

Activación de enlace

Se hace referencia a la unidad de mensaje que se utiliza para transportar las características del nodo y del enlace a un nodo adyacente como ***Identificación de intercambio*** (XID). Si **USE_PU_NAME_IN_XID=1**, se utiliza el nombre de PU en el campo de nombre de CP del XID. De lo contrario, se utiliza en nombre de punto de control en ese campo. Los XID se intercambian entre nodos antes y durante la activación del enlace para establecer y negociar las características del enlace y del nodo, y después de la activación del enlace para comunicar los cambios de estas características.

Los nodos APPN intercambian el XID de formato 3 (XID3) con otros nodos T2.1 o de límite para realizar la negociación de funciones. Para las conexiones PU 2.0, se utiliza la palabra clave **LINK_STATION** para especificar el nombre de PU y el ID de nodo que se intercambian en el XID3. Si **USE_PU_NAME_IN_XID=1**, se utiliza el nombre de PU en el campo de nombre del XID. De lo contrario, se utiliza en nombre de punto de control en ese campo. La información acerca de las características del nodo emisor están contenidas en el XID3, incluyendo la función de estación de enlace (primaria, secundaria o negociable), número de TG, tipo de nodo, número de enlace lógico, tamaño máximo de unidad básica de transmisión que puede recibirse, ID de nodo y nombre de PU. Normalmente, el nombre de PU es el nombre de punto de control, pero pueden especificarse un nombre de PU e ID de nodo alternativos en la palabra clave **LINK_STATION** para dar soporte a conexiones simultáneas de PU 2.0.

Tipos de enlace

Normalmente, se definen los seis tipos de enlace siguientes en los nodos de Communication Server:

- Acceso primario de red, activado inicialmente (APPN o sistema principal)
- Acceso primario de red, enlace con el sistema principal
- Acceso primario de red, en uso todo el tiempo (se utiliza cuando es necesario)
- Acceso secundario de red, enlace de entrada (características de enlace predefinidas)
- Acceso secundario de red, uso limitado (también se le hace referencia como enlace de recursos limitados)

La configuración de Communications Server proporciona una manera de definir y controlar la utilización de estos tipos de enlace. Esta sección describe los parámetros de configuración del nodo, DLC y enlace utilizados, así como las relaciones y dependencias que existen entre estos parámetros. Se describen las siguientes categorías:

- Parámetros de definición y de activación de enlace
- Parámetros de desactivación de enlace
- Otros parámetros de enlace

Se describen los parámetros siguientes:

- **Parámetros de definición y activación**
  - Activar en el arranque
  - Activar bajo pedido
  - Reintento automático de enlace
  - Número máximo de intentos de activación
  - Reactivación solicitada por el usuario
- **Parámetros de desactivación**
  - Tiempo de espera excedido de inactividad
  - Recurso limitado
- **Otros parámetros de enlace**
  - Red de conexión
  - Soporte de sesión CP-CP
  - Soporte de direccionamiento de alto rendimiento (HPR)
  - Tipo de nodo adyacente
  - Servidor de nodo de red preferido
  - Sesiones SSCP solicitadas
  - Nombre de PU (cuando las sesiones SSCP solicitadas son **1**)

Nota: Estos parámetros están en el archivo ACG y puede que no estén disponibles en los paneles (mediante **Configuración de nodos**).

Parámetros de definición y activación de enlace

Esta sección describe los parámetros de definición y de activación.

Activar en el arranque

Un enlace ***activar en el arranque*** se utiliza normalmente para los enlaces de acceso de red primarios que se activan inicialmente cuando se inicia Communications Server. El enlace se activa cuando se inicia Communications Server en la máquina y permanece activo mientras Communications Server esté en ejecución.

Para definir un enlace para que se active en el arranque, especifique **ACTIVATE_AT_STARTUP = 1** en la palabra clave **LINK_STATION** del archivo ACG. Generalmente, los enlaces se configuran para activarse en el arranque cuando son importantes para la conectividad de la red. Un enlace importante también se puede configurar para el reintento automático de enlace (consulte el apartado “Reintento automático de enlace” en la página 37).

El enlace de un nodo final APPN (EN) con su servidor de nodos de red (NN) preferido es un ejemplo de este tipo de enlace.

Son ejemplos de enlaces que no se activan en el arranque, codificados como **ACTIVATE_AT_STARTUP = 0**, un enlace con el sistema principal que no se necesita inmediatamente cuando se inicia Communications Server, un enlace de entrada cuyas características de enlace van a ser controladas por un nodo o un

enlace que sería muy costoso mantener activo todo el tiempo. Estos enlaces se definen como no activar en el arranque y se activan cuando una aplicación o el asociado piden recursos del enlace (consulte el apartado “Activar bajo petición” en la página 37).

Activar bajo petición

Normalmente, un enlace ***activar bajo petición*** (también se hace referencia como “activar automáticamente”) se utiliza para acceder a una LU asociada que necesita la activación dinámica del enlace. Cuando se inicia Communications Server, el enlace permanece inactivo. Sin embargo, se coloca en la topología como un enlace disponible si se especifica un nombre de CP adyacente. El enlace se activa cuando un programa de transacción (TP) pide una conexión con una LU remota que necesita que el enlace esté activo. Communications Server utiliza la LU asociada completamente calificada definida para activar el enlace.

Para definir un enlace como activar bajo petición, **ACTIVATE_AT_STARTUP = 0** y **FQ_ADJACENT_CP_NAME**=(idred.nombrecp) deben estar configurados en la palabra clave **LINK_STATION** del archivo ACG del nodo que lo origina. Si la asociada no es **FQ_ADJACENT_CP_NAME**, configure la palabra clave **PARTNER_LU**.

Con frecuencia, un enlace activar bajo petición también se configura como un recurso limitado (consulte el apartado “Recurso limitado” en la página 40) o con un tiempo de espera de inactividad (consulte el apartado “Tiempo de espera de inactividad” en la página 39) para que el enlace se desactive cuando ya no se necesite.

Un ejemplo de un enlace activar bajo petición es un enlace que define una conexión con un asociado que necesite estar activo durante un período de tiempo limitado. El enlace puede costar más de lo que se desea para mantenerlo activo siempre. Por ejemplo, puede tener un conjunto de uno o varios sistemas en comunicación normalmente. Al final de cada día, es necesario que una de las máquinas active un enlace con alguna máquina remota, para enviar los resultados del día, o para realizar una copia de seguridad de los datos.

Otro ejemplo puede ser cuando hay conexiones con un servidor de datos o con un servidor de impresión. La conexión necesita los recursos del servidor. Para evitar las limitaciones del número máximo de estaciones de enlace y de sesiones en el servidor, configure un enlace activar bajo petición para liberar los recursos en el servidor de datos una vez se hayan completado las peticiones del enlace activar bajo petición.

Un enlace activar bajo petición no es necesariamente un enlace de recurso limitado, pero puede definirse como uno incluyendo el parámetro **LIMITED_RESOURCE = 1** en la palabra clave **LINK_STATION** (consulte el apartado “Recurso limitado” en la página 40).

Reintento automático de enlace

El reintento automático de enlace es una función de recuperación de errores que mejora la disponibilidad de un enlace que ha fallado. Si es necesario reactivar un enlace (sin la intervención del usuario) después de una anomalía, puede utilizarse el reintento automático de enlace. El reintento automático de enlace provoca

intentos automáticos de reactivación del enlace si se han especificado los siguientes parámetros en las palabras clave **LINK_STATION** o **PORT**:

- **DELAY_APPLICATION_RETRIES**
- **RETRY_LINK_ON_DISCONNECT**
- **RETRY_LINK_ON_FAILED_START**
- **RETRY_LINK_ON_FAILURE**.

Si se ha especificado uno de estos parámetros en la palabra clave **PORT**, la palabra clave **LINK_STATION** utiliza los valores si se ha especificado el parámetro **INHERIT_PORT_RETRY_PARMS**.

Después de una activación satisfactoria, el temporizador de intervalos se restablece en 0.

Puede ser beneficioso utilizar el reintento automático de enlace en cualquiera de las siguientes clases de enlaces:

- Un enlace con un NN que se activa en el arranque. Si el enlace falla, sólo se reactivaría un enlace de servidor de nodos de red (NN).
- Enlace con el sistema principal
- El enlace primario que tiene una reserva (también se define normalmente como un enlace de activar en el arranque)
- Cualquier enlace que necesite permanecer activo siempre.

Número máximo de intentos de activación

Número máximo de intentos de activación es un parámetro de activación de enlace que proporciona un mecanismo para impedir que el tráfico de sistema principal de LU dependiente (por ejemplo, LUA, 3270, una pasarela LU 2 y/o DLUR que intenta activar un enlace con el sistema principal para una aplicación en sentido descendente) reintente indefinidamente la activación del enlace. El parámetro de número máximo de intentos de activación **INHERIT_PORT_RETRY_PARMS** representa las veces que se intenta una petición de activar enlace. Una vez alcanzado este número de intentos, se rechazan las peticiones posteriores hasta que se restablece el número de intentos. Las peticiones de activación de enlace de LU dependiente emitidas después de alcanzar el número máximo de intentos de activación se rechazan inmediatamente sin ningún intento real de activar el enlace. En este caso, se devuelve un código de retorno primario de X'0003' y un código secundario de X'00000005', un reintento DLC, con un código de detección de X'00000000'. Las peticiones de activación de enlace de LU independiente emitidas después de alcanzar el número máximo de intentos de activación se intentan, pero se devuelve junto con el código de retorno primario X'0003' y secundario X'00000005', un código de detección de 081C0001 para indicar que se ha alcanzado el límite máximo de intentos de activación.

Nota: Si un TP como, por ejemplo, una aplicación LUA, está en un bucle tratando de activar una sesión con el mismo sistema principal que la aplicación LU dependiente, el TP hace que se exceda el número máximo de intentos de activación antes de que la aplicación dependiente pueda realizar su primera petición.

El número máximo de intentos de activación se restablece de la manera siguiente:

- Cuando un TP independiente activa el enlace. Es responsabilidad de los TP comprobar el código de detección e implantar un protocolo razonable para que la activación del enlace no reintente infinitamente la activación.
- Cuando el usuario activa el enlace utilizando **Operaciones de nodos SNA**.
- Cuando se activa el enlace desde otra dirección (por ejemplo, por el asociado).

Si **Operaciones de nodos SNA** está tratando activar un enlace, el número máximo de intentos de activación disminuye en 1 y se pasa por alto el resultado. Si se ha excedido el límite en un enlace con el sistema principal de pasarela, la activación del enlace se intentará después de 30 minutos si se ha activado un enlace de estación de trabajo. Esto permite cesar los reintentos, aunque se reinician después, cuando se han reiniciado las estaciones de trabajo. Cuando la pasarela, LUA, u **Operaciones de nodos SNA**, activa satisfactoriamente un enlace, el número máximo de intentos de activación se establece en 0.

Para configurar el número máximo de intentos en un enlace, se configura el parámetro **MAX_ACTIVATION_ATTEMPTS**= n en la palabra clave **LINK_STATION**, donde n es el número de intentos de -1 a 127. Un -1 indica que debe utilizarse el valor de la palabra clave **PORT** y 0 indica reintentar infinitamente.

Reactivación solicitada por el usuario

Reactivación solicitada por el usuario es cuando el usuario pide que se reactive un enlace desde **Operaciones de nodos SNA** o desde la línea de mandatos utilizando, por ejemplo, Communications Server.

Parámetros de desactivación de enlace

Las siguientes secciones describen los parámetros de desactivación.

Tiempo de espera de inactividad

Tiempo de espera de inactividad es un parámetro de desactivación de enlace SDLC que controla cuándo se desactivan los enlaces. El valor de tiempo de espera de inactividad especifica el tiempo (en segundos) que el enlace puede estar desocupado antes de que se desactive. Es similar a **LINK_DEACT_TIMER** de la palabra clave **LINK_STATION**. La diferencia es que **LINK_DEACT_TIMER** espera que finalicen todas las sesiones (la cuenta de sesiones es 0) antes de desencadenar la desactivación del enlace. **INACTIVITY_TIMER** pasa por alto la cuenta de sesiones y activa la desactivación después de que el enlace haya estado desocupado durante el tiempo especificado.

La función de tiempo de espera de inactividad se ha implantado para manejar la situación en la que una sesión de emulador, LUA, 3270 o una conexión LEN, se deja activa por accidente durante largos períodos de tiempo. Cuando el nodo detecta que no hay actividad en este tipo de conexión durante el período de **INACTIVITY_TIMER**, el enlace se desactiva automáticamente, sin tener en cuenta si existen sesiones y conversaciones en el enlace. Por definición, **LINK_DEACT_TIMER** se considera que no interrumpe, pero **INACTIVITY_TIMER** se considera que interrumpe.

Notas:

1. El tiempo de espera de inactividad puede utilizarse en los enlaces de recurso limitado o en los enlaces de recurso no limitado. Si se define un enlace como de recurso limitado y las conversaciones permanecen activas, el tiempo de espera de recurso limitado no caducará y el enlace se desactivará cuando caduque el tiempo de espera de inactividad. Si un enlace se define como de recurso no limitado, el tiempo de espera de inactividad se utiliza para desactivar el enlace para liberar recursos en el extremo remoto.
2. Actualmente con HPR, se pasa por alto el tiempo de espera de inactividad. Esto es debido a que HPR no puede saber el tipo de tráfico que hay en el enlace y el protocolo de latencia HPR genera suficiente tráfico para que el enlace nunca esté desocupado.

Para configurar el tiempo de espera de inactividad de una conexión SDLC, se codifica el parámetro **INACTIVITY_TIMER**= n en el parámetro **LINK_STATION_SDLC_SPECIFIC_DATA** de la palabra clave **LINK_STATION** del archivo ACG, donde n es 40-160. Para configurar el tiempo de espera de inactividad de un enlace, se codifica el parámetro **LINK_DEACT_TIMER**= n en la palabra clave **LINK_STATION** del archivo ACG, donde n es 0—1 000. El 0 indica que no hay tiempo de espera (el enlace permanecerá siempre activo). El valor por omisión de SDLC es 80 y el valor por omisión del enlace es 10.

Recurso limitado

Un enlace de recurso limitado se utiliza normalmente para los enlaces de acceso de red primarios o secundarios de uso limitado. Un enlace de recurso limitado es el que se desactiva automáticamente cuando su cuenta de sesiones llega a 0. El enlace de recurso limitado puede definirse como **ACTIVATE_AT_STARTUP=1** o **ACTIVATE_AT_STARTUP=0**. Si el enlace es **ACTIVATE_AT_STARTUP=1**, se inicia al iniciar Communications Server. Si el enlace es **ACTIVATE_AT_STARTUP=0**, se coloca en la topología al iniciar Communications Server, si se especifica el nombre de CP adyacente, y se activa cuando se solicitan servicios.

Nota: Los enlaces de activar en el arranque no se colocan en la topología a menos que estén activos.

Para configurar un enlace de recurso limitado, se especifica **LIMITED_RESOURCE = 1** en la palabra clave **LINK_STATION** del archivo ACG. Se especifica **LINK_DEACT_TIMER**= n en la palabra clave **LINK_STATION** y debe especificarse en el parámetro **ADJACENT_NODE_TYPE=LEARN**.

Nota: Si **CP_CP_SESSION_SUPPORT=1**, el enlace no es un enlace de recurso limitado. La verificación de la configuración indicará esto como un aviso. Las sesiones CP-CP activas impedirán que se desactive el enlace.

Redes de conexión

Las redes de conexión permiten que los nodos APPN de una LAN tengan enlaces directos entre sí sin necesitar definiciones de enlaces lógicos en cada nodo. Esta característica reduce grandemente la definición del sistema sin añadir al rendimiento la carga de direccionar todas las sesiones a través de un nodo. También permite que los nodos nuevos que se han añadido a la LAN participen completamente en conversaciones APPC sin necesidad de cambiar la definición en cada nodo alternativo.

Un nodo de red de la red de conexión supone que todos los nodos de una red de conexión pueden tener enlaces directamente entre sí. Cuando se calcula la ruta para una sesión, el nodo de red toma en consideración el enlace directo y selecciona normalmente el enlace directo como la ruta óptima. Una vez calculada la ruta directa, el nodo de red envía simplemente al nodo final la dirección del asociado que se ha de utilizar para activar el enlace.

Es posible que no se tome la ruta de red de conexión cuando la seguridad de la red de conexión sea menor que la necesaria. Si el DLC de red de conexión no es seguro y se utiliza una modalidad como #BATCHSC en el parámetro **MODE_NAME**, el nodo de red intenta encontrar una ruta segura, haciendo caso omiso de la red de conexión.

Si se están utilizando puentes de la LAN, APPN ve toda la red puenteada como una sola red lógica. Como se pueden activar los enlaces entre dos sistemas cualquiera de la LAN, sólo es necesaria una red de conexión. La red de conexión debe definirse en todos los sistemas APPN de la LAN.

Un nodo de red conoce la información de red de conexión durante el registro EN y las búsquedas de directorio APPN. Entonces, el servidor de nodos de red tiene suficiente información para calcular la conexión directa entre los nodos de punto final de sesión sin direccionamiento a través de nodos intermedios.

Sólo los nodos finales y los nodos de red pueden aprovechar las ventajas de la red de conexión; los enlaces con nodos LEN deben seguir definiéndose explícitamente.

La Figura 12 ilustra un ejemplo de red de conexión. Esta vista de una LAN muestra una red de conexión con el nombre de LOCALNET.IBMLAN. Con este tipo de definición, cualquier EN puede conectarse directamente a cualquier otro EN siempre que NN1 sea el servidor de nodos de red activo para todos los nodos finales.

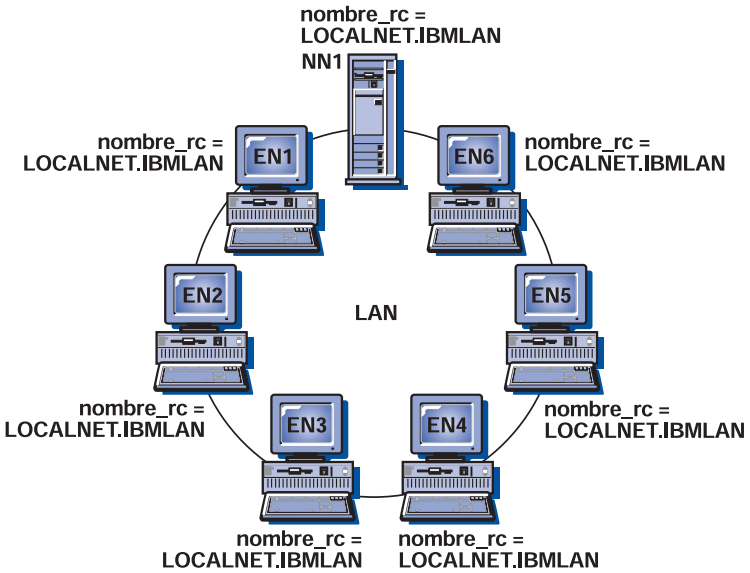


Figura 12. Un ejemplo de red de conexión

Otros parámetros de enlace

Otros parámetros de la palabra clave **LINK_STATION** que se mencionan en las secciones precedentes, pero que pueden definirse obvia ni implícitamente son:

- Tipo de nodo adyacente
- Servidor de nodo de red preferido
- Sesiones SSCP solicitadas

Esta sección contiene una breve definición de cada uno de ellos.

Tipo de nodo adyacente

El tipo de nodo adyacente especifica el tipo de nodo que es adyacente al nodo que define el enlace. Los tipos válidos son:

- DSPU_NOXID
- DSPU_XID
- END_NODE
- HOST_DEP_LU_ONLY
- HOST_XID0
- LEARN
- NETWORK_NODE.
- SUBAREA_LEN

Consulte el manual *Configuration File Reference* para obtener más detalles.

Servidor de nodo de red preferido

El servidor de nodo de red preferido especifica si el nodo de red adyacente se ha de utilizar como servidor de nodos de red en el enlace que se define.

Sesiones SSCP solicitadas

Las sesiones SSCP solicitadas especifica si se piden sesiones SSCP-PU desde el sistema principal en el enlace que se define.

Servicios del directorio

Un nodo de red proporciona los servicios del directorio a las LU ubicadas en el nodo de red y a las LU de los nodos finales que el nodo de red sirve. El nodo de red también ayuda en los servicios del directorio proporcionados por otros nodos de red de la red respondiendo positivamente a las peticiones de búsqueda de directorio recibidas cuando el recurso nombrado se encuentra en el directorio local. El directorio local correlaciona un nombre de LU con el nombre de punto de control del nodo en el que está ubicada la LU. Si el punto de control de destino es un LEN o un nodo final, el directorio incluye el nombre del nodo de red de servicio.

El componente de servicios del directorio reside en cada nodo; sin embargo, su ámbito y sus funciones varían según el nivel de soporte del directorio en el nodo.

Un nodo final mantiene un directorio local que contiene entradas para las LU que residen localmente. Además, el nodo final mantiene las entradas de directorio para las LU de nodos adyacentes con las que el nodo final ha mantenido una sesión. En el caso de una sesión LU-LU con un nodo similar adyacente, una búsqueda en el directorio local devuelve el punto de control de destino adecuado asociado con la LU que se busca, permitiendo seleccionar el enlace lógico adecuado.

En un nodo LEN, se entran en el directorio todas las LU asociadas, como muestra el ejemplo de la Figura 13. Las que no están en un nodo final similar adyacente sino fuera, en la red APPN, se asocian en su directorio con su servidor de nodos de red designado. El nodo LEN envía una petición de activación (BIND) de sesión LU-LU a su servidor de nodos de red para cualquier LU asociada en su directorio con su servidor; el servidor localiza automáticamente la LU de destino para la misma y reenvía BIND correctamente. El nodo de red puede enviar una búsqueda Localizar, esperar una respuesta y, a continuación, enviar BIND.

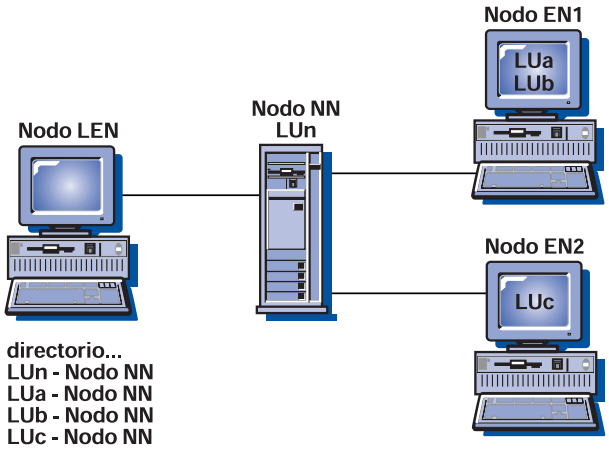


Figura 13. Directorio de nodo LEN. El directorio de nodo LEN debe contener todas las LU con el que se comunica. Puesto que el nodo de red (NN) adyacente sirve al nodo LEN incluso sin sesiones CP-CP, el nodo LEN debe definir el punto de control del nodo de red como el "punto de control propietario" de todas las LU, incluso las LU ubicadas en los nodos finales (EN).

Cuando una LU no está representada en un directorio de nodo final, el nodo final inicia una búsqueda Localizar para buscar la LU deseada. Para activar la búsqueda, el nodo final invoca los servicios de su servidor de nodos de red. La Figura 14 en la página 44 muestra un ejemplo de un directorio de nodo final.

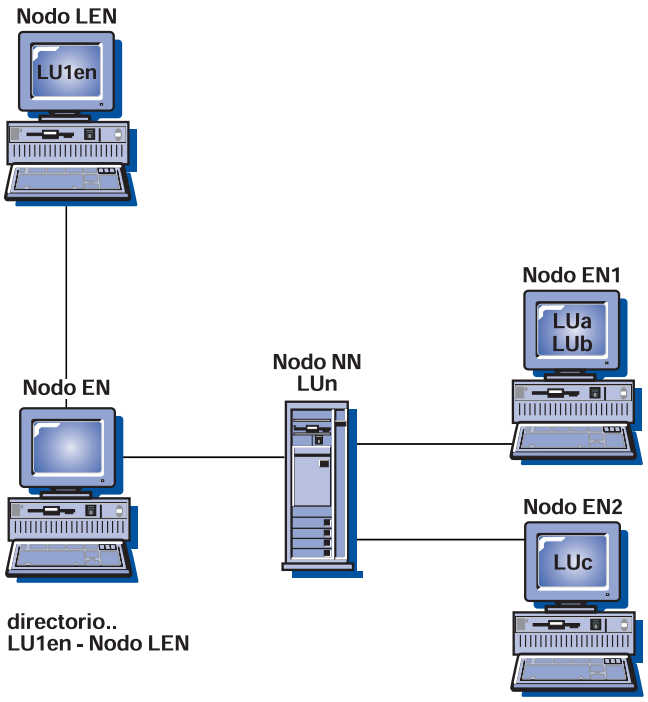


Figura 14. Directorio de nodo final. El nodo final (EN) utiliza los servicios de su servidor de nodos de red para buscar la ubicación de las LU. Ninguna de las LU de la red APPN necesita estar definida en el nodo final. Sin embargo, la LU de nodo LEN adyacente debe estar definida porque no está conectada al nodo de red y no forma parte de la red APPN.

Un nodo de red proporciona servicios del directorio distribuidos a sus nodos finales servidos en cooperación con todos los demás nodos de red de la red APPN. El nodo de red de origen recibe el nombre de una LU de destino en una petición de búsqueda Localizar desde un nodo final servido o el nombre de una LU secundaria de un BIND desde un nodo LEN. El nodo de red verifica la ubicación actual de la LU si está representada en el directorio del nodo de red (pero no es el nodo de red en sí). La verificación se realiza enviando una búsqueda dirigida al servidor de nodos de red de destino.

Si la LU no está en el directorio del nodo de red de origen, el nodo de red inicia una búsqueda en la red. La búsqueda se inicia enviando una búsqueda generalizada a cada nodo de red adyacente, cada uno de los cuales propaga a su vez la búsqueda y devuelve las respuestas indicando el éxito o el fracaso. Para necesidades futuras, el nodo de red pone en antememoria la información obtenida de las búsquedas generalizadas satisfactorias.

Un nodo final APPN también puede recibir (y responder a) las peticiones de búsqueda Localizar de su servidor de nodos de red para buscar, o asegurar la presencia continuada de, LU específicas en el nodo final.

Cada nodo final puede registrar sus LU con su servidor nodo de red enviando al nodo de red un mensaje de registro. Si el nodo final está registrado en el servidor de nodo de red, el nodo de red mantiene la información del directorio actual perteneciente a los nodos finales de su dominio.

La Figura 15 en la página 45 muestra un ejemplo de directorio de nodo de red.

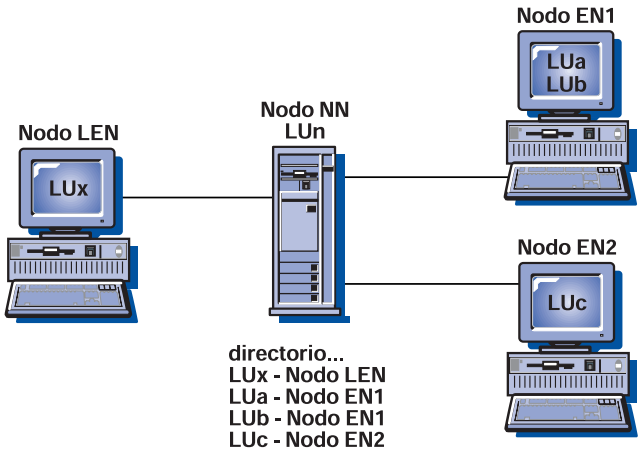


Figura 15. Directorio de nodo de red. El directorio de nodo de red (NN) contiene todas las LU a las que sirve. Los nodos finales (EN) registran sus LU; la LU de nodo LEN debe configurarse.

Topología y servicios de selección de ruta

Un nodo de red proporciona los servicios de selección de ruta para sí mismo y para los nodos finales a los que sirve. Mantiene una base de datos interna de topología de la red que contiene toda la información actual de topología acerca de la red. Esta información de topología consiste en las características de todos los nodos de red de la red y de todos los enlaces entre nodos de red. Todos los nodos de red contienen una copia de la base de datos de topología.

Un nodo de red utiliza la base de datos de topología de red para calcular las rutas para las sesiones que se originan en las LU que contiene y los nodos finales a los que sirve. Cada ruta que un nodo de red calcula es la ruta actual con el menor peso desde el nodo que contiene la LU de origen al nodo que contiene la LU de destino. Para proporcionar una vía de acceso adecuada a través de la red, primero el algoritmo utilizado para seleccionar la ruta asigna pesos a los enlaces y nodos. Basándose en el significado relativo de las características de la clase de servicio solicitado, el algoritmo de peso calcula un valor escalar para cada nodo y enlace lógico.

Base de datos de topología

La base de datos de topología de la red de un nodo de red contiene información acerca de todos los nodos de red y de todos los grupos de transmisión que los interconectan. Es una base de datos completamente duplicada que se comparte entre todos los nodos de red de la red y se utiliza para la selección de la ruta. El mantenimiento de la base de datos necesita actualizaciones generalizadas de todos los nodos de red. Las actualizaciones se llevan a cabo a través de los mensajes de actualización de base de datos de topología (TDU), que contienen la información de identificación de nodo, las características del nodo y del enlace y los números de secuencia de actualización para identificar los cambios más recientes para cada recurso descrito en una TDU.

Una base de datos de topología local de un nodo final contiene información acerca de sí mismo y de los nodos directamente conectados solamente.

El componente de topología y servicios de direccionamiento utiliza las sesiones CP-CP entre los nodos de red para intercambiar información para crear y mantener una base de datos de topología. Esta base de datos de topología de los nodos de red se mantiene actualizada utilizando las actualizaciones que se transmiten entre todos los nodos de red siempre que se activa o desactiva un recurso (nodo o enlace) o que cambian las características de un recurso existente.

Se mantiene una base de datos de configuración local y una base de datos de topología de red en cada nodo de red tal como se ilustra en la Figura 16 en la página 47. La base de datos de configuración local es exclusiva para el nodo, mientras que la base de datos de topología de red se reproduce en todos los nodos de red.

La Tabla 2 muestra la información contenida en la base de datos de configuración en el nodo de red local.

Tabla 2. Base de datos de configuración de NN local

Nodo	Enlaces	Conexión
NN5	e	NN5—EN1
	a	NN5—NN7
	b	NN5—NN6
NN7	a	NN7—NN5
	d	NN7—NN8
NN6	b	NN6—NN5
	f	NN6—EN2
	c	NN6—NN8
	g	NN6—EN3
NN8	c	NN8—NN6
	d	NN8—NN7
	j	NN8—EN3
	h	NN8—EN4

La Tabla 3 muestra la información contenida en la base de datos de topología de red en el nodo de red local.

Tabla 3. Base de datos de topología de red de NN local

Nodo	Enlaces	Conexión
NN5, NN6, NN7, NN8	a	NN5—NN7
	a	NN7—NN5
	b	NN5—NN6
	b	NN6—NN5
	c	NN6—NN8
	c	NN8—NN6
	d	NN7—NN8
	d	NN8—NN7

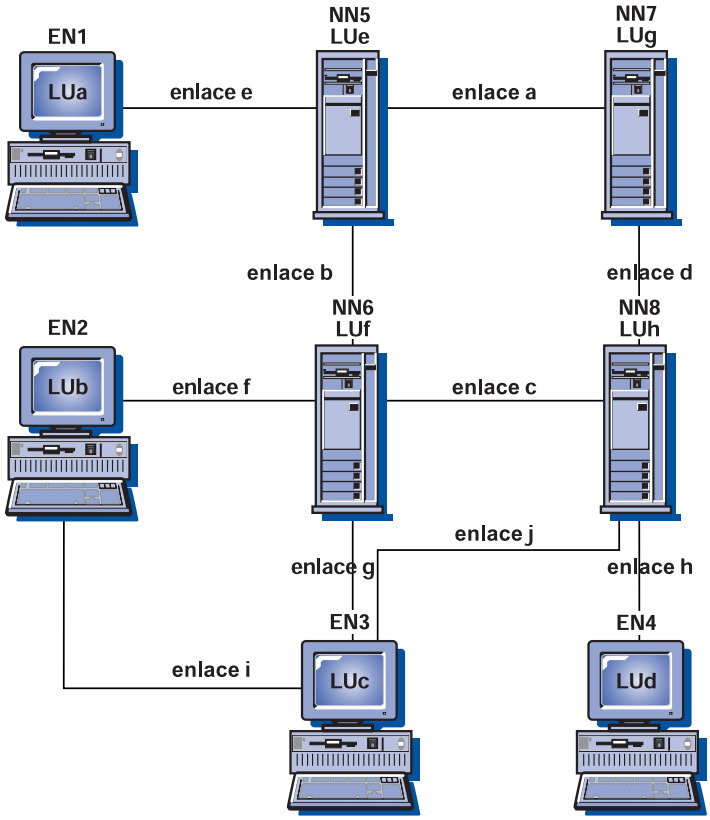


Figura 16. Base de datos de configuración local y base de datos de topología de red en nodos de red

Modalidades

La modalidad determina los valores para las características de la sesión y el número de sesiones entre asociados de sesión. Por ejemplo, el tamaño de la unidad de petición (RU) más grande que se va a intercambiar en una sesión (es decir, el ***tamaño máximo de RU***) es una de las características de la modalidad. La modalidad especifica también una clase de servicio, que se utiliza para seleccionar la ruta para la sesión.

Clase de servicio

En el momento de inicio de sesión, BIND especifica un nombre de modalidad. Este nombre de modalidad se asocia con una definición de clase de servicio (COS) que se utiliza para determinar la ruta más conveniente entre los nodos de origen y de destino de la sesión. Las definiciones de COS especifican las características que poseen los nodos y enlaces que se han de incluir en la ruta seleccionada para la sesión. Esta especificación permite que el algoritmo de selección de ruta determine si un nodo o un enlace es aceptable. Cuando es aceptable, el algoritmo calcula la ruta mejor para la sesión.

Puesto que las definiciones de COS pueden variar, diferentes sesiones pueden utilizar distintas rutas entre los mismos nodos de origen y de destino, según el nombre de modalidad especificado. Cada nodo de red es capaz de calcular la ruta de menos peso (la más deseable) para cualquier destino.

Cuando una sesión pasa por una red APPN y una red de subárea, utiliza dos clases de servicio:

- En la red APPN, la sesión utiliza la clase de servicio (COS) definida para la modalidad utilizada por el programa de transacción. Esta definición está en la configuración activa de la estación de trabajo. Esta COS se utiliza para direccionar la sesión en la red APPN.

  Si utiliza la modalidad en blanco por omisión, la COS asociada es #CONNECT.

- En la red de subárea, el nombre de la COS puede grabarse en la tabla de modalidades de conexión, en la entrada para el nombre de modalidad utilizada por la sesión. El programa VTAM utiliza este nombre de COS para direccionar la sesión a través de la red de subárea.

  Si se utiliza la modalidad en blanco por omisión o si no se define ninguna COS en una entrada de la tabla de modalidades de conexión, la COS toma por omisión la entrada en blanco en la tabla ISTSDCOS.

En ambos casos, cada red utiliza el nombre de modalidad para buscar el nombre de COS, pero los dos nombres de COS no son necesariamente el mismo.

Prioridad de transmisión SNA

La prioridad de transmisión es un valor especificado en la clase de servicio. La prioridad de transmisión se envía en la petición BIND en el vector de control Clase de servicio/Prioridad de transmisión (COS/TPF). Una vez establecida la sesión, los datos de sesión posteriores fluyen con la prioridad de transmisión especificada en el vector de control COS/TPF.

Los datos que fluyen en sesiones que utilizan una clase de servicio con una alta prioridad pueden pasar a los datos de las sesiones con una prioridad inferior. Debe dar una prioridad alta a las sesiones que transportan tráfico interactivo en las que el tiempo de respuesta es importante, por ejemplo, sesiones de emulador. Las sesiones que transportan grandes volúmenes de datos, por ejemplo, transferencias de archivos para NetView Distribution Manager, deben tener una prioridad inferior. El soporte de prioridad de transmisión ayuda a evitar que las sesiones con grandes volúmenes bloquee el tráfico de las sesiones interactivas.

Las cuatro prioridades de transmisión son red, alta, media y baja. La prioridad de red se utiliza para los datos de control de red como, por ejemplo, la topología y los servicios del directorio. Las demás prioridades se utilizan para los datos del usuario.

Communications Server da soporte a la prioridad de transmisión para los enlaces LAN, SDLC y X.25. El beneficio es más aparente cuando la red contiene enlaces de baja velocidad congestionados.

Selección de ruta

Después de que servidor de nodos de red reciba una respuesta de su búsqueda Localizar, el componente de topología y servicios de direccionamiento calcula la ruta mejor desde el nodo de origen al nodo de destino para la COS pedida. Puesto que el componente topología y servicios de direccionamiento envía y recibe actualizaciones de la base de datos de topología como características de cualquier cambio de recurso, cada ruta se calcula con la información más reciente.

Selección de ruta para usuarios VTAM

Para direccionar el tráfico APPC a través de una subárea, las estaciones de trabajo conectadas a la subárea deben estar definidas como nodos de red en Communications Server. En cada nodo de red, se define un enlace que conecta el nodo con la subárea. Desde el punto de vista del nodo de red, las LU asociadas del otro lado de la subárea están definidas como ubicadas en el sistema principal (un nodo LEN). Desde el punto de vista del sistema principal, cada nodo de red conectado a la subárea debe definirse en el programa VTAM con una macro PU. Todas las unidades lógicas LU 6.2 de destino de la red APPN para una conexión en particular se definen en la PU (nodo de red) como si estuviesen ubicadas realmente en la PU. Sin embargo, las LU pueden localizarse realmente en otros nodos de la red APPN conectada al nodo de red. El sistema principal sólo ve la PU de nodo de red. La PU de nodo de red también puede ser una PU pasarela. No se permite el tráfico SETN (**CP_CP_SESS_SUPPORT=NO**) cuando el parámetro se establece en YES en el NCP y no hay ninguna sesión de PU ni de punto de control.

Si el nombre de PU de la definición VTAM es el mismo que el nombre de punto de control definido en Communications Server, tenga en cuenta que no podrá definir el punto de control como una LU en las definiciones VTAM. Los nombres deben ser exclusivos en el programa VTAM, ya sean nombres de PU o de LU.

La macro PU debe contener **XID=YES** para utilizar un intercambio de XID durante la activación de la PU. Este parámetro se codifica en el nodo principal NCP. No debe estar en la sentencia PU de un nodo principal conmutado.

En el caso de dispositivos SNA conmutados, puede utilizar un nuevo parámetro en la macro PU: **CPNAME**=cccccccc. Especifica el nombre de punto de control del nodo de red conectado a la subárea. Debe especificarse **CPNAME** o **IDBLK** e **IDNUM** en una sentencia de definición de PU conmutada. Pueden especificarse ambos. El nodo de red proporciona su nombre de punto de control al programa VTAM en el intercambio de XID durante la secuencia de conexión. El programa VTAM utiliza el nombre de punto de control para localizar la macro PU correspondiente. Si no hay ninguna macro PU con el nombre de punto de control correspondiente, el programa VTAM utiliza **IDNUM** e **IDBLK** para localizar la macro PU.

Para direccionar el tráfico APPC en una red APPN a través de la subárea y hacia otra porción de la red APPN, el nombre de red (**NETID**) del VTAM propietario debe coincidir con el ID de red de la red APPN. En Communications Server, el ID de red (del nodo de red conectado a la subárea) se puede buscar utilizando el perfil de características de nodo local SNA.

Direccionamiento de sesiones intermedias

El direccionamiento de sesiones intermedias es una función realizada por un nodo de red. Esta posibilidad permite que un nodo de red reciba y direccione los datos destinados a otro nodo. El origen y destino de los datos puede ser un nodo final, un nodo de red o un nodo LEN. El fragmento de sesión entre dos nodos adyacentes se denomina una etapa de sesión.

Soporte de direccionamiento de alto rendimiento (HPR)

Communications Server da soporte a conexiones de direccionamiento de alto rendimiento (HPR) sobre Enterprise Extender (IP), control síncrono de enlace de datos (SDLC), LAN, WAN, canal, Canal de múltiples vías (MPC) y X.25.

El direccionamiento automático de red (ANR) HPR minimiza los requisitos de almacenamiento y proceso de los nodos intermedios, lo que es una solución mejor que el direccionamiento de sesiones intermedias (ISR) de APPN para redes de alta velocidad con proporciones de error bajas.

HPR mejora el direccionamiento SNA con estas características principales:

- Nodos intermedios sin estado

  Los nodos intermedios sin estado no tienen conocimiento de las conexiones que pasan a través de ellos.

  Un nodo intermedio HPR no necesita ningún bloque de control ni agrupaciones de almacenamientos intermedios para dar soporte a las conexiones que pasan a través suyo. Tampoco necesita tablas de direccionamiento porque la información de direccionamiento se transporta en cada paquete. Mediante la utilización de ANR, un nodo intermedio HPR simplemente recibe un paquete, examina la cabecera del paquete para buscar un identificador para el enlace lógico con el siguiente nodo y envía el paquete en ese enlace.

- Un nodo intermedio HPR:
  - No recupera los paquetes porque los puntos finales de conexión HPR detectarán y recuperarán los paquetes perdidos utilizando el protocolo de transporte rápido (RTP).

    Si la LAN tiene altas proporciones de error, también puede elegir el soporte de protocolo de recuperación de errores (ERP) a nivel de enlace. Sin embargo, no es necesario en enlaces con bajas proporciones de error.
  - No vuelve a ensamblar los paquetes segmentados y después a segmentarlos porque los puntos finales de conexión HPR elegirán automáticamente un tamaño de paquete soportado por todos los nodos intermedios de la ruta.
  - No gestiona activamente los almacenes intermedios ni evita la congestión porque los puntos finales de conexión HPR emplean algoritmos de control de flujo que evitan la congestión en los nodos intermedios.
  - No determina la ruta del paquete realizando una búsqueda en la tabla porque los puntos finales de conexión HPR efectúan el direccionamiento de origen, y crean la información de direccionamiento del paquete utilizando las etiquetas elegidas para el rendimiento óptimo por cada nodo intermedio.

  Para conseguir nodos intermedios sin estado:
  - Los puntos finales de la ruta deben tener posibilidades de almacenamiento intermedio que reflejen la combinación del retardo de ruta y productividad de la aplicación, un valor que depende de la configuración de la red.
  - Los enlaces de datos deben soportar tamaños de campos I lo suficientemente grandes para contener cabeceras HPR y seguir transportando datos de aplicación eficazmente.

  - Los enlaces de datos deben ser muy fiables porque una alta proporción de errores afectará negativamente a la productividad HPR.

  En el caso de configuraciones en las que no se pueden satisfacer estas condiciones, APPN sin HPR sigue siendo una opción de implantación válida. La tecnología HPR es una opción APPN y todavía está disponible y se da soporte a APPN sin HPR.

- Evitación de la congestión

  Una red HPR puede alcanzar utilizaciones de enlace muy altas. Mediante la utilización de la técnica denominada control de flujo basado en velocidad automática (ARB), los puntos finales de conexión HPR detectan automáticamente la congestión de la red y reducen la carga de transmisión. Esto evita la pérdida de paquetes que, en otros algoritmos de direccionamiento, pueden estar causados por la falta de almacenamientos intermedios disponibles en nodos intermedios.

- Redireccionamiento automático sin interrupción

  Cuando un punto final de conexión HPR detecta que una ruta ha fallado, calcula automáticamente una nueva ruta, restablece la conexión y recupera cualquier paquete perdido debido a la anomalía. Puesto que los nodos intermedios HPR no tienen estado (es decir, no tienen conocimiento de las conexiones que pasan a través suyo), no participan en este protocolo de recuperación. Puesto que no se pierde ningún paquete si la ruta se conmuta satisfactoriamente, la anomalía no interrumpe las aplicaciones que utilizan la ruta.

- Software compatible con el hardware existente

  HPR es una extensión del software de APPN; puede utilizar HPR en los adaptadores de LAN o WAN existentes y los enlaces de frame relay. Puesto que HPR no intenta proporcionar un ancho de banda dedicado ni un transporte en tiempo real garantizado (deja este nivel de función a los Servicios de red de banda amplia), las restricciones del rendimiento en los retardos de reenvío de paquetes son los mismos que para APPN sin HPR. Los protocolos de punto de control que utiliza HPR son los de APPN básico con pequeñas adiciones, para que los nodos HPR puedan instalarse, incrementándolos, en una red APPN existente sin una coordinación ni planificación previa.

Protocolo de transporte rápido (RTP)

RTP es un conjunto de formatos de mensajes y protocolos diseñado para utilizar los medios de comunicación de datos modernos, minimizar los gastos generales de los nodos intermedios y conmutar automáticamente las vías de acceso cuando falla un enlace de la vía de acceso.

Las conexiones RTP se establecen en una ***subred HPR*** y se utilizan para transportar el tráfico de la sesión. Una subred HPR es la parte de una red APPN que es capaz de establecer conexiones RTP y de transportar tráfico de sesiones HPR. Puede decirse que las conexiones RTP son ***conductos de transporte*** en los que se transportan sesiones. Estas conexiones pueden transportar datos a muy altas velocidades, utilizando el direccionamiento intermedio de nivel inferior, y minimizar el tráfico de los enlaces para la recuperación de errores y el control de flujo. Estos flujos los gestionan los puntos finales de conexión RTP.

La vía de acceso física de una conexión RTP puede conmutarse automáticamente para redireccionar los datos ordenado un nodo o un enlace que ha fallado, sin inte-

rrumpir las sesiones. Los datos de la red en el momento de la anomalía se recuperan automáticamente.

RTP efectúa la recuperación de errores basándose en un sistema de extremo a extremo, en lugar de basarse en el nivel de enlace. El rendimiento se mejora reduciendo el número de flujos necesarios para realizar la recuperación de errores. También se da soporte a los protocolos de recuperación de errores a nivel de enlace (ERP) para todas las conexiones. ERP es un método de detectar un paquete perdido en un extremo de un enlace y de recuperarlo pidiendo al otro extremo del enlace que retransmita el paquete. Si se utiliza ERP, los paquetes HPR se envían como tramas de información numeradas (I-FRAMES). Cuando se pierde una trama, el DLC detecta la pérdida y el remitente retransmite la trama. Si no se utiliza ERP, los paquetes HPR se envían como tramas de información no numeradas (UI-FRAMES). Cuando se pierde una trama, el DLC no puede detectar la pérdida y el protocolo de transporte rápido (RTP) de HPR debe detectar y recuperar los paquetes perdidos en los puntos finales de la conexión.

En cualquier caso, RTP detecta siempre y recupera los paquetes perdidos en los puntos finales de conexión. Para una conexión determinada, no hay restricciones en el número de enlaces que utilizan ERP o que no lo utilizan.

ERP puede habilitarse o inhabilitarse en cada enlace. Puesto que RTP detecta y recupera los paquetes perdidos en los puntos finales de conexión, pueden utilizarse enlaces ERP o enlaces que no son ERP cuando se construye la red. Esto le permite especificar ERP a nivel de enlace en los enlaces que tienen una alta proporción de pérdida de paquetes y maximizar la productividad en otros enlaces especificando que no utilicen ERP a nivel de enlace. En general, no se recomienda la utilización de ERP en las LAN.

Nota: ERP está siempre habilitado en un entorno de red de área amplia (WAN).

RTP también realiza el control de flujo y el control de congestión de extremo a extremo. RTP utiliza una técnica llamada control de flujo basado en velocidad automática (ARB) para utilizar toda la anchura de banda de la red cuando sea posible. RTP aumenta la velocidad a la que se envían los paquetes cuando la red soporta este aumento de velocidad de envío. La congestión se reconoce automáticamente y la velocidad de envío se reducirá según ella cuando se produzca la congestión. Las posibilidades efectivas de enlaces configuradas de la vía de acceso de conexión se utilizan para determinar tanto la velocidad de envío inicial como el aumento de velocidad de envío.

El soporte para los flujos de control (CF) sobre conexiones RTP está ahora disponible con HPR en Communications Server. Anteriormente, los flujos de control, incluyendo sesiones CP-CP y mensajes de definición de rutas, utilizaban las conexiones APPN mientras que los flujos de datos utilizaban las conexiones HPR. Ahora tanto los flujos de control como los flujos de datos pueden utilizar las conexiones RTP. Los beneficios de este soporte incluyen la conmutación automática de vías de acceso para sesiones CP-CP.

Los flujos de control fluyen automáticamente sobre RTP si ambos puntos finales de la conexión dan soporte a esta función.

Direccionamiento automático de red (ANR)

El Direccionamiento automático de red (ANR) es una técnica de direccionamiento sin estado que RTP habilita, en el que un mensaje llega con una etiqueta que identifica exclusivamente el siguiente salto en la vía de acceso. Debido a su simplicidad, el ANR puede llevarse a cabo en un nivel bajo, sin conocer las conexiones que utilizan la vía de acceso. ANR minimiza los ciclos y los requisitos de almacenamiento para los paquetes de direccionamiento a través de nodos intermedios.

La función de conmutación rápida de paquetes ANR mejora el rendimiento en los nodos intermedios direccionando a un nivel inferior que APPN y realizando una recuperación de errores, segmentación, control de flujo y control de congestión en el nodo final, en lugar de hacerlo en el nodo intermedio.

Los nodos ANR intermedios no conocen las sesiones SNA ni las conexiones RTP. La información de direccionamiento de cada paquete se transporta en una cabecera de red con el paquete. Cada nodo elimina la información que ha utilizado de la cabecera antes de reenviar el paquete, de modo que el siguiente nodo puede encontrar su información de direccionamiento en un lugar fijo de la cabecera. No hay necesidad de guardar las tablas de direccionamiento para los conectores de sesión como en el APPN base, de modo que la conmutación de paquetes a través de los nodos puede realizarse más rápidamente.

Soporte de LU

SNA define las LU de tipo 0, 1, 2, 3, 4, 6.0, 6.1, 6.2 y 7. Las LU de tipo 0, 1, 2, 3, 4 y 7 dan soporte a las comunicaciones entre los programas de aplicación y las distintas clases de estaciones de trabajo. Las LU de tipo 6.0 y 6.1 proporcionan comunicaciones entre los programas ubicados en los nodos de subárea de tipo 5. La LU de tipo 6.2 da soporte a las comunicaciones entre dos programas ubicados en los nodos de subárea de tipo 5 o en los nodos periféricos de tipo 2.1, o en ambos, y entre programas y dispositivos.

Communications Server da soporte a las LU de tipo 0, 1, 2 y 3, que dan soporte a comunicaciones con aplicaciones del sistema principal que dan soporte a dispositivos como, por ejemplo:

LU tipo 0 Terminales financieras 3650 y 4700

LU tipo 1 Impresoras 3270

LU tipo 2 Monitores interactivos 3270

LU tipo 3 Impresoras 3270

La comunicación sólo se produce entre las LU del mismo tipo. Por ejemplo, una LU 2 se comunica con otra LU 2; no se comunica con ninguna LU 3. Communications Server también da soporte a las LU de tipo 6.2 o APPC.

Las funciones SNA de Communications Server permiten que las aplicaciones utilicen la interfaz de programación de aplicaciones (API) para proporcionar la posibilidad de proceso de transacciones distribuidas en las que dos o más programas cooperan para llevar a cabo una función del proceso. Esta posibilidad implica la comunicación entre los dos programas para que puedan compartir los recursos locales como, por ejemplo, ciclos de procesador, bases de datos, colas de trabajo e interfaces físicas como teclados y monitores.

Communications Server da soporte a APPC a través de las API APPC. Consulte las siguientes publicaciones para obtener más información:

- *Client/Server Communications Programming*
- *System Management Programming*

Las siguientes funciones de Communications Server dan soporte a un rango de tipos de LU:

- Pasarela SNA

  La pasarela SNA permite que los sistemas principales IBM System/370 (S/370) o los sistemas principales de arquitectura System/390 (S/390), o ambos, den soporte a estaciones de trabajo conectadas a la LAN que utilizan LU de tipo 0, 1, 2, 3 ó 6.2 para comunicarse a través de una estación de trabajo de pasarela SNA.

  La pasarela SNA da soporte también a las LU de tipo 1, 2 ó 3 para sistemas principales AS/400, que pueden procesar los datos o pasarlos a través hacia sistemas principales de arquitectura S/370 o S/390.

- Aplicación de LU convencional (LUA)

  La LUA consiste en software del sistema que suministra rutinas de servicio para dar soporte a las LU 0, 1, 2 y 3.

Soporte SDDLU

El soporte de LU dependiente de definición propia (SDDLU) le permite definir dinámicamente y activar una LU dependiente en el sistema principal (VTAM). En VTAM, se conoce como definición dinámica de LU dependientes (DDDLU). SDDLU se habilita en Communications Server mediante la codificación de una sentencia LU_MODEL en una definición de LU.

Para habilitar el recurso DDDLU en VTAM, codifique el operando LUGROUP en la sentencia de definición para la PU y codifique un nodo principal de grupo de LU. Para utilizar la rutina de salida SDDLU suministrada por IBM que genera los nombres de LU automáticamente, también debe codificar el operando LUSEED en la sentencia PU.

El operando LUGROUP especifica el nombre del grupo de definiciones LU modelo que VTAM utilizará cuando defina dinámicamente la LU para esta PU. El nodo principal del grupo de LU contiene las sentencias de definición modelo. Las definiciones dinámicas para las LU se construyen utilizando las definiciones de LU modelo contenidas en este nodo principal.

El operando LUSEED proporciona un nombre patrón que se utiliza con la rutina de salida SDDLU para crear un nombre para la LU creada dinámicamente. Cuando se han añadido las sentencias correctas a la sentencia PU y se ha codificado el nodo principal del grupo de LU, estos nodos principales necesitan estar activos para que la función SDDLU se habilite.

Soporte del peticionario de la unidad lógica dependiente

El Peticionario de unidad lógica dependiente (DLUR) es una arquitectura pensada para proporcionar soporte de LU dependiente en una red APPN. Communications Server da soporte a todas las funciones DLUR básicas y a las siguientes funciones opcionales:

- Soporte de LU dependiente con definición propia (SDDLU)

  Mediante la utilización del soporte SDDLU, las LU soportadas por DLUR pueden definirse dinámicamente en VTAM, eliminando, de esta manera, la necesidad de tener que predefinir estas LU.

- Soporte Tomar/Devolver

  Este soporte permite que las sesiones LU-LU permanezcan activas incluso cuando la conexión entre los nodos DLUR y DLUS haya fallado. La conexión puede volverse a establecer con el mismo o con otro DLUS, sin que las sesiones LU-LU se interrumpan.

- Soporte de múltiples subredes.

  Este soporte permite que un nodo DLUR, el nodo DLUS y el nodo que contiene la aplicación estén en subredes diferentes.

- Registro de LU servidas por DLUS

  Un DLUR de nodos finales registra sus LU de modo que el nodo de red pueda localizar estas LU sin tener que pasar las peticiones de localizar al DLUR.

- Soporte de DLUS de reserva

  Cuando falla la conexión con el DLUS primario o no se activa, Communications Server intentará automáticamente establecer una conexión con el DLUS de reserva.

Utilización de DLUR

Para utilizar la función DLUR, se configura una definición **DLUR_DEFAULTS** y se utiliza el nombre de enlace de esa definición como enlace con el sistema principal para las definiciones de LUA, LU 6.2 dependiente o pasarela. Communications Server envía PUNAME, CPNAME y NODEID al DLUS. PUNAME se envía como parte de la información de señalización (CV X'0E').

- Si DLUS es de nivel superior (soporta la comprobación de CV X'0E' en REQACTPU) utiliza PUNAME en su algoritmo de búsqueda. Este está disponible en VTAM 4.3 con PTF o superior.
- Si el DLUS es de nivel inferior, hace caso omiso del CV X'0E'.
- Si no hay ninguna coincidencia de PUNAME o el DLUS es de nivel inferior, el DLUS intenta localizar una PU con un nombre de CP coincidente o con NODEID (IDBLK/IDNUM) predefinido en un nodo principal de conmutación VTAM o creado dinámicamente utilizando la salida ISTEXCCS.

Las conexiones con la red que utilizan la conectividad de su elección (Red en anillo, SDLC, AnyNet, etcétera) deben estar configuradas y activadas antes de que se haya establecido la conexión DLUR a DLUS. Una vez exista la conexión APPN entre DLUR y DLUS, se establecen un par de sesiones de control entre el DLUR y DLUS utilizando una modalidad especial, CPSVRMGR. También se hace referencia a este par de sesiones de control como conductos CP-SVR y aparece como

un enlace con Communications Server. Entonces puede activarse, desactivarse y visualizarse utilizando **Operaciones de nodos SNA**.

Una vez activado el conducto, puede proporcionarse el soporte SSCP a PU y SSCP a LU a las PU y a las LU que tienen definido el conducto como su enlace con el sistema principal. Las sesiones de LU a LU no utilizan el conducto, pero utilizarán la vía de acceso mejor disponible a través de la red.

En el entorno DLUR, puede definirse cualquier número de PU dedicadas en las sesiones LU 6.2. Esto permite que la pasarela proporcione el acceso de gestión de la red a través de la PU dedicada, a las estaciones en sentido descendente sin necesitar numerosos enlaces físicos con los sistemas principales.

La Figura 17 muestra una estación de trabajo de Communications Server actuando como pasarela DLUR para la estación de trabajo y un controlador 4702.

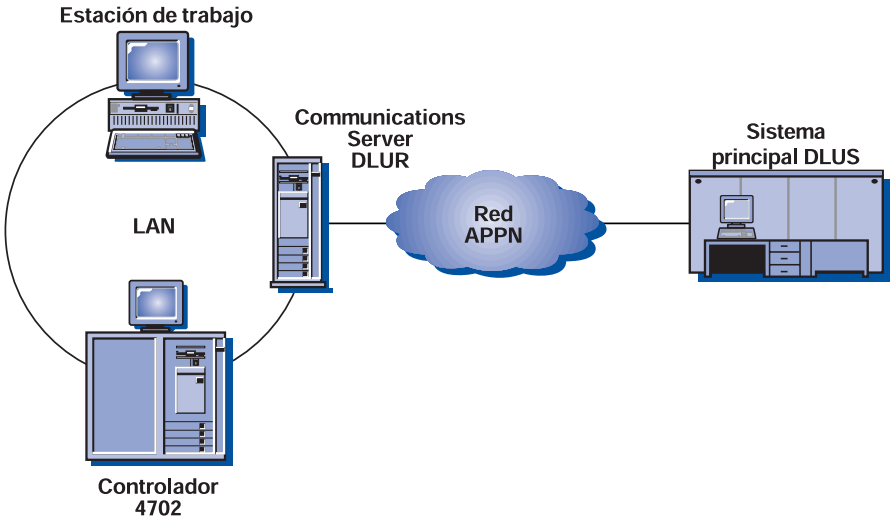


Figura 17. Conexión DLUR para un sistema principal a través de la pasarela Communications Server

Sesiones LU-LU

Las LU de Communications Server pueden iniciar sesiones y responder a las peticiones de iniciación de sesiones. Una LU inicia y responde a las peticiones de acuerdo al tipo de LU: independiente o dependiente.

LU independiente

Una LU independiente puede activar una sesión LU-LU (es decir, enviar una petición BIND) sin ayuda del SSCP; por lo tanto, no tiene ninguna sesión SSCP-LU. Una LU independiente es capaz de enviar y recibir peticiones BIND. Se hace referencia al remitente de BIND como la LU primaria (PLU); se hace referencia al receptor de BIND como la LU secundaria (SLU).

Sólo una LU 6.2 puede ser una LU independiente. Communications Server da soporte a protocolos LU independientes para otros nodos de tipo 2.1, así como para nodos de subárea de tipo 5 de nivel de red de entrada inferior.

Las LU independientes pueden tener sesiones paralelas entre el mismo par de LU y pueden tener múltiples sesiones entre una LU y varias otras LU. Sus límites de

sesiones se establecen en base al nombre de modalidad, que puede ser de 1 a 32 767.

La Figura 18 muestra cómo se pueden establecer sesiones múltiples y paralelas por una LU independiente. LUx da soporte a las sesiones paralelas con LUy y una sola sesión con LUz. La dirección de las flechas de la sesión muestra la relación PLU-SLU. LUx actúa como la PLU de la sesión con LUz y para una de las sesiones con LUy. LUx actúa también como la SLU para una de las sesiones paralelas con LUy.

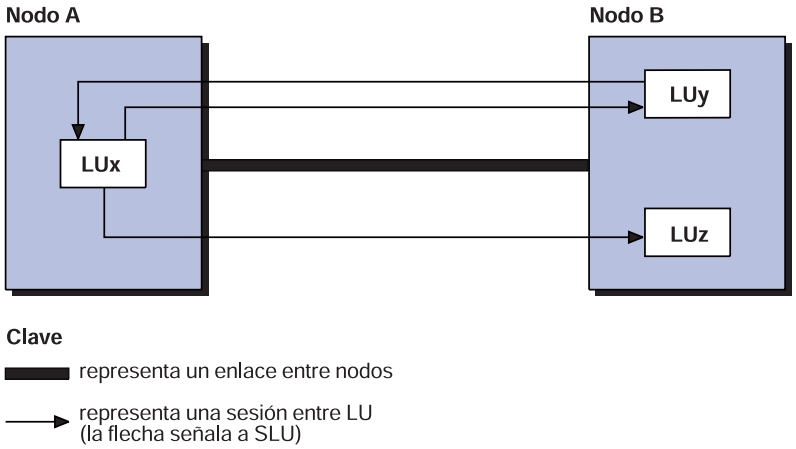


Figura 18. Sesiones múltiples y paralelas

LU dependiente

Una LU dependiente es una LU que está controlada por el sistema principal SNA. Para activar una sesión LU-LU, una LU dependiente necesita la ayuda de un SSCP. Necesita una sesión SSCP-LU para enviar una petición BIND. Los protocolos de LU dependientes están soportados por Communications Server pero sólo para los nodos de subárea de tipo 5 que utilizan los protocolos de tipo 2.0, no para otros nodos periféricos de tipo 2.1. Las LU dependientes sólo actúan como SLU y tienen un límite de sesiones LU-LU de 1. Sin embargo, el soporte de múltiples PU en Communications Server, permite establecer múltiples sesiones SSCP-PU con sesiones LU dependientes.

La función de peticionario de LU dependientes (DLUR) permite que Communications Server aproveche las ventajas del soporte SSCP ampliado proporcionado por un servidor de LU dependientes (DLUS). Algunos de los beneficios de esta función son:

- Las LU dependientes pueden residir en nodos que no son adyacentes al sistema principal.
- La lógica de búsqueda de APPN encuentra la mejor vía de acceso para las sesiones LU-LU.
- Las LU dependientes de SNA pueden obtener ventajas de una red APPN.

Para utilizar DLUR, configure un parámetro **DEFINE_DEPENDENT_LU_SERVER** y utilice el nombre del enlace de esta definición para las definiciones de LUA, LU 6.2 dependiente o pasarela.

LU 6.2

Las LU independientes se definen en el programa VTAM codificando LOCADDR=0. Con LOCADDR=0 pueden definirse tantas LU como se deseen. Sin embargo, tenga en cuenta que no todas las LU 6.2 son LU independientes.

Cuando se definen las LU de una parte de la red APPN en el programa VTAM, debe hacerlo como si estuviese en el nodo de red que conecta esta parte de la red APPN con la red de subárea. Después de la definición de PU de este nodo de red, defina cada LU a la que desee llegar desde la otra parte de la red APPN. No olvide que los puntos de control son LU.

Debe definirse una LU en VTAM para establecer una sesión con otra LU si esta sesión pasa a través de la red de subárea. No hay ninguna manera efectiva de rodearla (por ejemplo, comodines de APPN); VTAM debe saber el nombre de cada LU de destino.

Puesto que una red APPN está pensada para poder cambiar fácilmente, debe definir las LU de la red APPN en un nodo principal especial siempre que sea posible. También puede definir, en VTAM, LU que todavía no existen.

Otras LU

Si el nodo de red utiliza su conexión con la red de subárea para la emulación de 3270, las LU de tipo 2 de la emulación 3270 se definen en la misma macro PU que las LU de tipo 6.2 de la red APPN. El enlace también se utilizará para la conexión entre la emulación 3270 y el sistema principal.

Nodo de red APPN y soporte de T2.1

APPN es una ampliación de la arquitectura de nodos SNA y de tipo 2.1 (T2.1) de IBM. APPN permite la interconexión de sistemas de tamaños muy diferentes formando redes de topología dinámica. Una red APPN es más fácil de utilizar, es más fiable y proporciona más flexibilidad que las redes SNA tradicionales.

Consulte la publicación *3174 APPN Implementation Guide* para obtener información adicional sobre nodos de red APPN.

Compresión de datos

La compresión de datos es el proceso de comprimir bytes repetidos o series de datos repetidos para reducir la longitud de los registros o de los bloques. Esto reduce el tiempo de transferencia necesario para las comunicaciones. Mediante la reducción de la cantidad de datos transferidos entre las sesiones del sistema principal y la estación de trabajo, puede aumentar la productividad de las líneas de velocidad lenta y disminuir los costes por bit de líneas caras.

El aumento del rendimiento, medido por el número de bytes transferidos, que se puede esperar por la utilización de la compresión de datos es, con frecuencia, una proporción de 2:1. Lo que significa que, con la compresión de datos activa, se ahorra un byte de cada dos en los almacenamientos intermedios necesarios para la conversión de protocolos de nivel inferior.

La compresión de datos es beneficiosa cuando se necesita:

- Tiempos de respuesta mejorados, específicamente en líneas de baja velocidad

- Costes reducidos en líneas cuyas tarifas se basan en el volumen de datos
- Menos líneas alquiladas

Sin embargo, la compresión de datos no debe aplicarse a cada sesión que se ejecute ya que existen inconvenientes que se han de tener en cuenta:

- La compresión y descompresión necesitan ciclos adicionales de CPU
- Será necesario un almacenamiento de datos incrementado (de 32 bytes a 9,0 KB)
- La compresión de datos necesita un enlace seguro, tal como se define en la la tabla de clases de servicio (COS) de APPN.
- Es posible que se haya de ajustar el tamaño de RU para obtener el rendimiento mejor. Cada RU se comprime y después se envía. Si se envían paquetes, un tamaño de RU mayor en la modalidad permitirá enviar más paquetes completos.

  Nota: La cantidad de almacenamiento incrementado depende del algoritmo de compresión que utilice. Este aumento es adicional al almacenamiento necesario para el mensaje.

Para ver descripciones detalladas y técnicas de distintos algoritmos de compresión, consulte las publicaciones siguientes:

- *Formatos SNA*
- *Better OPM/L Text Compression IEEE Transactions on Communications, vol COM-34, no 12, pgs 1176-1182,1986*
- *IBM ITSC VTAM V3R4 and V3R4.1 Planning Guide*
- *A Technical Guide to ESA/390 Compression*

Las secciones siguientes describen la compresión a nivel de sesión SNA y la implantación de Communications Server.

Arquitectura de compresión a nivel de sesión SNA

La compresión a nivel de sesión SNA implanta la compresión de datos en la semisesión LU-LU. Con Communications Server está disponible para todos los tipos de LU soportados, es decir: Las LU de tipo 0, 1, 2, 3 y 6.2. La compresión de datos a nivel de sesión proporciona estas ventajas:

- Es más eficaz comprimir los datos antes de cifrarlos
- Según los tipos de datos serán más eficaces unos algoritmos u otros
- Los programas de aplicación no tienen que proporcionar su propia lógica de compresión

Generalmente, se definen dos algoritmos para la compresión a nivel de sesión SNA, Codificación de longitud de ejecución (RLE) y un formato de Lempel-Ziv (LZ). Communications Server da soporte a la compresión a nivel de sesión SNA que utiliza los siguientes algoritmos:

- SIN compresión.
- Compresión RLE; RLE es el algoritmo má sencillo y más ampliamente conocido, que sustituye las series o los bytes idénticos por series codificadas más cortas.

- La compresión LZ9; LZ9 es un algoritmo de compresión dinámica que comprime las series que se han visto con anterioridad (en las RU actual o precedentes) en un código de 9 bits que representa el índice de origen cero de una entrada en la tabla de compresión/descompresión. Las entradas de la tabla almacenan las series vistas anteriormente.
- La compresión LZ10; LZ10 es un algoritmo de compresión dinámica que comprime las series que se han visto con anterioridad (en las RU actual o precedentes) en un código de 10 bits que representa el índice de origen cero de una entrada en la tabla de compresión/descompresión. Las entradas de la tabla almacenan las series vistas anteriormente.

Normalmente, LZ comprime los datos mejor que RLE, pero tiene un mayor coste de memoria y de función de CPU.

La compresión a nivel de sesión SNA ve la sesión en dos direcciones, PLU-SLU y SLU-PLU. La unidad lógica primaria (PLU) es la LU responsable de activar la sesión. La unidad lógica secundaria (SLU) es la LU que responde. La PLU activa una sesión enviando una petición de Vincular sesión (BIND) a la SLU, que responde con una petición BIND. Esto significa que pueden utilizarse diferentes algoritmos de compresión en las direcciones PLU-SLU y SLU-PLU. Esto se lleva a cabo a través de la negociación BIND de los niveles de compresión. LU 6.2 puede utilizar cualquier combinación de niveles de compresión para una sesión (por ejemplo, PLU podría utilizar RLE y SLU-PLU podría utilizar LZ9). Los demás tipos de LU tienen la compresión habilitada o inhabilitada. Cuando está habilitada, el nivel de compresión de PLU-SLU es LZ9 y de SLU-PLU es RLE.

Compresión de datos de Communications Server

Communications Server da soporte a la compresión de datos a nivel de sesión SNA con los algoritmos de compresión RLE, LZ9 y LZ10. Con Communications Server, puede especificar la utilización de la compresión de datos para las comunicaciones en sesiones CPI-C (a través de la sesión APPC), sesiones APPC (LU 6.2) y sesiones LUA (LU 0, LU 1, LU 2 y LU 3).

Se utiliza una configuración de dos partes para habilitar la compresión de datos. El nodo de Communications Server debe tener habilitada la compresión de datos y primero debe habilitarse la LU (APPC y LUA). Los dos campos de compresión de los nodos (nivel y señal) están en la ventana de características del nodo local (palabra clave **NODE** del archivo .ACG).

El campo de nivel de compresión establece el nivel máximo con el que puede iniciarse cualquier sesión: NONE, RLE, LZ9 o LZ10. Este campo tiene prioridad sobre todos los niveles de compresión configurados o que se han intentado (la única excepción es DFT autónomo, que no necesita la definición de nodos). Si está configurando una sesión utilizando LUA (LU 0, LU 1, LU 2 y LU 3) para dar soporte a la emulación 3270 o a las impresoras, es necesario LZ9 para la compresión de datos. Los demás niveles de compresión no permiten la compresión de datos para estos tipos de LU.

El tamaño de unidad de petición por omisión para las modalidades comprimidas es el doble del tamaño de la unidad de transmisión básica (BTU) de la conexión. Si está utilizando la conmutación de paquetes, es posible que no desee utilizar este tamaño por omisión; en su lugar, utilice un tamaño mayor y segmente los paquetes.

La compresión de LU 6.2 puede habilitarse mediante:

- La utilización de las modalidades suministradas con Communications Server
  - #INTERC
  - #BATCHC
  - #BATCHCS
  - #INTERCS
- El cambio o la adición de modalidades con la compresión habilitada

Los tres campos de compresión de modalidad, la compresión necesaria, el nivel de compresión PLU->SLU y el nivel de compresión SLU->PLU, se visualizan en el panel Definición de modalidad (palabra clave **MODE** en el archivo .ACG).

La compresión necesaria puede tener dos valores.

Prohibida Sin compresión.

Pedida Utilícelo para pedir la compresión de datos con los valores definidos en el nivel de compresión PLU->SLU y en el nivel de compresión SLU->PLU. Es posible que el nivel pedido no se pueda obtener por las siguientes razones:

- Los valores del nodo han limitado el nivel permitido
- La SLU ha negociado los niveles, bajándolos

La SLU acepta los niveles de compresión pedidos por la PLU, a menos que esté limitada por sus valores de compresión del nodo.

Para obtener más información sobre la compresión de Communications Server, consulte el texto de la ayuda en línea para el producto o la publicación *Configuration File Reference*.

Cifrado a nivel de sesión SNA

El cifrado a nivel de sesión SNA le permite cifrar todos los datos o los datos seleccionados que se transfieren entre la estación de trabajo y el sistema principal. Si desea proteger cualquier dato de la estación de trabajo utilizando el cifrado, el sistema principal debe configurarse también para utilizar el cifrado.

Debe estar instalado un adaptador Coprocesador de criptografía IBM SecureWay 4758 PCI (al que se hace referencia como IBM 4758) en el servidor para permitir la confidencialidad de los datos. Este adaptador debe inicializarse siguiendo las instrucciones proporcionadas con el adaptador.

En Communications Server, el cifrado a nivel de sesión LU 6.2 se configura en base a la descripción de modalidad utilizada para un programa de transacción determinado. Hay dos niveles de cifrado:

- Nivel de sesión APPC

  Estrictamente entre dos LU, no se implican los puntos de control en la conversión de claves
- Conversión de claves de sesión APPN

Además de la LU de origen, también convierten las claves el punto de control de la LU de origen (EN o NN) y posiblemente su servidor NN.

Para configurar una modalidad de cifrado, active la ventana Características de SNA y seleccione **MODALIDADES**. Después, en la ventana Definición de modalidad, seleccione **Configurar...**. Aparece la ventana Soporte de compresión y de cifrado a nivel de sesión. Los parámetros para la configuración del cifrado están divididos en dos partes:

- Para el cifrado a nivel de sesión, puede especificar si el cifrado es opcional (las LU negocian) u obligatorio (debe utilizarse el cifrado).

  Nota: El cifrado de Communications Server para un sistema principal siempre se establece para que sea obligatorio.

- En la conversión de claves de sesión APPN, puede especificar que sólo la LU convierta la clave, que sólo el nodo final convierta la clave de sesión o que el nodo final y su nodo de red conviertan la clave.

Communications Server necesita otros productos para el almacenamiento y conversión de claves. Es necesario el producto Arquitectura de criptografía común (CCA) para el almacenamiento de claves, gestionado por los programas de utilidad suministrados con el adaptador IBM 4758. Communications Server llama a un producto CCA, que interactúa con el adaptador IBM 4758 para obtener las claves y cifrar los datos.

Usuarios VTAM:

Communications Server no cifra la sesión SNASVCMG. Debe especificar ENCR=OPT en la sentencia APPL de la definición de aplicación VTAM. Cuando trabaje con VTAM, debe especificar el cifrado en la sentencia MODEENT. Por ejemplo:

```
ENCR=B'0011' PARA CIFRADO OBLIGATORIO
```

Para utilizar el recurso de cifrado VTAM, debe iniciar el Recurso de criptografía programada (PCF) de IBM antes de iniciar VTAM.

Empezando por VTAM V3R4.1, VTAM utiliza una nueva interfaz para el Recurso de servicio de cifrado integrado/MVS (ICSF/MVS) para los servicios de cifrado como, por ejemplo, proveer el cifrado a nivel de sesión. Esta interfaz se ajusta a la Arquitectura de cifrado común (CCA) tal como la implanta ICSF/MVS. Con este soporte, puede iniciar y detener el servicio de cifrado después de que se haya iniciado VTAM y puede cambiar la clave maestra sin interrumpir VTAM ni las sesiones LU-LU activas.

Para obtener información sobre cómo definir el cifrado de datos, consulte la publicación *OS/390 eNetwork Communications Server: SNA Network Implementation*.

Servicios de gestión

Los servicios de gestión (MS) de Communications Server son funciones distribuidas entre los componentes de la red que hacen funcionar, gestionan y controlan una red. Esta posibilidad se basa en la arquitectura de servicios de gestión SNA documentada en el manual *Systems Network Architecture Management Services Reference*.

Puntos focales, puntos de servicio y puntos de entrada

Communications Server proporciona el soporte de programación que permite la instalación de las aplicaciones de punto de servicio focal (FP), punto de servicio (SP) y punto de entrada (EP). Las aplicaciones SP de servicios de gestión sólo son una variación de las aplicaciones EP de los servicios de gestión y sólo se distinguen en las clases de funciones que proporcionan; de lo contrario, interactúan con un punto focal de servicios de gestión como aplicaciones EP de servicios de gestión.

Punto focal Un punto focal de servicios de gestión es un punto central de control para la gestión de una red. Desde una aplicación SP de servicios de gestión o EP de servicios de gestión, el punto focal de servicios de gestión puede pedir determinados datos relativos al funcionamiento de una red como, por ejemplo, los datos de un problema y de rendimiento o la identificación de un producto.

El punto focal de servicios de gestión también puede aceptar determinados datos de gestión no solicitados de los nodos que gestiona basándose en la categoría de los datos de servicios de gestión. Un ejemplo de una categoría de servicios de gestión son las alertas MS. Un punto focal de servicios de gestión puede gestionar una o varias categorías de datos de servicio de gestión y, puede haber uno o varios puntos focales de servicios de gestión en una red. IBM Communications Server, el programa IBM NetView y el sistema operativo IBM OS/400 son ejemplos de productos que proporcionan la posibilidad de punto focal de servicios de gestión.

Punto de servicio Un SP de servicios de gestión es la función de un nodo que puede pedir y captar datos de dispositivos que, por sí mismos, no pueden servir como EP de servicios de gestión como, por ejemplo, dispositivos conectados por protocolos de LAN (pero no por protocolos SNA de nivel superior) al nodo SP de servicios de gestión. Aparte de reunir datos que no son locales, un SP de servicios de gestión funciona como un EP de servicios de gestión en relación al punto focal de servicios de gestión. Los productos IBM NetView/PC y IBM LAN Network Manager son ejemplos de aplicaciones EP de servicios de gestión que proporcionan las funciones SP de servicios de gestión y las funciones EP de servicios de gestión.

Punto de entrada Un EP de servicios de gestión es la función de un nodo que capta los datos de servicios de gestión locales y los envía a un punto focal de servicios de gestión para su proceso, en una petición o sin solicitud. Communications Server proporciona la función EP de servicios de gestión para enviar alertas al punto focal de servicios de gestión de alertas. Estas alertas pueden originarse en Communications Server o en los DLC que utiliza. Communications Server también proporciona soporte de programación para aplicaciones como, por ejemplo, los productos de programa IBM NetView/PC e IBM LAN Network Manager, suministrando las alertas que se han de enviar al punto focal de servicios de gestión de alertas.

Niveles de arquitectura de servicios de gestión SNA

Un producto SNA implanta un nivel en particular (o generación) de la arquitectura Servicios de gestión SNA, y algunos productos soportan varios niveles de la arquitectura. Communications Server puede enviar datos de servicios de gestión y recibir datos de servicios de gestión de, productos SNA que implantan cualquiera de los tres niveles de la arquitectura de servicios de gestión. Estos niveles son:

Nivel de soporte de múltiples dominios (MDS) Un producto SNA que implanta el nivel MDS de la arquitectura de servicios de gestión como, por ejemplo, Communications Server e IBM NetView Versión 2 Release 2 (o posterior). Puede enviar y recibir unidades de mensajes MDS (MDS-MU). IBM NetView Versión 2 Release 2 proporciona el nivel MDS como una LU de subárea, no como punto de control (CP), e utiliza las sesiones de modalidad SNASVCMG para transportar MDS-MU. Como punto focal, da soporte a relaciones explícitas (primarias) e implícitas (de reserva) FP-EP. NetView Versión 2 Release 2 continúa dando soporte a la relación FP-EP del sistema principal para los productos EP que no tengan soporte de nivel MDS.

Nivel de migración Un producto SNA que implanta el nivel anterior de la arquitectura de servicios de gestión como, por ejemplo, IBM OS/400 Versión 1 Release 3 Nivel de modificación 0 (o anterior). Un producto de nivel de migración puede dar soporte a relaciones explícitas, por omisión y FP-EP. La relación FP-EP se infiere cuando se activan las sesiones CP-CP para un nodo de nivel de migración. Un nodo de red (NN) de servicio de nivel de migración no envía las Posibilidades MS para notificación PF a sus nodos finales (EN) servidos y un EN servido a nivel de migración no acepta las Posibilidades MS para notificación de su NN de servicio. Puede enviar y recibir CP-MSU pero no MDS-MU. Como punto focal, sólo da soporte a la categoría MS de alertas.

Nivel de Transporte de vectores de gestión de redes (NMVT) Un producto SNA que implanta el nivel NMVT de la arquitectura de servicios de gestión SNA como, por ejemplo IBM NetView Versión 2 Release 1 (o posterior). NMVT es una unidad de petición (RU) de servicios de gestión que fluye en una sesión activa entre los servicios de gestión de PU y los servicios de gestión de punto de control. Si un NMVT se direcciona desde una estación de trabajo a través de una pasarela, la pasarela añade su nombre de punto de control al NMVT.

Control de flujo

Para controlar el flujo de datos en una red, Communications Server utiliza el ritmo adaptador a nivel de sesión. El ritmo se produce entre cada par de nodos adyacentes que participan en la ruta. El ritmo entre dos nodos adyacentes es independiente del ritmo utilizado entre otros nodos adyacentes de la ruta.

Ritmo a nivel de sesión

El ritmo adaptador a nivel de sesión utiliza un esquema basado en ventanas, en el que un remitente sólo puede enviar un número limitado, o ***ventana***, de unidades de petición por cada otorgamiento explícito de permiso para continuar. El tamaño de la ventana puede cambiarse en base a las condiciones del receptor. Esta función permite que un nodo controle la cantidad de datos que se envían y reciben durante el funcionamiento normal de la sesión. El control de ventanas permite que

el nodo receptor gestione su velocidad para recibir los datos en sus almacenamientos intermedios de sesión. El ritmo adaptador a nivel de sesión proporciona a un nodo que da soporte a muchas sesiones, un medio dinámico de asignar recursos a una sesión que tiene una ráfaga de actividad y de reclamar los recursos no utilizados a sesiones que no tienen actividad. El ritmo adaptador de nivel de sesión permite que el nodo receptor utilice sus recursos de almacenamiento intermedio disponibles de manera eficaz.

Puesto que cada etapa de sesión entre los puntos finales tiene un ritmo independiente, tanto los nodos de punto final como los intermedios pueden adaptar su ritmo para las sesiones que manejan de acuerdo a sus propias condiciones locales de congestión. Esta acción es la base para el control de flujo global y la gestión de congestión en las redes APPN.

Sin embargo, si una sesión interactiva y una sesión que transfiere un archivo grande comparten un enlace, los datos de la sesión interactiva deben transmitirse tan rápido como sea posible. Hay dos formas de hacerlo:

1. Asignar una prioridad inferior a la sesión de transferencia de archivos. #BATCH utiliza prioridad baja.
2. Utilice un ritmo fijo con un tamaño de ventana pequeño para la sesión de transferencia de archivos para permitir que los datos de la sesión interactiva utilicen el enlace cuando la sesión de transferencia de archivos esté esperando la respuesta del ritmo. Si está conectado directamente a un sistema principal NCP, se puede utilizar el ritmo fijo de ventana de dos direcciones para establecer el ritmo en ambas direcciones para la ventana receptora en la modalidad definida.

Ritmo adaptador BIND

El tráfico BIND se puede producir en ráfagas, en particular en el arranque del nodo o de la red. Por lo tanto, el ritmo adaptador BIND existe para controlar el flujo de peticiones BIND entre dos nodos adyacentes. Se emplea el mismo algoritmo de ventana utilizado para el ritmo de nivel de sesión.

Segmentación y ensamblación

Para transmitir RU más largas que la unidad básica de transmisión de tamaño máximo permitida por un enlace en particular, Communications Server da soporte a la segmentación y ensamblación de datos. Estos segmentos se ensamblan en RU completas en cada nodo asociado. Esta acción permite que el tamaño de RU definido para una sesión sea independiente del enlace que se utiliza para la ruta.

Ritmo de direccionamiento de alto rendimiento

El direccionamiento de alto rendimiento (HPR) proporciona un nuevo método de control de flujo llamado control adaptador de congestión basado en la velocidad (ARB). ARB regula el flujo de tráfico previendo la congestión de la red y reduciendo la velocidad de envío de un nodo a la red, impidiendo la congestión en lugar de reaccionando a ella.

Ritmo fijo

El ritmo fijo le permite compartir una conexión física entre dos sesiones. Sin el ritmo fijo, los datos que se han de transmitir se colocan en una cola de control de enlace de datos (DLC) común y los datos interactivos siguen a los datos puestos en cola anteriormente. El ritmo fijo reduce también la cantidad de almacenamiento que se puede utilizar para colocar datos en la cola DLC. El ritmo fijo de dos direcciones puede utilizarse con un NCP para evitar la definición del ritmo fijo del sistema principal. Sin embargo, en general, el ritmo adaptador es el método más eficaz de transferencia de datos entre nodos.

La prioridad de la transmisión, como el ritmo fijo, permite la compartición de un enlace físico entre dos sesiones. Sin embargo, bloqueará almacenamiento a medida que se coloquen los datos en las colas DLC, pero no necesita las respuestas de ritmo adicionales que se necesitan para el ritmo fijo.

Partición de LU entre sistemas principales

Cuando se definen múltiples conexiones de sistema principal de subárea, se necesita que el tráfico del dominio de un sistema principal determinado entre sólo en un enlace lógico. Tenga en cuenta que las conexiones de marcación manual parecen como un solo enlace. Debe definir una PU diferente para dar soporte a cada sistema principal diferente. Sólo los enlaces de sistema principal definidos en el punto de control tienen sesiones CP-CP y participan en la red APPN. Los enlaces que tienen **USE_PU_NAME_IN_XID=1** no pueden tener sesiones CP-CP. Por el contrario, los enlaces de sistema principal pueden tener sesiones CP-CP y también pueden participar en la comunicación APPN. La palabra clave **LINK_STATION** especifica el nombre de PU y el enlace lógico que se ha de utilizar para la PU. Si son necesarios enlaces paralelos (en situaciones en que hay más de 254 LU dependientes), uno de los enlaces debe tener el soporte de sesión CP-CP establecido en No.

Cada LU dependiente se puede definir como asociada a solo una PU. La palabra clave **LOCAL_LU** especifica el nombre de enlace con el sistema principal utilizado para la LU de tipo 6.2. La palabra clave **LU_0_TO_3** especifica el nombre de enlace con el sistema principal para LUA y el perfil 3270 especifica el enlace con el sistema principal para cada sesión de emulación 3270.

El punto de control define automáticamente una PU con el mismo nombre que el punto de control. Las LU dependientes que están definidas en un SSCP de subárea se pueden asociar con la PU de punto de control. (De hecho, la LU definida automáticamente para el punto de control también se puede definir como dependiente.) Cada PU 2.0 adicional para un sistema principal de subárea diferente necesita un enlace separado y una definición de PU. Una PU se define especificando la PU en una palabra clave **LINK_STATION**. No es necesario si todas las LU son independientes.

Si la sesión SSCP-PU ha de enviar alertas al sistema principal, defina el enlace de punto focal con la palabra clave **NODE** en el archivo .ACG. Si un sistema principal tiene que recibir las alertas, especifique un enlace lógico para el punto de control con el sistema principal. Si el enlace con ese sistema principal no está disponible, Communications Server registra las alertas. Las únicas peticiones de gestión de red que se aceptan de un sistema principal PU 2.0 son las de PU de punto de control. Las respuestas se envían al mismo sistema principal utilizando la PU de punto de control.

Cada unidad lógica dependiente debe tener una dirección local configurada que sea a misma que la configurada en el sistema principal. Sin embargo, la utilización de la misma pasarela SNA permite la conversión de la dirección de pasarela. Una LU 6.2 dependiente puede actuar como una LU independiente para un nodo similar; es decir, sólo es dependiente para la subárea. Una LU como esta no debe formar parte de una red APPN con cualquier otra conexión con la misma subárea, es decir, la subárea que contiene el SSCP de control. Sólo está permitida una conexión de subárea en la red APPN, a menos que las subáreas sean independientes. Aunque una pasarela pueda tener enlaces paralelos con la misma subárea, sólo puede tener sesiones CP-CP y tráfico APPN.

Un SSCP de la red de subárea activa las LU dependientes que controla después de que se haya establecido el enlace con el mismo. Hasta que se active una LU, la LU no puede iniciar una sesión. Cuando se desactiva un APPC, se pide la desconexión de cada sistema principal activo que tenga una sesión con una PU del nodo. Cada sistema principal libera el enlace después de desactivar las LU y después la PU de la sesión SSCP-PU.

Soporte de pasarela SNA

Communications Server proporciona una pasarela Systems Network Architecture (SNA) de funciones completas. La pasarela permite que múltiples estaciones de trabajo conectadas a la LAN accedan a sistemas principales System/370 o System/390 a través de una o varias conexiones físicas con uno o varios sistemas principales. Esto ayuda a reducir el coste por estación de trabajo de las conexiones de sistema principal.

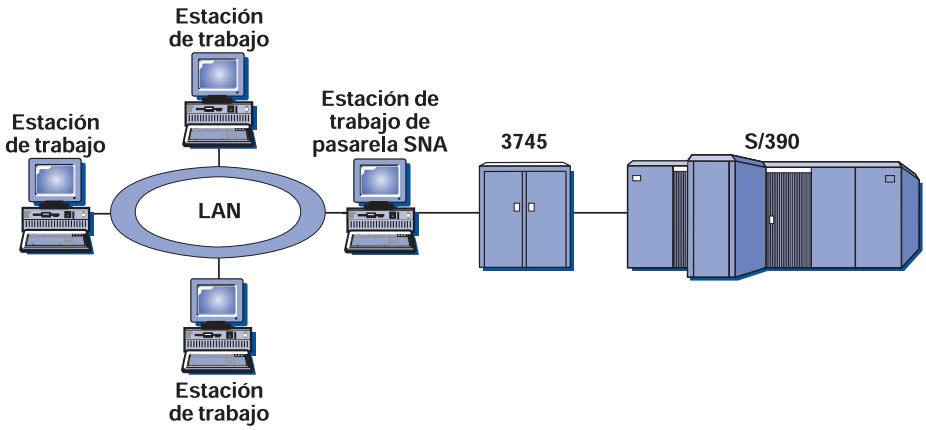


Figura 19. Ejemplo de configuración de pasarela SNA

La pasarela de Communications Server da soporte a los protocolos SNA LU 0, 1, 2, 3 y LU 6.2 dependiente (APPC). Con la función AnyNet SNA sobre TCP/IP, las estaciones de trabajo pueden comunicarse ahora con la pasarela SNA en una red IP. La pasarela también da soporte a la LU 0, 1, 2 ó 3 para un sistema principal AS/400 que utiliza el paso a través SNA. El sistema principal AS/400 pasa los datos a través a un sistema System/390.

Una pasarela también puede actuar como conversor de protocolo entre estaciones de trabajo conectadas a una LAN y a una línea de sistema principal WAN.

Las LU definidas en la pasarela pueden estar dedicadas a una estación de trabajo en particular o agrupadas entre múltiples estaciones de trabajo. La agrupación permite que las estaciones de trabajo compartan LU comunes, lo que aumenta la eficacia de las LU y reduce los requisitos de configuración y de arranque en el sistema principal. También puede definir múltiples agrupaciones de LU, cada agrupación asociada con una aplicación específica. Y puede definir agrupaciones comunes que se asocian con múltiples sistemas principales. Cuando un cliente se conecta a una pasarela, la pasarela recupera una LU de la agrupación para establecer una sesión. La LU se devuelve a la agrupación para que otras estaciones de trabajo la accedan cuando se termine la sesión.

Además, una pasarela SNA puede dar soporte al reenvío de transportes de vectores de gestión de red (NMVT) entre las estaciones de trabajo y el sistema principal.

Cada sistema principal ve la pasarela SNA como un nodo PU 2.0 SNA, que da soporte a una o varias LU por estación de trabajo. Por lo que se refiere al sistema principal, todas las LU pertenecen a la PU de pasarela SNA. La pasarela SNA puede tener múltiples conexiones de sistema principal simultáneamente y puede dirigir diferentes sesiones de estación de trabajo a sistemas principales específicos.

Para las estaciones de trabajo soportadas, la pasarela SNA se parece a un controlador de comunicaciones SNA PU 4 y reenvía peticiones del sistema principal como, por ejemplo, BIND y UNBIND. Las LU de estación de trabajo no conocen la pasarela SNA. Sin embargo, la pasarela SNA, conoce todas las LU de las estaciones de trabajo.

Las aplicaciones en sentido descendente que utilizan los protocolos de conectividad SNA para la LU 0, 1, 2 y 3 y 6.2 dependiente y en comunicación a través de una pasarela SNA para un sistema principal, están soportadas por Communications Server. La Tabla 4 en la página 69 resume las características de pasarela SNA.

Tabla 4. Resumen de pasarela SNA

Característica	Descripción
Estaciones de trabajo activas	254 (LAN) por adaptador 128 (X.25)
DLC	AnyNet (SNA sobre TCP/IP) Twinaxial (sólo en sentido ascendente) LAN (cualquier adaptador de red que se ajuste a NDIS**) X.25 SDLC (síncrono, asíncrono y AutoSync) Canal OEM (solo en sentido ascendente) Canal MPC (sólo en sentido ascendente, necesita DLUR) Ampliación de empresa
Estaciones de trabajo en sentido descendente	Cualquier producto que da soporte a los protocolos de conectividad SNA para las LU 0, 1, 2, 3 y 6.2.
Adiciones y cambios dinámicos	Sí
Soporte de estación de trabajo implícita	Sí
Agrupación de LU	Sí
Número máximo de LU	254 por PU; ningún límite en el número de PU
Modalidad de funcionamiento	Múltiples PU en sentido descendente (no aparentes para el sistema principal) PU no visibles para el sistema principal (excepto cuando son a través de DLUR)
Soporte de múltiples PU	Sí
Soporte de segmentación	Sí
Tipos de LU soportados	LU 0, 1, 2, 3 y 6.2 dependiente

Planificación e instalación

© Copyright IBM Corp. 1989, 1996

Planificación del soporte de AnyNet

Communications Server permite dos tipos de soporte de AnyNet:

- Nodo de acceso y pasarela AnyNet SNA sobre TCP/IP
- Nodo de acceso y pasarela AnyNet Sockets sobre SNA

La función AnyNet SNA sobre TCP/IP de Communications Server permite que aplicaciones SNA se comuniquen en redes IP y SNA interconectadas.

La función de nodo de acceso SNA sobre TCP/IP permite que se comuniquen aplicaciones SNA que residen en una red IP. Esta función soporta la LU6.2 independiente y las LU 0, 1, 2, 3 ó 6.2 dependientes con o sin el peticionario de LU dependientes (DLUR). Además, el nodo de acceso SNA sobre TCP/IP puede utilizarse conjuntamente con la pasarela SNA para permitir sesiones de pasarela SNA sobre TCP/IP.

La función de pasarela SNA sobre TCP/IP amplía el alcance de las aplicaciones SNA permitiendo que las aplicaciones SNA de una red SNA se comunique con aplicaciones SNA de una red IP. La pasarela SNA sobre TCP/IP da soporte a sesiones LU 6.2 independientes.

Para obtener más información sobre cómo configurar AnyNet SNA sobre TCP/IP, consulte el apartado “Configuración de AnyNet SNA sobre TCP/IP”.

La función de nodo de acceso Sockets sobre SNA permite que los programas de aplicación TCP/IP que utilizan la interfaz de socket WinSock 1.1 y WinSock 2.0 se comuniquen sobre una red SNA.

La función de pasarela Sockets sobre SNA permite que las aplicaciones de sockets de las redes SNA y TCP/IP se comuniquen. Las pasarelas Sockets sobre SNA se utilizan con frecuencia para conectar redes TCP/IP aisladas utilizando una red principal SNA.

Consulte el apartado “Configuración de AnyNet Sockets sobre SNA” en la página 86 para obtener más información sobre la configuración de Sockets sobre SNA.

Configuración de AnyNet SNA sobre TCP/IP

Esta sección contiene información detallada acerca de la configuración de AnyNet SNA sobre TCP/IP.

Correlación de recursos SNA con direcciones IP

Uno de los pasos más cruciales para permitir la comunicación SNA sobre TCP/IP no se realiza a través de paneles del Communication Server. Antes de poder establecer sesiones o conexiones SNA, SNA sobre TCP/IP debe determinar la dirección IP del asociado. Esto se consigue correlacionando el identificador SNA del asociado con una dirección IP utilizando los pasos siguientes:

1. SNA sobre TCP/IP recibe el identificador SNA de Communications Server en uno de los formatos siguientes:

© Copyright IBM Corp. 1989, 1996

- Para nombres de LU, `idred.nombrelu`
- Para nombres de CP, `idred.nombrecp`
- Para los valores DBLK e IDNUM, configurados como `ID de nodo adyacente`, con dos campos: `ID de bloque` e `ID de unidad física`.

2. SNA sobre TCP/IP toma el identificador y genera un nombre de dominio:
   - Para nombres de LU, `nombrelu.idred.sufijosna`
   - Para nombres de CP, `nombrecp.idred.sufijosna`
   - Para los valores IDBLK e IDNUM, `bbbnnnnn.sufijosna`

     Nota: El valor por omisión para `sufijosna` es **SNA.IBM.COM**. Para obtener información adicional sobre el sufijo de nombre de dominio SNA, consulte la ayuda en línea.

   La Figura 20 muestra ejemplos de nombres de dominio generados por SNA sobre TCP/IP.

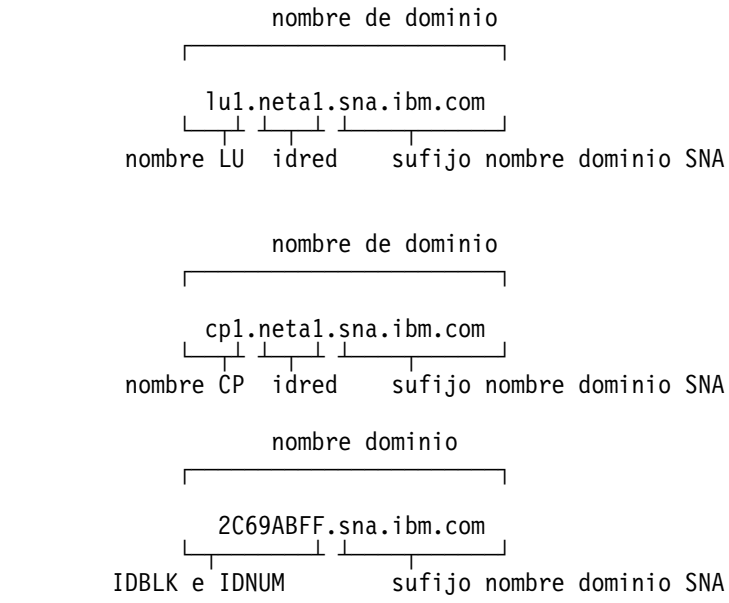


Figura 20. Formatos de los nombres de dominio que SNA sobre TCP/IP crea

3. SNA sobre TCP/IP pide que el nombre de dominio se convierta en una dirección IP.
4. TCP/IP utiliza el archivo HOSTS o el servidor de nombres del dominio para convertir el nombre de dominio en una dirección IP (por ejemplo, `9.67.192.28`).

Cuando la dirección IP incluye pasarelas SNA sobre TCP/IP, tenga en cuenta los siguientes puntos adicionales en la correlación de direcciones:

- Si se puede llegar a la LU asociada a través de una pasarela, el nombre de dominio del asociado debe correlacionarse con la dirección IP de la pasarela. Si existen pasarelas paralelas, el nombre de dominio debe correlacionarse con cada dirección IP de pasarela.
- Para minimizar la información de correlación de direcciones necesaria para AnyNet, tome en consideración la utilización de un convenio de denominación en el que el nombre de LU sea el mismo que el nombre del sistema principal

TCP/IP. Por ejemplo, suponga que el nombre de sistema principal del sistema sea PATR.ANYNET.EMPRESA.COM. Si utiliza el nombre de LU PATR y el idred ANYNET y después establece el sufijo de nombre de dominio SNA en EMPRESA.COM, AnyNet pedirá a TCP/IP que resuelva el nombre PATR.ANYNET.EMPRESA.COM. Este nombre ya debe estar en el servidor de nombres del dominio.

Definición de nombres de dominio y direcciones IP

Esta sección describe la función de resolución de nombres TCP/IP, utilizada por AnyNet para correlacionar los recursos SNA con direcciones IP. Esta función pide a los archivos HOST locales y a cualquier servidor de nombres del dominio que conviertan un nombre de dominio (por ejemplo, `lu1.neta1.sna.ibm.com`) en una dirección IP (por ejemplo, 10.1.1.1).

Archivo HOSTS Puede utilizar los archivos HOST de TCP/IP para correlacionar los nombres de dominio con las direcciones IP de la red. Sin embargo, cuando la red vaya crezca y el mantenimiento del archivo HOSTS de cada estación de trabajo de usuario final consuma demasiado tiempo, se recomienda utilizar un servidor de nombres del dominio.

El archivo HOST (en el subdirectorio drivers\etc del directorio del sistema Windows NT) lista:

- La dirección IP
- El nombre de dominio
- Otros alias para el nombre de dominio

Por ejemplo, si la dirección IP es 10.1.1.1, el ID de red es NETA1, el nombre de recurso SNA es LUA1 y el sufijo de nombre de dominio SNA es el valor por omisión (`sna.ibm.com`), entre lo siguiente en el archivo HOSTS:

```
10.1.1.1      lua1.neta1.sna.ibm.com
```

Servidor de nombres de dominio Los nombres de dominio y las direcciones IP también pueden definirse en la base de datos del servidor de nombres de dominio.

Un servidor de nombres de dominio correlaciona cada identificador SNA con una dirección IP correspondiente. La ubicación de estos servidores se configura en la sección Red del Panel de control.

Para obtener más información sobre los archivos HOSTS y los servidores de nombres de dominio, consulte la documentación de TCP/IP. Si la estación de trabajo utiliza el soporte de TCP/IP en Windows NT, consulte la documentación en línea de TCP/IP que se incluye con el producto Windows NT.

Consideraciones de pasarela SNA sobre TCP/IP

La información siguiente pertenece a las pasarelas pero no a las funciones de nodo de acceso.

Definición de nombres de CP exclusivos y nombres de red de conexión

Para configuraciones que tienen dos o más pasarelas SNA sobre TCP/IP que conectan una red SNA con dos o más redes IP, necesita definir un nombre de punto de control (CP) SNA exclusivo y un nombre de red de conexión SNA exclusivo para cada red IP.

Todas las LU que residen en nodos de acceso de la red IP parecen residir en un nodo con este nombre de CP.

Utilice el archivo de datos invertido del servidor de nombres de dominio o el archivo HOSTS para definir el nombre de CP y el nombre de red de conexión para una red IP determinada. Correlacione la dirección IP 127.0.0.3 con el nombre CP y correlacione la dirección IP 127.0.0.4 con el nombre de red de conexión.

El siguiente ejemplo muestra las entradas en el archivo de datos invertido. Para una red IP con el ID de red SNA NETA, el nombre de CP MINOMBCP y el nombre de red de conexión MICNET, se definirían las siguientes entradas:

```
127.0.0.3       NETA.MINOMBCP.
127.0.0.4       NETA.MICNET.
```

Notas:

1. Sólo es necesario un punto al final del nombre si la definición está en el archivo de datos invertido DNS. No se utiliza ningún punto en las definiciones del archivo HOSTS.
2. No incluya el sufijo de nombre de dominio SNA.

La función AnyNet SNA sobre TCP/IP de Communications Server proporciona un nombre de CP por omisión ($ANYNET.$GWCP) y un nombre de red de conexión por omisión ($ANYNET.$GWCNET). En las configuraciones con una red IP, puede utilizar el valor por omisión no definiendo ningún nombre de CP ni ningún nombre de red de conexión. En las configuraciones con múltiples pasarelas que se conectan a múltiples redes IP, una red IP puede utilizar el valor por omisión. Sin embargo, debe definir un nombre de CP exclusivo y un nombre de red de conexión para todas las demás redes IP.

La Figura 21 en la página 77 muestra cómo definir el nombre de CP y el nombre de red de conexión para una configuración con dos redes IP.

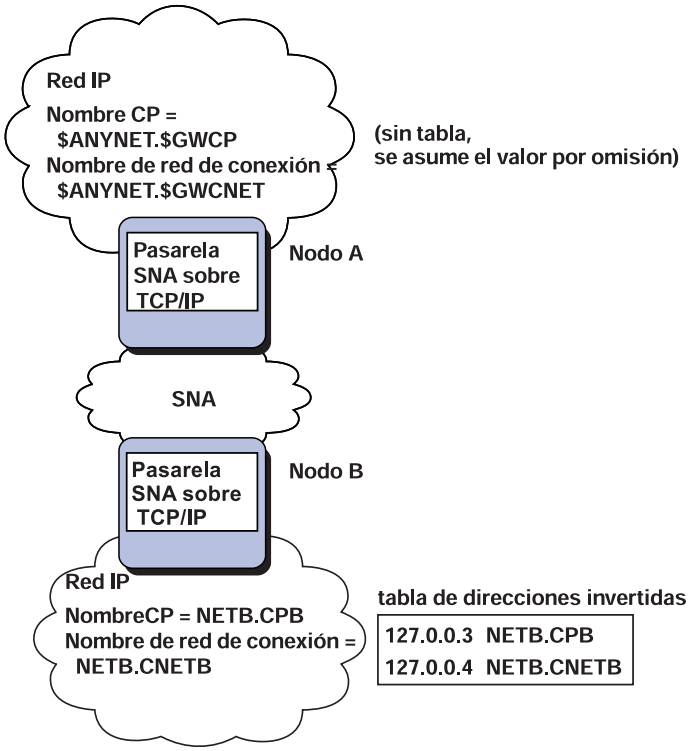


Figura 21. Definición de un nombre de CP y un nombre de red de conexión

Utilización de la entrada comodín para reducir las definiciones del servidor de nombres de dominio

Si está utilizando la pasarela SNA sobre TCP/IP y la configuración cumple con las siguientes restricciones de denominación, puede reducir el número de entradas del servidor de nombres de dominio definiendo una entrada de nombre de dominio para cada ID de red SNA que pueda accederse a través de una o varias pasarelas SNA sobre TCP/IP.

- Cada red SNA debe tener un ID de red SNA que sea exclusivo entre todas las redes SNA.
- Cada red IP debe tener un ID de red SNA que sea exclusivo entre todas las redes IP.
- Una red SNA y una red IP pueden tener el mismo ID de red SNA.

Mediante la codificación de una sola entrada de nombre de domino para cada ID de red SNA, es posible que no tenga que definir una entrada de nombre de dominio para cada LU de la red SNA con la que desee comunicarse en la red IP. Puede utilizar una entrada comodín (*) para especificar el nombre de LU de todas las LU que tengan el mismo ID de red SNA. Mediante la sustitución del *nombrelu* por una entrada comodín, se define una sola entrada de servidor de nombres de dominio que representa a todas las LU de esa red en particular.

Nota: Si utiliza la entrada comodín, debe utilizar todo el comodín. No son válidos los comodines parciales como, por ejemplo, LUA*.

La entrada comodín se correlaciona con la dirección IP de la primera pasarela SNA sobre TCP/IP utilizada para llegar a la red con ese ID de red SNA. Tal como se muestra en la Figura 22 en la página 78, las unidades lógicas SNAAPPL1,

APPC1, APPC2 y LU5 residen en la red NETB y solo se puede llegar a ellas desde la red IP a través de una pasarela SNA sobre TCP/IP con la dirección IP IPgwg. Si el sufijo de nombre de dominio SNA es SNA.IBM.COM, se define la siguiente entrada en el servidor de nombres de dominio:

```
*.NETB.SNA.IBM.COM        IPgwg
```

Esta entrada se utiliza para las cuatro unidades lógicas.

Nota: Tiene la opción de definir cada unidad lógica individualmente.

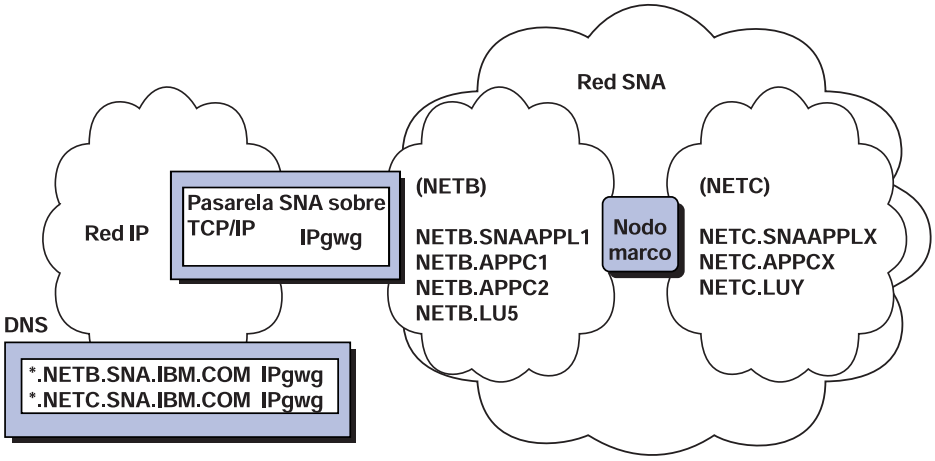


Figura 22. Definiciones del servidor de nombres de dominio para una sola pasarela conectada a una red SNA con dos ID de red

Cada red SNA debe tener una entrada exclusiva. Tal como se muestra en la Figura 22, si también tiene SNAAPPLX, APPCX y LUY en la red NETC, a la que sólo puede llegarse a través de la pasarela SNA sobre TCP/IP con la dirección IP IPgwg, las entradas del servidor de nombres de dominio son las siguientes:

```
*.NETB.SNA.IBM.COM        IPgwg
*.NETC.SNA.IBM.COM        IPgwg
```

Además, cada pasarela debe tener una entrada exclusiva. Si añade una pasarela SNA sobre TCP/IP paralela, tal como se muestra en la Figura 23 en la página 79, con la dirección IP IPgwh al ejemplo anterior, las entradas del servidor de nombres del dominio son las siguientes:

```
*.NETB.SNA.IBM.COM        IPgwg
*.NETC.SNA.IBM.COM        IPgwg
*.NETB.SNA.IBM.COM        IPgwh
*.NETC.SNA.IBM.COM        IPgwh
```

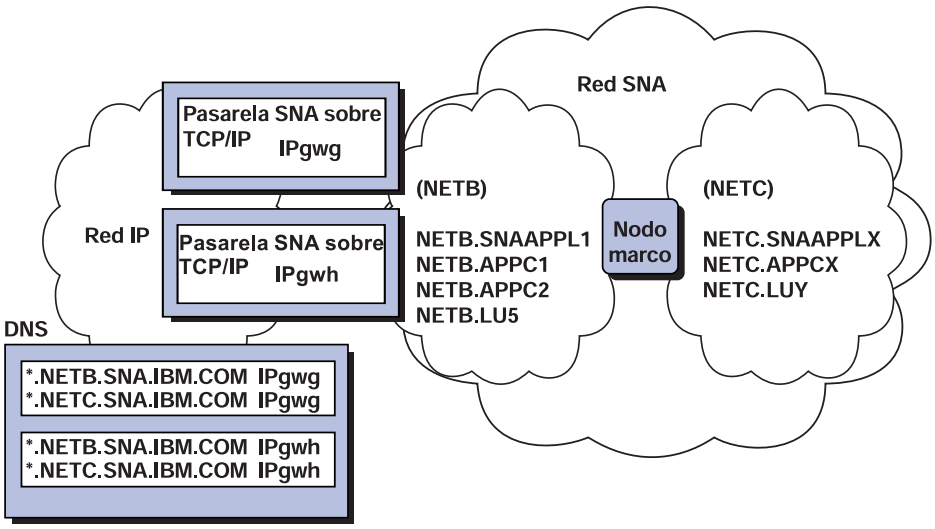


Figura 23. Definiciones del servidor de nombres de dominio para pasarelas paralelas conectadas a una red SNA con dos ID de red

Consideraciones de la función del nodo de acceso SNA sobre TCP/IP

La siguiente información sólo pertenece a los nodos de acceso y no a las pasarelas.

Cómo direccionar las sesiones SNA en AnyNet SNA sobre TCP/IP

Cuando una aplicación SNA inicia una sesión, Communications Server debe determinar primero el transporte que va a utilizar - SNA, IP o una combinación de los dos.

El transporte preferido se configura estableciendo la prioridad de direccionamiento. La prioridad de direccionamiento puede establecerse para todo el nodo a través de la prioridad de direccionamiento por omisión en el dispositivo AnyNet sobre TCP/IP o en base a la LU cuando se definen las LU asociadas.

La tabla de prioridades de direccionamiento sólo se utiliza para las sesiones nuevas. Las sesiones existentes previamente utilizan el mismo transporte; no se desactivan y vuelven a direccionar si se cambia la tabla de prioridades de direccionamiento.

Nota: La prioridad de direccionamiento para un nodo solo rige en las sesiones que se inician desde el nodo (sesiones de nodo de acceso). Las sesiones que pasan por un nodo no se ven afectadas por la prioridad de direccionamiento.

Puede establecer, o modificar, las prioridades de direccionamiento siguientes:

Nativo primero Las peticiones se direccionan sobre SNA. Si no hay ninguna ruta SNA disponible, las peticiones se direccionan sobre TCP/IP.

No nativo primero Las peticiones se direccionan sobre TCP/IP. Si no hay ninguna ruta TCP/IP disponible, las peticiones se direccionan sobre SNA.

Sólo nativo Las peticiones sólo se direccionan sobre SNA. Si no hay ninguna ruta SNA disponible, las peticiones fallarán.

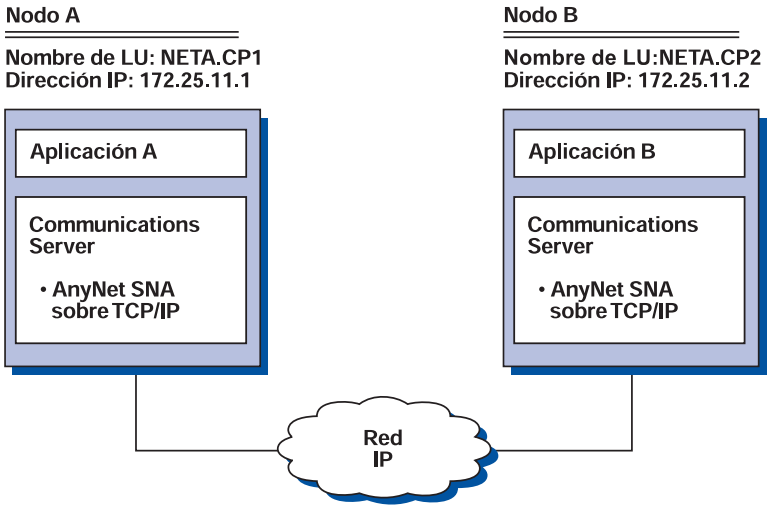
Sólo no nativo Las peticiones sólo se direccionan sobre TCP/IP. Si no hay ninguna ruta TCP/IP disponible, las peticiones fallarán.

Ejemplos de configuración AnyNet SNA sobre TCP/IP

Esta sección incluye ejemplos de AnyNet que permiten la comunicación SNA sobre IP. Las siguientes instrucciones de configuración sólo se completan para el sistema operativo Windows NT. En todos los ejemplos, el sufijo de nombre de dominio SNA es SNA.IBM.COM.

Para obtener más información acerca de la configuración de AnyNet para cualquier otra plataforma mencionada en esta sección (como, por ejemplo, VTAM o AS/400), consulte la documentación adecuada del producto.

Ejemplo 1. Ejecución de aplicaciones APPC o CPI-C sobre una red TCP/IP



Pasos

Siga estos pasos para establecer las comunicaciones entre dos nodos Windows NT. Tenga en cuenta que en este ejemplo, los nombres de CP se utilizan como nombres de LU.

Para el Nodo A, haga lo siguiente:

1. Añada la siguiente entrada al archivo HOSTS local:

   ```
   172.25.11.2  CP2.NETA.SNA.IBM.COM
   ```

2. Utilice **NETA.CP1** como el nombre de punto de control durante la configuración del nodo. Asegúrese de que la prioridad de direccionamiento está establecida en direcccionar las sesiones sobre TCP/IP. Consulte los paneles de ayuda de **Configuración de nodos** para obtener más información.

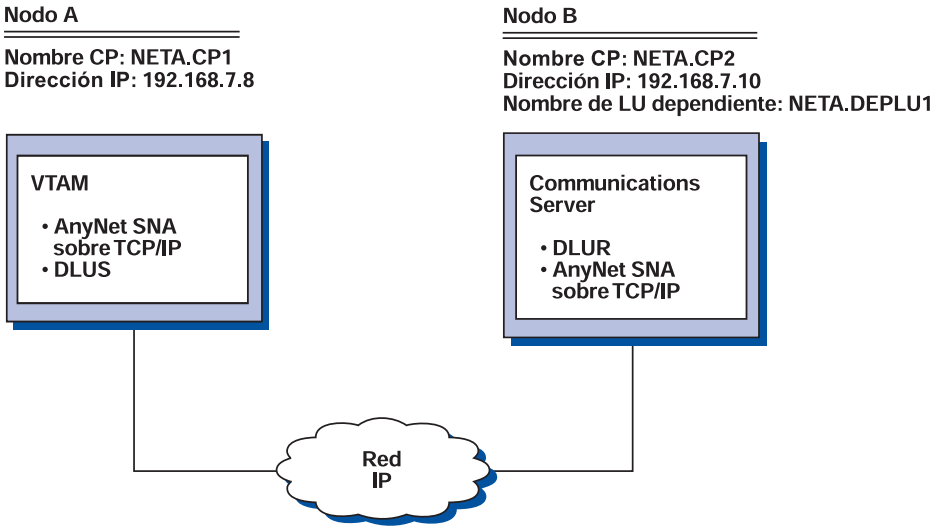
Para el nodo B, haga lo siguiente:

1. Añada la siguiente entrada al archivo HOSTS local:

   ```
   172.25.11.1  CP1.NETA.SNA.IBM.COM
   ```

2. Utilice **NETA.CP2** como el nombre de punto de control durante la configuración del nodo. Asegúrese de que la prioridad de direccionamiento está establecida en direcccionar las sesiones sobre TCP/IP. Consulte los paneles de ayuda de **Configuración de nodos** para obtener más información.

Ejemplo 2. Emulación 3270 a través de DLUR en una red TCP/IP



Pasos

Siga estos pasos para establecer la comunicación entre el Nodo A y el Nodo B.

Para el nodo B, haga lo siguiente:

1. Añada la siguiente entrada al archivo HOSTS local:

```
192.168.7.8    CP1.NETA.SNA.IBM.COM
```

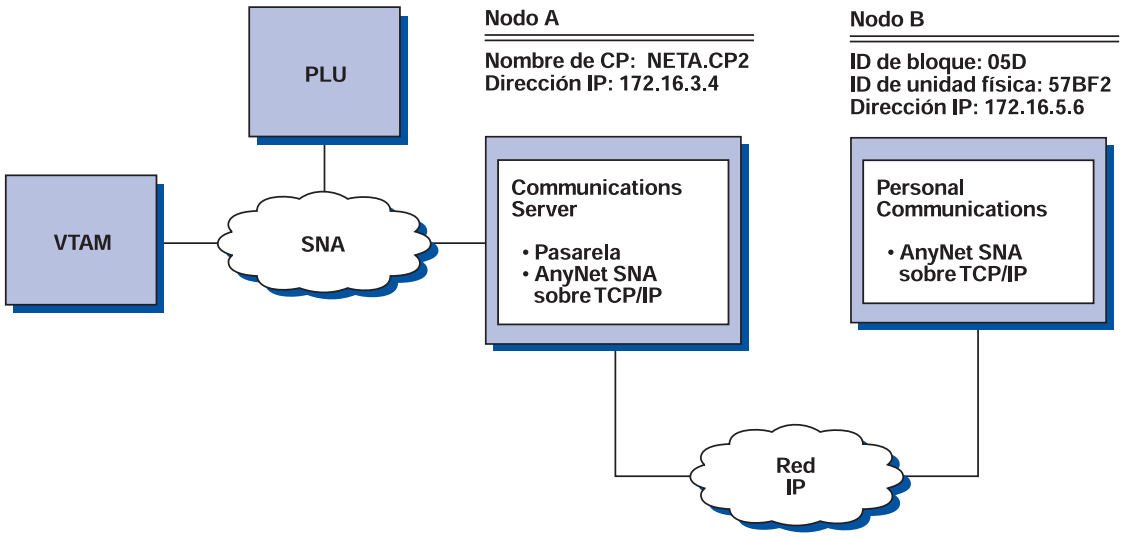
2. Utilice **NETA.CP2** como el nombre de punto de control durante la configuración del nodo y **NETA.CP1** como el nombre de DLUS cuando configure las PU DLUR. Asegúrese de que la prioridad de direccionamiento está establecida en direcccionar las sesiones sobre TCP/IP. Consulte los paneles de ayuda de **Configuración de nodos** para obtener más información.

Para el Nodo A, añada las entradas siguientes al archivo HOSTS:

```
192.168.7.10    CP2.NETA.SNA.IBM.COM
192.168.7.10    DEPLU1.NETA.SNA.IBM.COM
```

Tenga en cuenta que actualmente MVS AnyNet SNA sobre TCP/IP necesita DLUS/DLUR para la comunicación con LU dependiente.

Ejemplo 3. Utilización de una pasarela SNA para permitir la emulación 3270 entre redes SNA y TCP/IP



Pasos

Siga estos pasos para establecer las comunicaciones entre el Nodo B y el sistema principal VTAM.

Para el Nodo A, haga lo siguiente:

1. Añada la siguiente entrada al archivo HOSTS local:

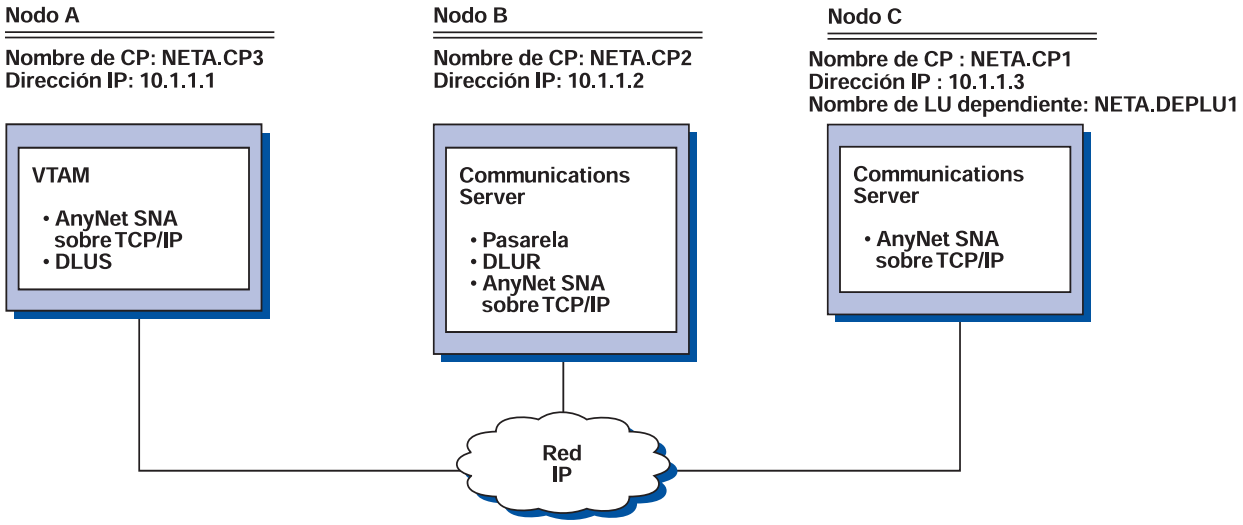
   ```
   172.16.5.6 05D57BF2.SNA.IBM.COM
   ```

2. Utilice **NETA.CP2** como el nombre de punto de control durante la configuración del nodo y utilice el dispositivo ANYNET para asignar plantillas implícitas al definir clientes. Consulte los paneles de ayuda de **Configuración de nodos** para obtener más información.

Para el Nodo B, añada lo siguiente al archivo HOSTS local:

```
172.16.3.4  CP2.NETA.SNA.IBM.COM
```

Ejemplo 4. Utilización de una pasarela SNA para la emulación 3270 en una red TCP/IP



Pasos

Siga estos pasos para establecer las comunicaciones entre el Nodo C y el Nodo A.

Para el nodo B, haga lo siguiente:

1. Añada la siguiente entrada al archivo HOSTS local:

   ```
   10.1.1.3  CP1.NETA.SNA.IBM.COM
   ```

2. Utilice **NETA.CP2** como el nombre de punto de control durante la configuración del nodo, **NETA.CP1** como el nombre de CP adyacente cuando defina la definición de conexión de AnyNet SNA sobre TCP/IP y **NETA.CP3** como el nombre de DLUS cuando asigne el DLUS a una plantilla de cliente. Asegúrese de que la prioridad de direccionamiento está establecida en no nativa NETA.CP3. Consulte los paneles de ayuda de **Configuración de nodos** para obtener más información.

Para el Nodo C, haga lo siguiente:

1. Añada la siguiente entrada al archivo HOSTS:

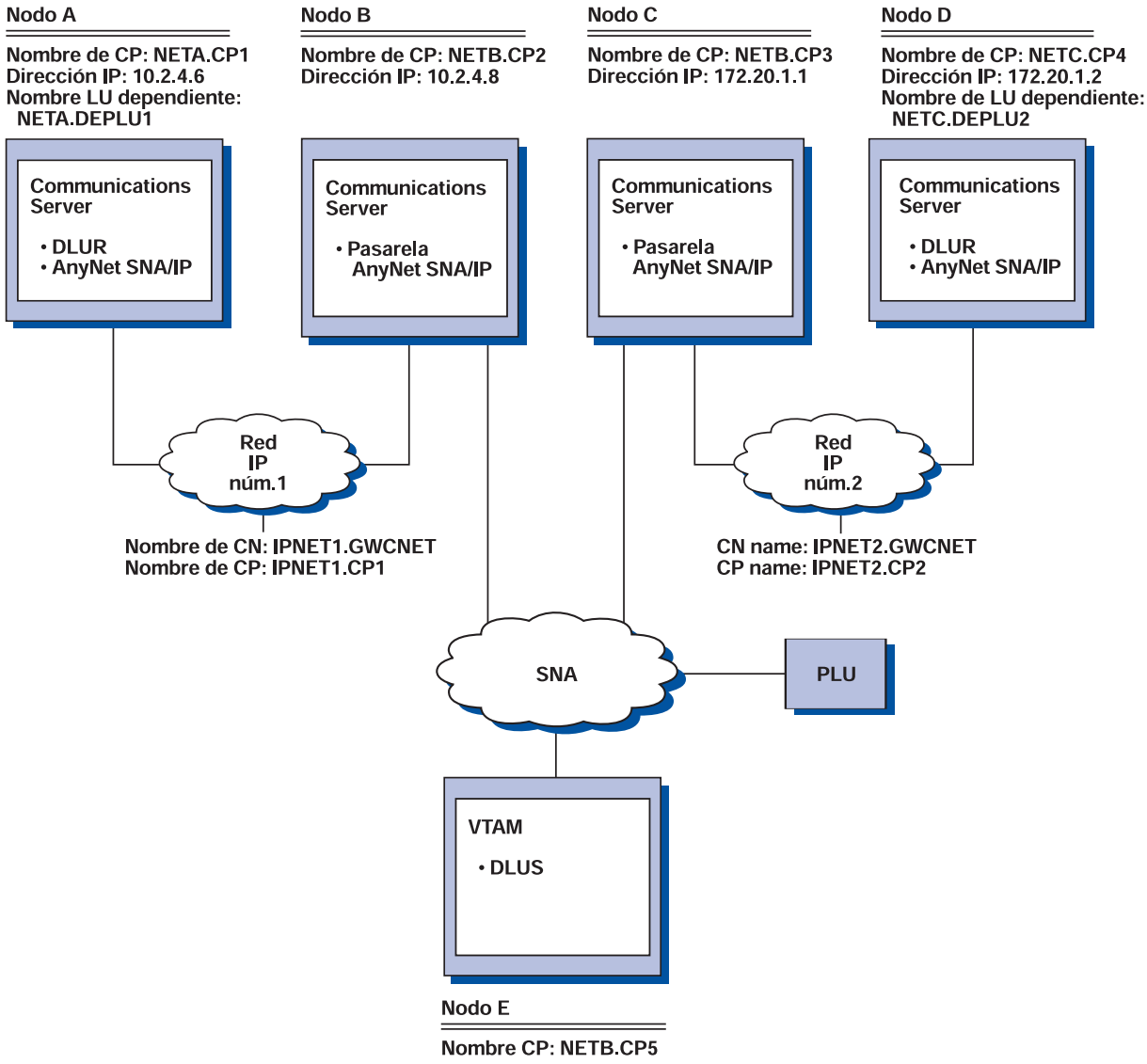
   ```
   10.1.1.2    CP2.NETA.SNA.IBM.COM
   ```

2. Utilice **NETA.CP1** como el nombre de punto de control durante la configuración y **NETA.CP2** como el nombre de CP adyacente al definir la definición de conexión de AnyNet SNA sobre TCP/IP. Consulte los paneles de ayuda de **Configuración de nodos** para obtener más información.

Para el Nodo A, añada la siguiente entrada en el archivo HOSTS:

```
10.1.1.2   CP2.NETA.SNA.IBM.COM
10.1.1.2   DEPLU1.NETA.SNA.IBM.COM
```

Ejemplo 5. Emulación 3270 desde dos estaciones de trabajo Windows NT en distintas redes IP



Pasos

Siga estos pasos para establecer las comunicaciones desde los Nodos A y D con el Nodo E.

Para el Nodo A, haga lo siguiente:

1. Añada las siguientes entradas al archivo HOSTS local:

```
10.2.4.8    CP5.NETB.SNA.IBM.COM
127.0.0.4   IPNET1.GWCNET
127.0.0.3   IPNET1.CP1
```

2. Utilice **NETA.CP1** como el nodo de punto de control durante la configuración del nodo y **NETB.CP5** como el nombre DLUS cuando configure PU de DLUR. Asegúrese de que la preferencia de direccionamiento para NETB.CP5 está

establecida en no nativo. Consulte los paneles de ayuda de **Configuración de nodos** para obtener más información.

Para el Nodo B, añada las siguientes entradas al archivo HOSTS:

```
10.2.4.6    CP1.NETA.SNA.IBM.COM
127.0.0.2   DEPLU1.NETA.SNA.IBM.COM
10.2.4.6    DEPLU1.NETA.SNA.IBM.COM
127.0.0.4   IPNET1.GWCNET
127.0.0.3   IPNET1.CP1
```

Para el Nodo C, añada las siguientes entradas al archivo HOSTS:

```
172.20.1.2  CP4.NETC.SNA.IBM.COM
127.0.0.2   DEPLU2.NETC.SNA.IBM.COM
172.20.1.2  DEPLU2.NETC.SNA.IBM.COM
127.0.0.4   IPNET2.GWCNET
127.0.0.3   IPNET2.CP2
```

Para el Nodo D, haga lo siguiente:

1. Añada la siguiente entrada al archivo HOSTS local:

   ```
   172.20.1.1  CP5.NETB.SNA.IBM.COM
   127.0.0.4   IPNET2.GWCNET
   127.0.0.3   IPNET2.CP2
   ```

2. Utilice **NETC.CP4** como el nodo de punto de control durante la configuración del nodo y **NETB.CP5** como el nombre DLUS cuando configure las PU DLUR. Asegúrese de que la prioridad de direccionamiento para NETB.CP5 está establecida en no nativo. Consulte los paneles de ayuda de **Configuración de nodos** para obtener más información.

Sugerencias de ayuda

Esta sección contiene sugerencias de ayuda sobre el ajuste, conectividad TCP/IP vía SLIP o PPP y direcciones IP dinámicas.

Ajuste

Si puede acceder a una LU a través de múltiples pasarelas SNA sobre TCP/IP y ha correlacionado ese nombre de LU con múltiples direcciones IP, aumente los parámetros **CONN_RETRY_SECS** y **CONNWAIT_SECS** de la palabra clave **ANYNET_COMMOM_PARAMETERS** al configurar los parámetros básicos de AnyNet. Esto asegura que se intentarán las conexiones TCP con todos los adaptadores y pasarelas posibles. Puede tardar más de 90 segundos que una conexión TCP falle con una dirección IP inactiva.

Direcciones IP dinámicas

Generalmente, AnyNet SNA sobre TCP/IP depende de recursos SNA (por ejemplo, nombres de LU, nombres de CP o idblk/num) que están correlacionados estáticamente con direcciones IP. Sin embargo, según la configuración y la forma en que se inician las conexiones, es posible que pueda utilizar AnyNet SNA sobre TCP/IP en entornos en que las direcciones IP se asignan dinámicamente (por ejemplo, DHCP).

Aplicaciones APPC o CPIC: Un nodo de acceso SNA sobre TCP/IP con una dirección IP asignada dinámicamente siempre puede iniciar sesiones con otro nodo de acceso o pasarela SNA sobre TCP/IP con una dirección IP estática.

La única forma de que un nodo de acceso o pasarela SNA sobre TCP/IP con una dirección IP estática (nodo A) pueda iniciar una sesión con un asociado con una dirección IP dinámica (nodo B) es que:

1. El nodo B haya iniciado primero una sesión con el nodo A o a través suyo.
2. La sesión que se ha iniciado en el Paso 1 siga activa.

Aplicaciones de LU dependiente

Nota: La información de esta sección se aplica a aplicaciones de LU 0, 1, 2, 3 o 6.2 dependiente.

Los nodos de acceso SNA sobre TCP/IP con direcciones IP asignadas dinámicamente pueden dar soporte a comunicaciones de LU dependiente si se cumplen los siguientes criterios:

- La comunicación de la LU dependiente se produce a través de una pasarela SNA a través de:
  - Communications Server/2 4.1 con el APAR JR10461 aplicado
  - Communications Server/2 V5
  - Communications Server para Windows NT 5.01 o superior
- El nodo de acceso SNA sobre TCP/IP con una dirección IP asignada dinámicamente inicia las conexiones con una pasarela SNA con una dirección IP estática.

La comunicación de la LU dependiente a través de DLUS/DLUR en AnyNet SNA sobre TCP/IP no está soportada si el nodo DLUR tiene una dirección IP asignada dinámicamente.

Configuración de AnyNet Sockets sobre SNA

Esta sección contiene información acerca de cómo configurar Sockets sobre SNA.

La función del nodo de acceso Sockets sobre SNA de Communications Server permite que las aplicaciones que cumplen con WinSock se comuniquen en redes SNA. La función de la pasarela Sockets sobre SNA permite que se comuniquen las aplicaciones de socket de las redes SNA e IP.

¿Cómo funciona Sockets sobre SNA?

La Figura 24 en la página 87 muestra la estructura de un nodo Windows NT que se ejecuta en Sockets sobre SNA e ilustra la forma en que los programas de aplicación de socket y Sockets sobre SNA funcionan en un nodo Windows NT.

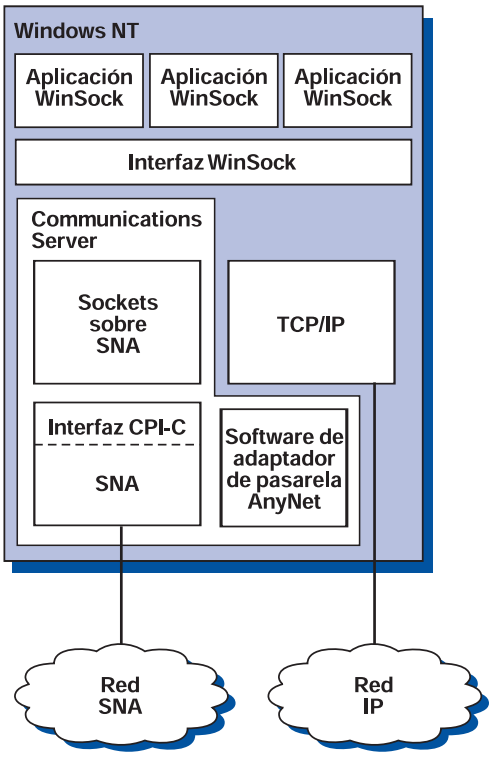


Figura 24. Estructura de un nodo Windows NT que ejecuta Sockets sobre SNA

WinSock es una API que permite que las aplicaciones de socket se ejecuten en un entorno Windows.

Sockets sobre SNA no proporciona una interfaz WinSock y no procesa las llamadas a socket. En su lugar, las aplicaciones WinSock utilizan la interfaz WinSock de la pila TCP/IP nativa. El código de la pasarela Sockets sobre SNA permite que estas aplicaciones se comuniquen en la red SNA.

La pasarela Sockets sobre SNA permitirá que las aplicaciones de socket que se ejecutan en una red IP se comuniquen con aplicaciones de socket que se ejecutan en nodos Sockets sobre SNA. Esto se consigue direccionando los paquetes entre las redes SNA e IP y transformándolas entre los protocolos SNA e IP. El controlador de dispositivo de la pasarela AnyNet ayuda en el direccionamiento de paquetes entre redes TCP/IP SNA, y el código de Sockets sobre SNA realiza la conversión entre los dos protocolos.

Generación de una llamada a LU 6.2 desde una llamada a socket

Para permitir que la información formateada en TCP/IP se direccione en SNA, Sockets sobre SNA correlaciona las direcciones IP con los nombres de LU calificados por la red SNA. Cuando un programa de aplicación invoca Sockets sobre SNA para establecer una conexión de corriente con otro programa de aplicación, Sockets sobre SNA establece dos conversaciones semidúplex de LU 6.2 para la conexión de corriente.

Sockets sobre SNA establece una conversación LU 6.2 para todos los datagramas enviados a un solo destino. Las conversaciones dedicadas al tráfico de datagramas se desasignan si no se utilizan durante el período de tiempo especificado.

Correlación de una dirección IP con un nombre calificado por la red SNA

Cuando un programa de aplicación invoca Sockets sobre SNA para comunicarse con otro programa de aplicación, suministra la dirección IP del nodo de destino. Sockets sobre SNA debe correlacionar la dirección IP con una dirección SNA para emitir una llamada a LU 6.2 adecuada. Para cada dirección IP que identifica un nodo, habrá un nombre calificado por la red SNA correspondiente.

La “Visión general de direccionamiento y correlación” en la página 89 explica la forma en que funciona la correlación de direcciones y proporciona directrices y requisitos para la preparación de la correlación de direcciones IP-LU.

Direccionamiento y correlación de datos en redes SNA e IP

Las pasarelas Sockets sobre SNA permiten la comunicación entre programas de aplicación de socket en redes IP y SNA combinando la función de direccionamiento de TCP/IP con las posibilidades de conversión de protocolo y de correlación de direcciones de Sockets sobre SNA.

La conversión de protocolo y la correlación de direcciones son necesarias cuando los datos se direccionan entre nodos que utilizan distintos protocolos de transporte. La pasarela Sockets sobre SNA realiza automáticamente la conversión de protocolo después de determinar el tipo de transporte asociado con la dirección IP de destino. Para ver un resumen del proceso de direccionamiento y de correlación, consulte el apartado “Cómo la pasarela Sockets sobre SNA direcciona y correlaciona los datos” en la página 91.

Soporte del programa de aplicación proporcionado por Sockets sobre SNA

Sockets sobre SNA da soporte a las aplicaciones WinSock 1.1 y WinSock 2.0 (sólo en Windows NT 4.0) que utilizan los sockets AF_INET.

Sockets sobre SNA no da soporte a las aplicaciones que utilizan la difusión.

Si intenta utilizar la pasarela Sockets sobre SNA para direccionar la información a un nodo MVS/ESA o desde el mismo, configurado con la función VTAM V3R4.2 Sockets sobre SNA, primero debe instalar la función `direccionar` en el nodo MVS/ESA. Para instalar la función `direccionar` en MVS/ESA, instale el arreglo temporal del programa (PTF) UW03567. Los PTF se pueden obtener en estas fuentes:

- Acceso de información
- SoftwareXcel Extended
- IBMLink (ServiceLink)

Si no tiene acceso a estas fuentes, póngase en contacto con el Centro de soporte IBM.

Planificación de Sockets sobre SNA

Esta sección describe los puntos a tener en cuenta por el planificador de la red antes de configurar una red con Sockets sobre SNA.

Visión general de direccionamiento y correlación

Esta sección explica los conceptos básicos del direccionamiento en Internet y cómo se relacionan estos conceptos con el direccionamiento y la correlación. Incluye la siguiente información:

Direccionamiento en Internet

Se asigna a cada sistema principal un mínimo de una dirección de Internet Protocol (IP), que se utiliza para direccionar los datos a través de la red.

Nota: En el conjunto de protocolos IP, ***sistema principal*** hace referencia a un sistema final y puede ser cualquier estación de trabajo; no tiene que ser necesariamente un sistema principal.

La dirección IP asignada al sistema principal no define ningún sistema principal en la red; define una interfaz de red en ese sistema principal para una red. Por ejemplo, la dirección de la interfaz de red SNA identifica la conexión de un nodo con la red SNA.

Un sistema principal de pasarela tiene una dirección IP exclusiva para cada interfaz de red. Puesto que la pasarela Sockets sobre SNA direcciona los datos SNA y TCP/IP, debe configurar direcciones IP exclusivas para las interfaces TCP/IP y SNA.

La sección siguiente describe el formato de dirección IP, las clases de dirección y las máscaras de red. Para obtener información más detallada, consulte la documentación TCP/IP.

Formato y clases de dirección IP: Una dirección IP consta de un campo de dirección de 32 bits, dividido en dos partes:

- La primera parte del campo de dirección contiene la dirección de red; la segunda parte contiene la dirección de sistema principal.
- El número de bits utilizados para las partes correspondientes a la red y al sistema principal de una dirección IP son variables, según la clase de la dirección IP.
- Una máscara de red le permite utilizar la parte correspondiente al sistema principal de la dirección IP como dirección de subred.

Las máscaras de red por omisión se muestran en la Tabla 5 en la página 90.

Tabla 5. Máscaras de dirección IP soportadas por Sockets sobre SNA

Para una dirección IP decimal con puntos en el formato *a.b.c.d*, el rango de valores para *a* es:	**Máscara de red por omisión**
1–127	255.0.0.0
128–191	255.255.0.0
192–223	255.255.255.0

Máscaras utilizadas por Sockets sobre SNA: Sockets sobre SNA utiliza dos tipos de máscaras:

- **Máscara de subred**

  La máscara de subred se utiliza en el direccionamiento y se especifica durante la configuración del nodo local y las rutas. Puede aceptar la máscara de subred por omisión o especificar un valor distinto al valor por omisión para definir las direcciones de subred.

- **Máscara de dirección**

  La máscara de dirección se utiliza para la correlación de la dirección IP-LU generada y se especifica durante la configuración.

Tabla de direccionamiento IP

Cada sistema principal tiene su tabla de direccionamiento IP que almacena información acerca de los posibles destinos y cómo llegar a ellos. Las entradas de ruta se añaden cuando:

- Se define la dirección IP local. Para obtener más información, consulte la ayuda en línea.
- Las sentencias de ruta se definen en la ventana **Configuración de nodos**. Pulse **Configurar AnyNet Sockets** y, a continuación, pulse **Rutas**. Para obtener más información, consulte la ayuda en línea.
- Se encuentra una ruta con menos saltos. Esto ocurre cuando la pasarela Sockets sobre SNA recibe una redirección ICMP o un mensaje RIP. Para obtener más información, consulte el apartado “Función de descubrimiento de ruta” en la página 92.

Para ver un ejemplo de tabla de direccionamiento, consulte la Figura 25 en la página 91.

ID de red SNA utilizado por Sockets sobre SNA

Para cada ruta que defina a través de la interfaz SNA (sna0), debe haber un ID de red SNA correspondiente con el que se correlaciona la dirección de red IP. El número de ID de red SNA que defina depende de cómo desee correlacionar la red IP con la red SNA.

Por ejemplo, si las aplicaciones de socket que utilizan SNA están configuradas para utilizar las subredes IP 9.67.0.0 y 9.77.0.0, puede definir un ID de red SNA que corresponda a cada subred IP, o puede definir un ID de red SNA que corresponda a ambas subredes. Sockets sobre SNA no necesita una correlación exclusiva de una dirección de red IP y un ID de red SNA.

Cómo se correlaciona una dirección IP con un nombre de LU

Puede utilizar la correlación explícita o generada para correlacionar direcciones IP con nombres de LU SNA:

- En la correlación explícita, todos los nombres de LU están definidos y se asigna cada dirección de sistema principal IP a un nombre de LU SNA específico durante la configuración.
- En la correlación generada, los nombres de LU se generan automáticamente. Durante la configuración, se especifica una dirección IP de red, una máscara de dirección, un ID de red y un valor de plantilla de LU.

  Sockets sobre SNA utiliza la máscara de red para correlacionar la parte correspondiente a la red de la dirección IP con el ID de red SNA y la parte correspondiente al sistema principal con el nombre de LU SNA. El valor de plantilla de LU se utiliza para determinar los caracteres y las posiciones de los caracteres utilizados en el nombre de LU.

  Puede visualizar el nombre de LU generado para una dirección IP determinada utilizando el programa de utilidad de línea de mandatos **sxmap**. La sintaxis para este programa de utilidad es:

  ```
  sxmap convert <dirección IP> <máscara de dirección> <plantilla de LU>
  ```

Cómo la pasarela Sockets sobre SNA direcciona y correlaciona los datos

Los pasos siguientes describen brevemente la forma en que la pasarela Sockets sobre SNA determina si ha de direccionar los datos sobre SNA o sobre TCP/IP, y cómo se maneja la correlación de direcciones:

1. Sockets sobre SNA busca en su tabla de direccionamiento para encontrar una ruta que permita que los datos alcancen la dirección IP de destino. Si Sockets sobre SNA no encuentra ninguna ruta coincidente, la petición de conexión se reenvía a la pila TCP/IP nativa.
2. Si Sockets sobre SNA encuentra una ruta coincidente, la entrada de ruta indica la forma en que se puede llegar al destino:
   a. Si la dirección del direccionador es la de una interfaz de red local como, por ejemplo, sna0, se puede llegar directamente a la red de destino, subred o dirección de sistema principal.
   b. Si la dirección del direccionador es la de una pasarela o direccionador, sólo se puede llegar al destino a través de esa pasarela o direccionador intermedio.

   La Figura 25 muestra un ejemplo de una tabla de direccionamiento IP.

```
Direcc. IP de destino     Máscara destino     Direcc. IP destino   Cta. utiliz.
-------------------------------------------------------------------------------
1.2.3.4                   255.255.255.255     199.245.253.1        10
10.0.0.0                  255.0.0.0           199.245.253.2        0
10.11.0.0                 255.255.0.0         199.245.253.113      37
127.0.0.1                 255.255.255.255     127.0.0.1            8
128.1.0.0                 255.255.0.0         199.245.253.3        0
199.245.253.0             255.255.255.0       199.245.253.113      368
```

Figura 25. Panel de ejemplo de un direccionamiento IP

3. Si no se encuentra ninguna ruta en la tabla de direccionamiento de Sockets sobre SNA, Sockets sobre SNA supone que el destino TCP/IP puede alcanzarse a través de una red IP nativa. Consulte la documentación TCP/IP para obtener más información sobre cómo TCP/IP direcciona los datos.
4. Si la ruta elegida indica que los datos deben pasar por la interfaz SNA (sna0), Sockets sobre SNA busca la dirección del siguiente salto en la tabla de correlación IP-LU:
   a. Si Sockets sobre SNA encuentra una entrada coincidente, se establece una conexión de LU 6.2.
   b. Si Sockets sobre SNA no encuentra ninguna entrada coincidente, el intento de conexión falla.
   c. Sockets sobre SNA pasa la dirección de destino y los datos a Communications Server.
5. Todas las rutas definidas para Sockets sobre SNA se duplican para la pila TCP/IP nativa de modo que se puedan direccionar los paquetes de IP sobre SNA.

Función de descubrimiento de ruta: La función de descubrimiento de ruta proporcionada por la pasarela Sockets sobre SNA puede ayudarle a direccionar el tráfico TCP/IP más eficazmente y reducir el número de sentencias de rutas definidas explícitamente en la red. No tiene que seleccionar ni configurar esta función.

Uno de los problemas que surgen en redes grandes es cómo descubrir la adición de nuevas redes o subredes y qué direccionador se ha de utilizar para obtener la nueva red o subred. Sockets sobre SNA resuelve este problema haciendo que todos los nodos utilicen inicialmente un direccionador por omisión que notifica a los demás nodos cuándo se descubre una ruta más directa. Esto es más eficaz que utilizar la típica solución de TCP/IP de difundir la información de direccionamiento.

Nota: Para utilizar de manera eficaz esta función, debe utilizarse la correlación algorítmica de las direcciones IP con los nombres de LU y una red principal APPN. De lo contrario, los nodos deben definir explícitamente los nombres de LU y las direcciones IP para todos los nodos remotos con los que se comunican.

La Figura 26 muestra un ejemplo de configuración.

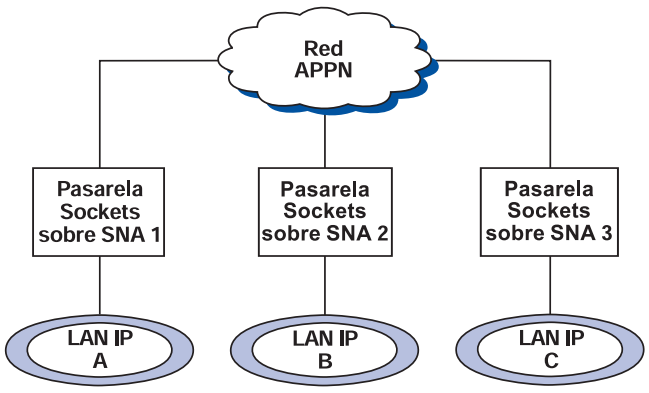


Figura 26. Ejemplo de red que utiliza la función de descubrimiento de ruta de Sockets sobre SNA

En este escenario:

- Las pasarelas 1, 2 y 3 son pasarelas Sockets sobre SNA conectadas a las LAN IP. Estas pasarelas conectan las LAN IP a una red principal APPN.
- La pasarela 1 es la única pasarela en la que se puede mantener una tabla de direccionamiento completa y permanente.

  Las pasarelas 2 y 3 definen la Pasarela 1 como su direccionador por omisión. Si la Pasarela 1 conoce una red o subred remota, las Pasarelas 2 y 3 no tienen que definir explícitamente estas rutas.
- Cuando las Pasarelas 2 y 3 direccionan datos a redes o subredes no definidas, estas peticiones se envían a su direccionador por omisión, la Pasarela 1.

  Si la Pasarela 1 conoce la red o subred y está disponible una vía de acceso más directa, la Pasarela 1 envía un mensaje de redireccionamiento ICMP de vuelta al peticionario indicando la vía de acceso que se ha de tomar en el futuro. Este mensaje de redireccionamiento ICMP actualiza la tabla de direccionamiento del peticionario. Por lo tanto, las Pasarelas 2 y 3 construyen dinámicamente sus tablas de direccionamiento para redes y subredes remotas, según proceda.
- Si se añaden nuevas pasarelas, actualice la tabla de direccionamiento permanente de la Pasarela 1. No es necesaria ninguna sentencia de ruta explícita para las Pasarelas 2 y 3.

Definición de modalidades de Sockets sobre SNA

Sockets sobre SNA utiliza las conversaciones LU 6.2 para permitir la comunicación entre programas de aplicación de sockets. Cuando se establece una conversación LU 6.2, Sockets sobre SNA define la modalidad y las características de la sesión asociada de la conexión. Communications Server utiliza el nombre de modalidad para identificar las características de la conexión entre los dos nodos Sockets sobre SNA.

La modalidad por omisión de Sockets sobre SNA es BLANK. Puede utilizar la modalidad por omisión de Sockets sobre SNA o definir la propia. Para cambiar la modalidad de Sockets sobre SNA, en la ventana **Configuración de nodos**, pulse **Configurar AnyNet Sockets sobre SNA** y, a continuación, pulse **Modalidades**. Puede definir otra modalidad por omisión para todo el tráfico TCP/IP y asignar una modalidad específica a una puerta TCP/IP específica.

Si especifica una modalidad alternativa que no está definida por Communications Server, debe definir las características de la sesión asociada con esa modalidad en Communications Server.

Cambio del intervalo de tiempo de espera de desocupación

La opción de inicio de tiempo de espera de desocupación le permite ajustar el número de segundos desocupados antes de que Sockets sobre SNA desasigne una conversación de datagramas. Este intervalo le permite equilibrar la utilización de los recursos del sistema para mantener una conversación de datagramas existente y el tardar más en restablecer una nueva conversación de datagramas. Por ejemplo, si establece este valor bajo, las conversaciones de datagramas no utilizadas finalizan más pronto, pero se tarda más en enviar el siguiente datagrama. El intervalo de tiempo de espera de desocupación por omisión es de 90 segundos.

Para modificar la opción de inicio, en la ventana **Configuración de nodos**, pulse **Configurar AnyNet Sockets sobre SNA** y, a continuación, pulse **Ver/Cambiar/Añadir**, pulse la pestaña **Avanzados** y seleccione un nuevo valor para esta opción.

Planificación de la comunicación cliente/servidor

Este capítulo contiene información acerca de la planificación de los clientes API SNA para Communications Server y Novell IntranetWare para SAA.

Clientes API SNA

Esta sección contiene información específica para los clientes API SNA.

Instalación y configuración

Para obtener información acerca de la instalación y configuración de clientes API SNA de Communications Server, consulte el manual *Quick Beginnings*.

Lightweight Directory Access Protocol

Lightweight Directory Access Protocol (LDAP) proporciona una manera estándar de acceder a los servicios del directorio. LDAP le permite leer, buscar, añadir y eliminar información de bases de datos centralizadas o distribuidas. LDAP es similar al anterior protocolo X.500 Directory Access Protocol (DAP), pero sin parte de su actividad general (por ejemplo, las capas OSI de sesión y presentación). Puede utilizar **Configuración de cliente LDAP** para configurar la información del cliente API SNA y almacenarla en un servidor LDAP.

Configuración de cliente LDAP muestra la organización lógica y las relaciones entre los clientes y sus configuraciones.

Para obtener más información sobre la utilización de estas áreas principales, consulte los paneles de ayuda para **Configuración de cliente LDAP**.

Árbol de información del directorio

El Árbol de información del directorio (DIT) conecta todos los Agentes de servicio del directorio (DSA) en un modelo predefinido. El modelo es una estructura jerárquica ampliable que se compone de varios objetos básicos. Un DIT LDAP típico tendrá una raíz, bajo la cual se definirán los ***países*** (c). Normalmente debajo de los países están las ***organizaciones*** (o) y debajo de cada organización están los ***individuos***, ((cn) o (uid)) o ***unidades organizativas*** (ou). Por ejemplo, una entrada LDAP completamente diferenciada se especificaría como:

```
c=US, o=compañía.com, ou=Ventas, cn=temp
```

Jerarquía de clientes

La jerarquía de clientes está en relación al DIT LDAP al que se ha conectado. Puede añadir clientes o unidades organizativas a la jerarquía de clientes o suprimir usuarios o unidades organizativas de la jerarquía de clientes.

Jerarquía de configuraciones

La jerarquía de configuraciones muestra, de manera lógica mediante una vista en árbol, la configuración del cliente y todas las relaciones entre las definiciones de configuración. La jerarquía de configuraciones le permite crear, modificar o eliminar definiciones.

© Copyright IBM Corp. 1989, 1996

Cliente API común para Communications Server para Windows NT e IntranetWare para SAA

El cliente que se suministra con Communications Server permite que los clientes localicen y accedan a los servidores IBM Communications Servers e IntranetWare for SAA (IWSAA) de la red.

Opciones de instalación para la ubicación de configuración

Durante la instalación del cliente, el usuario puede elegir la ubicación de configuración del cliente. Existen tres opciones:

- El archivo de configuración INI, que es el método utilizado en las versiones anteriores de Communications Server y es el método por omisión cuando se instala el cliente API SNA que se incluye con Communications Server
- Servicios del directorio Netware (NDS), que es el método utilizado con las versiones anteriores de IWSAA y es el método por omisión cuando se instala el cliente API SNA que se incluye con IntranetWare para SAA
- Lightweight Directory Access Protocol (LDAP)

La ubicación de configuración contiene listas de servidores, nombres de usuario y toda la demás información de configuración del cliente.

Ubicaciones de configuración

Puesto que la información de configuración es independiente del tipo de servidor (Communication Server para Windows NT o IntranetWare para SAA), la información puede almacenarse en NDS, INI o LDAP. Por ejemplo, los nombres y direcciones de los Communication Server pueden almacenarse en NDS, INI o LDAP para el cliente API. Como los programas de administración NDS sólo se suministran con IntranetWare para SAA, la configuración de la información del cliente API en NDS necesita que el producto IntranetWare para SAA exista en la red. El cliente API común le permite integrar fácilmente los distintos tipos de servidores en la misma red.

Programa de utilidad de configuración

Utilice el programa de utilidad **Establecer opciones de configuración** para cambiar la ubicación de la configuración cliente (INI, NDS o LDAP) después de la instalación.

Localización de servidores

El cliente permite al usuario localizar y acceder a los servidores IBM Communications Server e IWSAA utilizando los protocolos de transporte TCP/IP y SPX.

TCP/IP: El método utilizado para localizar los servidores utilizando el protocolo de transporte TCP/IP es idéntico. El administrador de la red puede controlar el acceso a los servidores a través de la configuración del servidor. Consulte el apartado “Planificación de ámbitos TCP/IP” en la página 146 para obtener más información.

SPX: Los métodos utilizados para localizar los servidores utilizando el protocolo de transporte SPX son diferentes. La localización de los servidores IBM Communications Server e IWSAA tarda más tiempo que la localización de servidores IBM Communications Server o IWSAA solamente.

El cliente API SNA de Communications Server intenta localizar primero los servidores IBM Communication Server y después los servidores IWSAA. Si no existe ningún servidor IWSAA en la red o no se puede acceder, el usuario puede establecer una variable de entorno para impedir la localización de servidores IWSAA. El establecimiento de la variable mejora el rendimiento en un entorno en el que sólo se accede a servidores IBM Communication Server por el protocolo de transporte SPX. La variable de entorno es **SNA_API_CLIENT_NO_CC**. El establecimiento de la variable no afecta a la localización del servidor utilizando el protocolo de transporte TCP/IP.

Asignación de una LU local por omisión

Puede asignar un alias de LU local por omisión para cada usuario mediante la configuración del archivo INI o la configuración LDAP para clientes API SNA de Windows de 32–bits.

Los programas APPC pueden utilizar un alias de LU local por omisión en lugar de especificar uno directamente. Cuando un programa APPC emite un verbo TP_START con el campo de alias de LU local establecido en ceros binarios o todo blancos ASCII, la API APPC utiliza el alias de LU local por omisión configurado.

Los programas EHNAPPC pueden utilizar un alias de LU local por omisión en lugar de especificar uno directamente. Cuando de deja en blanco el campo de LU local del panel de configuración AS/400, se utiliza el alias de LU local por omisión configurado.

Los programas CPI-C pueden utilizar un alias de LU local por omisión en lugar de especificar uno directamente. Cuando se deja en blanco el campo de alias de LU local del registro complementario CPI-C y no se ha definido ningún valor utilizando la variable de entorno APPCLLU, la API CPI-C utiliza el alias de LU local por omisión configurado al iniciar una conversación.

Los programas del Gestor de acoplamiento pueden utilizar un alias de LU local por omisión en lugar de especificar uno directamente. Cuando se deja en blanco el campo de alias de LU local del registro del gestor de acoplamiento, el Gestor de acoplamiento utiliza el alias de LU local por omisión configurado al procesar las peticiones de conversación de entrada.

Asignación de LU asociada por omisión

Puede asignar un alias de LU asociada por omisión para cada usuario mediante la configuración del archivo INI o la configuración LDAP para clientes API SNA de Windows de 32–bits.

Los programas APPC pueden utilizar un alias de LU asociada por omisión en lugar de especificar uno directamente. Cuando un programa APPC emite un verbo ALLOCATE con el campo de alias de LU asociada establecido en ceros binarios o todo blancos ASCII, la API APPC utiliza el alias de LU asociada por omisión configurado.

Los programas CPI-C pueden utilizar un alias de LU asociada por omisión en lugar de especificar uno directamente. Cuando se deja en blanco el campo de alias de LU asociada del registro complementario CPI-C, la API CPI-C utiliza el alias de LU asociada por omisión configurado al iniciar una conversación.

Asignación de un nombre de sesión LUA por omisión

Puede asignar un alias de LU asociada por omisión para cada usuario mediante la configuración del archivo INI o la configuración LDAP para clientes API SNA de Windows de 32–bits.

Los programas LUA como, por ejemplo, los emuladores 3270 pueden utilizar un nombre de sesión LU por omisión en lugar de especificar uno directamente. Cuando un programa LU emite un verbo RUI_INIT o SLI_OPEN con el campo del nombre de LU LUA establecido en ceros binarios o en todo blancos ASCII, la API RUI/SLI utiliza el nombre de sesión LUA por omisión configurado.

Cifrado de datos de cliente/servidor

El cifrado de datos de cliente/servidor permite al cliente pedir el cifrado de los datos de la aplicación en las comunicaciones entre el cliente API SNA y Communications Server.

El cifrado de datos puede estar activado, desactivado o ser opcional. El cifrado de datos opcional significa que se utiliza el cifrado si el servidor le da soporte.

Seguridad del servidor de clientes

Communications Server permite que los clientes API SNA de Windows 95 y Windows NT utilicen la seguridad del dominio Windows NT para autentificar la conexión cliente en el servidor, sin volver a entrar el id de usuario y la contraseña. El cliente debe formar parte de un dominio Windows NT, por ser partícipe de un dominio de Communications Server o por conectarse localmente con un id de usuario y una contraseña sincronizados.

Es necesario que los usuarios de clientes API SNA externos al dominio Windows NT proporcionen el id de usuario y la contraseña, a través de una solicitud o almacenando estos valores en el archivo de configuración del cliente.

Los usuarios autorizados para un servidor de clientes se mantienen en el grupo local IBMCSAPI, que está ubicado directamente en el Communications Server o en el controlador del dominio en el que Communications Server participa. Este grupo de usuarios se crea durante la instalación y puede administrarse utilizando la aplicación Administrador de usuarios de Windows NT.

Puede determinar si el id de usuario y la contraseña son necesarios para la conexión con el servidor cambiando la entrada del valor **LogonControl** en el servidor por cero (0), lo que elimina el requisito de especificar el id de usuario y contraseña por el cliente.

Se hace un seguimiento de los registros de seguimiento de comprobación de las conexiones cliente con el servidor en el Registro de sucesos de Windows NT. Puede ver los registros utilizando el Observador de sucesos de Windows NT bajo el registro **Aplicación**. Si no desea realizar un seguimiento de las conexiones cliente con el servidor, puede cambiar la entrada del valor **AuditTrail** del servidor por cero (0).

Puede acceder a las entradas de los valores **LogonControl** y **AuditTrail** a través de Windows NT Registry Editor bajo la clave:
`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/IBM SNA Client Services`.

Clientes Novell IntranetWare para SAA

Communications Server da soporte a clientes conectados por IPX o TCP/IP que ejecutan paquetes de software emulador que implanta la arquitectura Queue Element/Message Unit (QEL/MU) de Novell para la emulación 3270, permitiendo que los clientes accedan a los datos del sistema principal. Esto incluye el soporte de características de clientes conocidas, incluyendo las categorías de LU dedicadas, agrupadas y públicas (a las que algunas veces se hace referencia como tipos de recurso).

Communications Server da soporte a clientes Novell IntranetWare para SAA en Windows 95, Windows NT, Windows 3.1 y OS/2.

Es necesario TCP/IP, IPX/SPX o ambos para que los clientes Novell IntranetWare para SAA se comuniquen con Communications Server. Si está ejecutando IPX, también necesita tener habilitado el software siguiente en el servidor:

- Gateway Service para Netware
- Agente SAP
- NWLink IPX/SPX o un transporte compatible

Si Communications Server se ejecuta en un controlador primario o de reserva, los usuarios deben tener derechos de usuario en el grupo IBMCSAPI para conectarse localmente al servidor.

Planificación del acceso a datos legados

Este capítulo contiene información acerca de las funciones de Communications Server que le permiten acceder a la información del sistema principal.

AS/400 OLE DB Provider

Las aplicaciones que utilizan OLE DB o ActiveX pueden comunicarse mediante Communications Server para acceder, a nivel de registro, a los archivos de AS/400. Para acceder a archivos del AS/400 es necesario definir el AS/400 remoto, dónde están almacenados los archivos, como una LU asociada.

AS/400 OLE DB Provider puede instalarse como un componente de Communications Server o como un componente del cliente API SNA para Windows 95. También puede instalarse como un componente del cliente API SNA para Windows NT; sin embargo, necesita una estación de trabajo o servidor Windows NT 4.0 o posterior. Si no tiene instalado Microsoft Data Access Components (MDAC) Versión 1.5, Communications Server lo instalará automáticamente cuando instale este componente.

Si instala AS/400 OLE DB Provider en una máquina que ya tiene instalado Client Access Versión 3 Release 2 MD (o inferior), algunas funciones de Client Access estarán inhabilitadas, incluyendo el soporte de los programas ActiveX y OLE DB que utilizan Client Access para acceder a las colas de datos del AS/400, así como a mandatos remotos, llamadas a programas distribuidos, procedimientos almacenados y sentencias SQL del mismo.

Si desea continuar utilizando estas funciones a través de Client Access, no instale el componente AS/400 OLE DB durante la instalación de Communications Server. Si instala el componente AS/400 OLE DB Provider durante la instalación de Communications Server y desea recuperar las funciones de Client Access, puede volver a instalar Client Access. Sin embargo, si vuelve a instalar Client Access, no podrá utilizar AS/400 OLE DB Provider en Communications Server.

Cuando Client Access se instala después de Communications Server, se sobregraba la información de registro. Si desea utilizar AS/400 OLE DB Provider en Communications Server después de instalar Client Access, puede ejecutar la herramienta REGSVR32.EXE en los archivos cwbzzodb.dll y cwbzzidx.dll para restaurar la información de registro de AS/400 OLE DB Provider.

Puede utilizar AS/400 OLE DB Provider para conectar los clientes Windows 95 y Windows NT 4.0 mediante Communications Server a uno o varios AS/400, tal como se muestra en la Figura 27 en la página 102. Esta configuración proporciona a los clientes que tienen instalado AS/400 OLE DB Provider el acceso a registros específicos de los archivos del AS/400.

© Copyright IBM Corp. 1989, 1996

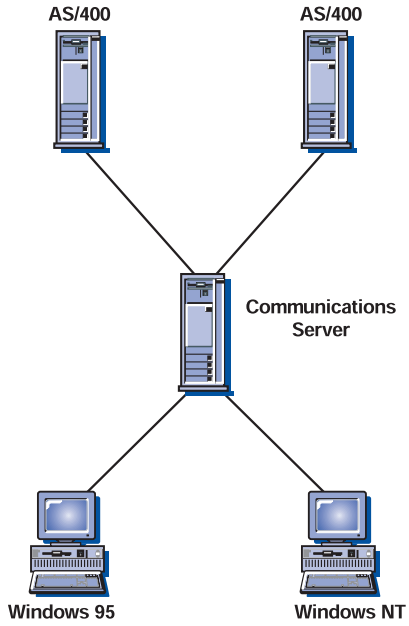


Figura 27. AS/400 OLE DB Provider

En esta figura, ambos clientes tienen instalado AS/400 OLE DB Provider. Alternativamente, puede instalar y utilizar la función desde el servidor.

La documentación de esta función, así como la información acerca del desarrollo de las aplicaciones OLE DB y ActiveX utilizando Client Access, se proporciona en el directorio `csnt\sdk\as400_oledb`.

Servidor de carpetas compartidas AS/400

Puede crear dispositivos de disco en un servidor que se comunica con carpetas AS/400 a través del Sistema de archivos integrado (IFS) de AS/400. Si el servidor comparte estos dispositivos de disco, los clientes pueden conectarse y utilizar estos dispositivos para obtener acceso a las unidades AS/400 sin ninguna configuración adicional ni instalación de código en la máquina servidora. Se pueden conectar múltiples clientes a las carpetas del sistema AS/400 como si fueran unidades de sus estaciones de trabajo.

El soporte de carpetas compartidas se habilita a través de la aplicación **Configuración de nodos**. Cuando un dispositivo de disco está disponible para el usuario, actúa como una unidad de discos soportada por el sistema. Utilice las interfaces proporcionadas por Windows NT para controlar el dispositivo. Los usuarios pueden compartir la unidad en la red, pero mantienen derechos de acceso individuales.

El servidor de carpetas compartidas AS/400 necesita OS/400 Versión 3.1 o posterior.

Editor del sistema principal

El Editor del sistema principal proporciona el acceso en la Web para los sitios de la Web de gran volumen con contenido dinámico. Puede utilizar el Editor del sistema principal para acceder a los datos de los sistemas principales S/390 o AS/400 y para publicarlos en las páginas de la Web creadas dinámicamente a partir de su propio diseño.

El Editor del sistema principal consta de varios componentes. Para ver las descripciones de los componentes e información acerca de la instalación del Editor del sistema principal, consulte la publicación en línea *Quick Beginnings*.

Tres valores de registro habilitan el control basado en el registro sobre la utilización de cualquier JIT presente y una vía de acceso específica del Editor del sistema principal. Pueden existir posibles implantaciones incompatibles de Java en la misma máquina que el Editor del sistema principal.

JITCompiler Este valor indica el nombre del compilador JIT que se ha de utilizar para la creación de instancias del Editor del sistema principal de VM. Establece la propiedad del sistema **java.compiler** que rige la forma en que VM carga y utiliza los JIT.

EnableJIT Este valor booleano indica si se utiliza el JIT especificado por **JITCompiler**.

Classpath Este valor indica la vía de acceso de clase especificada en VM. Si no se especifica el valor o se especifica como nulo, se utiliza la variable de entorno del sistema.

Puede acceder a las entradas de los valores **JITCompiler**, **EnableJIT** y **Classpath** mediante Windows NT Registry Editor bajo la clave:
`HKEY_LOCAL_MACHINE/Software/IBM/Host Publisher/Config`.

Puesto que VM Java se inicializa en la inicialización del Editor del sistema principal, el Servidor de páginas y el Integrador deben reiniciarse antes de que los cambios del registro surtan efecto.

Proceso de página web

Después de crear una biblioteca Web utilizando el **Integrador**, debe implantar la biblioteca para que los clientes puedan utilizar un navegador Web para ver la biblioteca en la Web.

Cuando un cliente pulsa en un botón de la página Web, se envía una petición desde el sistema cliente a un servidor Web. El servidor Web se pone en contacto con el **Adaptador**, que determina que la petición se asocie con una página Web dinámica que existe como un archivo de biblioteca Web en una máquina de red que aloja un **Servidor de páginas**.

El **Asignador de tareas** determina qué **Servidor de páginas** debe dar servicio a la petición y el **Adaptador** direcciona la petición al **Servidor de páginas** recomendado.

El **Servidor de páginas** localiza la página en una de sus bibliotecas y empieza el proceso de la página. Explora el archivo por si hay distintivos DYNA.

- Si se encuentran distintivos DYNA, el **Servidor de páginas** busca en la biblioteca Web para identificar la ubicación de los objetos de integración asociados con los distintivos DYNA y procesa los mandatos para extraer el contenido dinámico. El **Servidor de páginas** resuelve cualquier script correspondiente al servidor que se encuentre en la página, sustituye los distintivos DYNA por distintivos HTML que incluyen la información extraída de la fuente y devuelve la página al **Adaptador**.
- Si no se encuentra ningún distintivo DYNA, el **Servidor de páginas** crea un archivo y lo envía al **Adaptador**.

El **Adaptador** envía la página al servidor Web, que reenvía la página a la máquina del cliente.

Configuraciones del Editor del sistema principal

Puede instalar varias configuraciones del Editor del sistema principal, dependiendo de factores como, por ejemplo, la potencia de las máquinas utilizadas y el rendimiento de la fuente de datos a la que se accede.

Para una configuración básica, el servidor Web, el **Servidor de páginas**, el **Adaptador**, **Asignador de tareas** están todos en la misma máquina.

Para una configuración ampliada, debe tener un servidor Web autónomo, múltiples **Servidores de páginas** autónomos y el **Asignador de tareas** debe estar en la misma máquina que el **Servidor de páginas** o el servidor Web.

Para una configuración óptima, debe tener un servidor Web autónomo, múltiples **Servidores de páginas** autónomos, un **Asignador de tareas** primario autónomo y un **Asignador de tareas** secundario autónomo.

La Figura 28 en la página 105 muestra un ejemplo de cómo puede utilizar un navegador Web con el Editor del sistema principal para acceder a la información de una aplicación 3270 de un sistema principal.

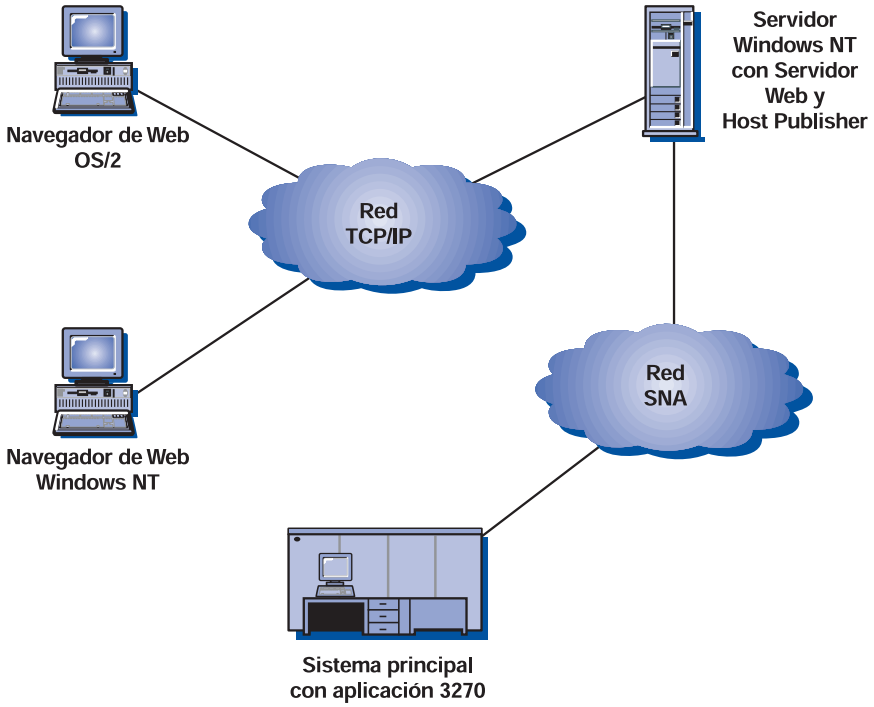


Figura 28. Editor del sistema principal y una aplicación de sistema principal integrada en un entorno Web

Configuración para aplicaciones de alta disponibilidad

Puede ampliar fácilmente el sitio Web si aumenta el volumen de actividad. Para asegurarse de que los clientes funcionan en un entorno tolerante de errores, el Editor del sistema principal le permite configurar el **Asignador de tareas** para continuar funcionando con componentes de espera.

El **Asignador de tareas** puede estar configurado para tener instancias tanto primaria como secundaria. Si el **Asignador de tareas** primario falla por alguna razón, el **Adaptador** y los **Servidores de páginas** intentan inmediatamente conectarse al **Asignador de tareas** secundario. Cada **Asignador de tareas** puede dar soporte a múltiples servidores Web

Puede reproducir las bibliotecas del Editor del sistema principal en múltiples **Servidores de páginas**. El **Asignador de tareas** trabaja con los **Servidores de páginas** para realizar el equilibrio de la carga y la asignación de recursos. Las peticiones de los clientes se envían al **Servidor de páginas** con más recursos disponibles. Los **Servidores de páginas** adicionales pueden iniciarse cuando aumenten las peticiones de los clientes.

Acceso de clientes a sistemas principales CICS

El software de cliente CICS para Windows NT se proporciona con Communications Server, lo que permite que los clientes se conecten a sistemas principales CICS mediante Communications Server.

La Figura 29 en la página 106 muestra un ejemplo de cómo puede configurar un cliente CICS para que acceda a la información de una base de datos CICS de un sistema principal.

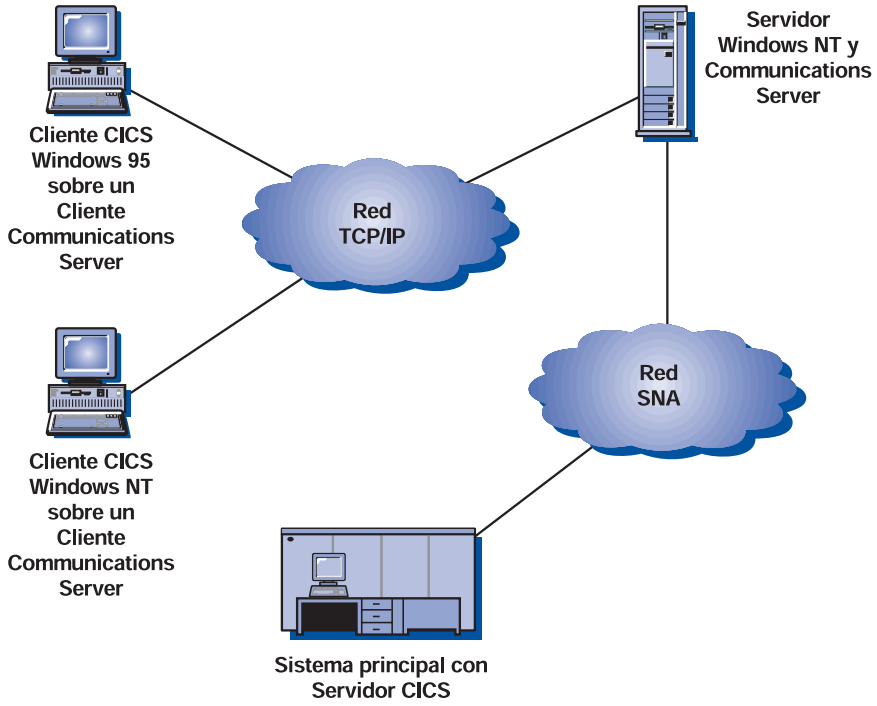


Figura 29. Entorno de cliente CICS

Para obtener más información sobre la configuración de clientes CICS, consulte la publicación *CICS Clients Adminstration*. Este manual está disponible en la siguiente ubicación de Internet:

http://www.software.ibm.com/ts/cics/library

Acceso de clientes a sistemas principales MQSeries

El software de cliente MQSeries para Windows NT se proporciona con Communications Server, lo que permite que los clientes se conecten a sistemas principales MQ mediante Communications Server.

La Figura 30 en la página 107 muestra un ejemplo de cómo puede configurar un cliente MQSeries para que acceda a la información de una base de datos MQSeries de un sistema principal.

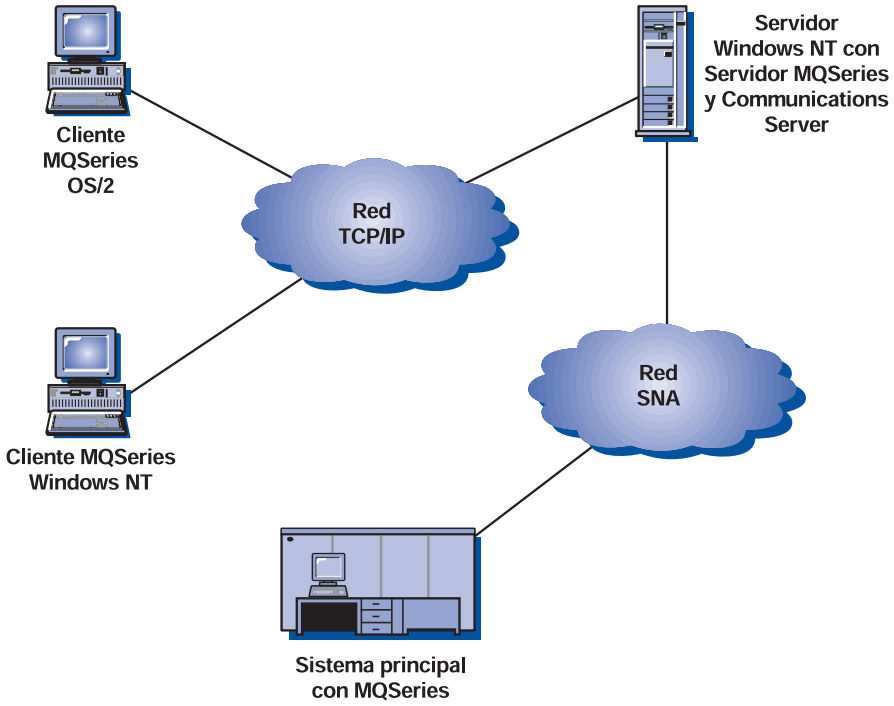


Figura 30. Entorno de cliente MQSeries

Para obtener más información sobre la configuración de clientes MQ, consulte la publicación *MQSeries Intercommunication*. Este manual está disponible en la siguiente ubicación de Internet:

http://www.software.ibm.com/ts/mqseries/library

Acceso de clientes a sistemas principales DB2

Communications Server incluye software “pruebe y compre” para DB2 Connect Enterprise Edition, un producto de conectividad de múltiples usuarios con el sistema principal. Puede instalar DB2 Connect Enterprise Edition en un servidor Windows NT.

Communications Server incluye también el DB2 Client Application Enabler (CAE) que proporciona el acceso del cliente al sistema principal. Puede instalar DB2 CAE en una máquina cliente que ejecute Windows 3.1, Windows 95, Windows NT u OS/2.

La Figura 31 en la página 108 muestra un ejemplo de cómo puede configurar DB2 Connect Enterprise Edition para acceder a la información de una base de datos DB2 de un sistema principal.

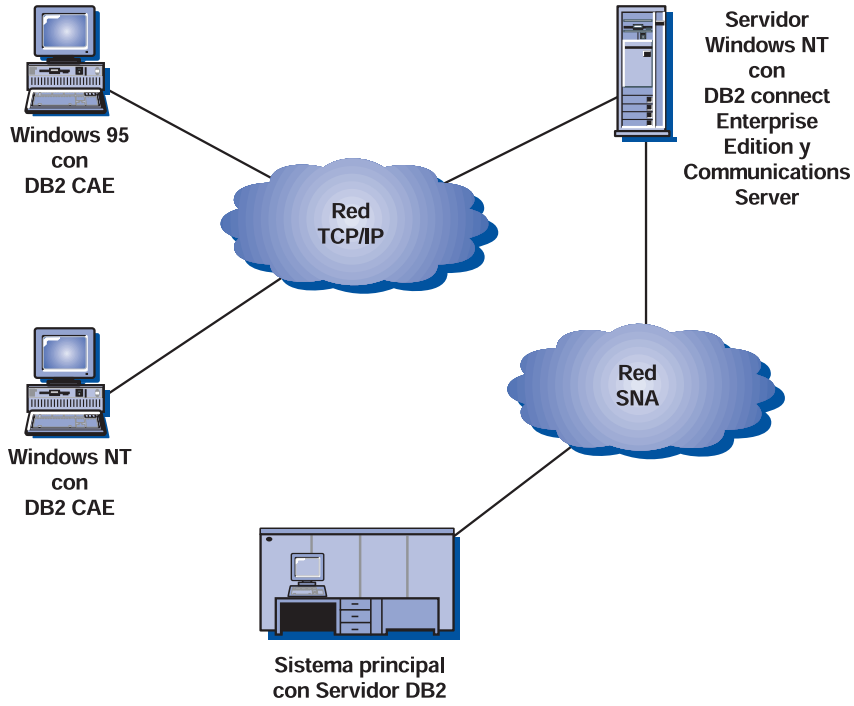


Figura 31. Entorno de DB2 Connect Enterprise Edition

Para obtener más información sobre la configuración de Communications Server para un sistema principal que ejecute DB2, vaya a la siguiente URL de Internet:

http://www.networking.ibm.com/cms/tips/csncfgdb2.htm

Planificación de HPR

Communications Server da soporte a conexiones de direccionamiento de alto rendimiento (HPR) sobre Enterprise Extender (IP), control síncrono de enlace de datos (SDLC), LAN, WAN, canal, Canal de múltiples vías (MPC) y X.25.

El direccionamiento automático de red (ANR) HPR minimiza los requisitos de almacenamiento y de proceso de los nodos intermedios, lo que representa una mejora en relación al direccionamiento de sesiones intermedias (ISR) APPN para redes de alta velocidad con proporciones de error bajas.

El soporte HPR de Communications Server incluye el soporte para el protocolo de transporte rápido (RTP) y el direccionamiento automático de red (ANR).

Características de enlace HPR

Para proporcionar los beneficios listados arriba, HPR supone que los enlaces de datos proporcionan proporciones bajas de tramas perdidas. HPR recupera condiciones que producen la pérdida de tramas, pero si las condiciones persisten durante largos períodos de tiempo, HPR supone que la congestión de la red es demasiado elevada y se reduce la productividad HPR. Conseguir una buena productividad HPR en un enlace determinado implica la configuración adecuada del nodo remitente, los recursos que constituyen el enlace entre los dos nodos y el nodo receptor.

Nota: Es aconsejable establecer valores ERP en los casos en que los recursos de la línea LAN tienen una alta pérdida de tramas.

Nodo remitente

Los adaptadores típicos utilizados con HPR enviarán tramas a la línea con bajas proporciones de anomalía. En el caso de Ethernet, el funcionamiento de HPR se degradará si la LAN está muy cargada y se producen muchas colisiones (por ejemplo, si la carga es superior a la velocidad nominal de Ethernet en un 30% o 40% aproximadamente). Para frame relay, los recursos deben estar configurados para que las conexiones individuales puedan entrar en ráfagas en la velocidad de línea de acceso sin causar condiciones de congestión en la red de frame-relay.

Recursos de línea

Los recursos de la LAN pueden tener una complejidad oculta sustancial, desde una gran cantidad de estaciones que comparten un solo segmento de la LAN a puentes entre los segmentos de la LAN, quizá con enlaces de ocultos de velocidad inferior, para segmentos simulados de la LAN que funcionan en subredes complejas. Debe cumplirse la suposición de pocas pérdidas de tramas. Por ejemplo, los enlaces de WAN entre los puentes de división deben utilizar recursos con proporciones bajas de error o deben compensar mediante la utilización de la recuperación de errores a nivel de enlace entre los puentes. Otro ejemplo es que deben evitarse las condiciones que producen el desbordamiento de los almacenamientos intermedios

© Copyright IBM Corp. 1989, 1996

de puentes (tormentas de difusión o ráfagas grandes de tramas de difusión).

Nodo receptor

Los adaptadores típicos utilizados con HPR recibirán tramas de la línea con bajas proporciones de anomalía. Sin embargo, algunos adaptadores, no podrán recibir tramas cuando lleguen tramas consecutivas demasiado deprisa. El mejor rendimiento HPR se realiza cuando el adaptador receptor puede manejar su tráfico sin que falten tramas de entrada.

Si la red tiene una alta proporción de errores, los administradores del sistema, pueden observar una productividad inferior a la esperada en las conexiones HPR.

Consideraciones sobre HPR

Las características de HPR se consiguen incluyendo información adicional en las cabeceras de las tramas. Si no necesita las características HPR, la actividad general adicional puede reducir el rendimiento de la red. Las características HPR son una ventaja cuando hay nodos intermedios o rutas alternativas. Sin embargo, si necesita un alto rendimiento entre dos nodos conectados por un solo enlace sin recuperación sin interrupción durante una anomalía del enlace, debe inhabilitar HPR cuando configure ese enlace.

HPR implanta la prioridad de puesta en cola. En general, el tráfico interactivo pasa a través de la red más rápido que el tráfico por lotes de prioridad inferior. Los adaptadores que ponen en cola tramas lo hacen sin tener en cuenta la prioridad y pueden interferir en la prioridad de puesta en cola de HPR. Es posible que tenga que reducir la profundidad de cola del adaptador para evitar que el tráfico de baja prioridad retarde el tráfico de alta prioridad. (Consulte la documentación del adaptador para obtener instrucciones sobre el establecimiento de la profundidad de cola del adaptador.)

Ahora, muchos PC tienen características avanzadas de gestión de alimentación que suspenderán la alimentación para los dispositivos (por ejemplo, unidades de discos) y reducirán la velocidad de reloj en una CPU de manera significativa para ahorrar energía si no se utiliza el teclado o el ratón. En una estación de trabajo, es una característica buena, pero en una plataforma de servidor, esta situación puede darse cuando está direccionando datos de un adaptador a otro (y no se produce ninguna actividad de disco). Para Communications Server, inhabilite la gestión de alimentación avanzada y la gestión de alimentación de hardware entrando en la configuración de BIOS durante el arranque (normalmente pulsando la tecla F1 cuando se inicializa el hardware) e inhabilitando estas opciones.

HPR utilizará más memoria de adaptador de LAN debido al aumento del rendimiento y de la puesta en cola. Muchos adaptadores de RAM compartida toman por omisión la utilización de 8 kilobytes de RAM compartida. Es necesario que el tamaño de RAM compartida sea de 16 kilobytes. Para ajustar esta configuración, consulte el manual de configuración del adaptador. Este valor está ubicado en la BIOS de la máquina o en las posiciones del conmutador del adaptador.

Nota: Si no aumenta la RAM compartida a 16 kilobytes, se degrada el rendimiento de la red.

No ajuste el valor de RAM compartida por encima de 16 kilobytes, el valor óptimo para la memoria del adaptador.

Si fallan los enlaces HPR bajo un tráfico pesado, puede establecer los temporizadores de recepción en un valor superior. Esto proporciona más tiempo para que los enlaces reciban un reconocimiento para las tramas enviadas.

En enlaces SDLC, es el Temporizador primario de recepción. El temporizador de recepción puede establecerse en el DLC o en una sentencia de enlace lógico.

Para calcular el valor mínimo del temporizador de recepción en décimas de segundos, utilice la siguiente fórmula:

```
[(cuenta_ventana_envío * tamaño_máximo_campo_i * 8) /velocidad de línea real]* 10
```

Consideraciones acerca del ajuste de parámetros en los DLC LAN

Puede especificar ocho parámetros que afectan a la rapidez con que Communications Server maneja la recuperación y anomalía de los enlaces LAN. Es posible que necesite ajustar estos parámetros para conseguir los mejores resultados si utiliza enlaces lentos, HPR o conexiones del sistema principal de reserva.

Debe tomar en consideración los siguientes parámetros cuando defina un dispositivo LAN en **Configuración de nodos**:

Bajo la pestaña **Avanzados**:

Intervalo de intentos de prueba El intervalo de intentos de prueba especifica el tiempo entre los intentos realizados para buscar la estación de enlace adyacente en la red de área local (LAN). El número de intentos realizados se basan en el valor especificado para el límite de intentos de prueba.

El valor por omisión es 8.

Límite de intentos de prueba El límite de intentos de prueba especifica el número máximo de intentos para buscar la estación de enlace adyacente en la red de área local (LAN) sin recibir ningún reconocimiento en el tiempo establecido por el valor de intervalo de intentos de prueba.

El valor por omisión es 5.

Tamaño máximo de PIU El tamaño máximo de unidad de información de vía de acceso (PIU) es el número máximo de bytes que están contenidos en el almacenamiento intermedio de datos utilizados por las sesiones SNA para este enlace. Si el valor del tamaño máximo de PIU excede del tamaño de trama soportado por el controlador de dispositivo local, el valor se reducirá para que coincida con el tamaño de trama.

El valor por omisión es 65535.

Bajo la pestaña **Rendimiento**:

tiempo de espera de desocupación El tiempo de espera de desocupación especifica el período de tiempo que el controlador espera recibir una trama antes de declarar que el enlace no es operativo.

El valor por omisión es de 30 segundos.

Retardo de reconocimiento El retardo de reconocimiento especifica el tiempo que el dispositivo de la LAN retiene una respuesta para una trama recibida a fin de permitir recibir más tramas y que se reconozcan con la misma señal Petición preparada (RR).

El valor por omisión es de 100 milisegundos.

Tiempo de espera de respuesta de sondeo

El tiempo de espera de respuesta de sondeo especifica el tiempo que el dispositivo de la LAN espera una respuesta a una trama enviada con el bit POLL establecido.

El valor por omisión es de 8 000 milisegundos.

Transmisiones pendientes anticipadas Las transmisiones pendientes anticipadas especifican el número máximo de tramas que el dispositivo de la LAN pone en cola para una estación de enlace antes de enviar una señal Recepción no preparada (RNR) a la estación de enlace adyacente.

El valor por omisión es de 16 tramas.

Recuento de almacenamiento intermedio de recepción El recuento de almacenamiento intermedio de recepción especifica el número de almacenamientos intermedios que están reservados a la memoria para conservar los datos recibidos del sistema principal hasta que puedan procesarse. Cada almacenamiento intermedio es del tamaño de la PIU.

El valor por omisión es de 32 almacenamientos intermedios.

Proceso de conmutación de vías de acceso HPR

HPR proporciona una conmutación de vías de acceso sin interrupciones para una conexión distinta si falla una conexión. Se reintenta la conexión que ha fallado antes de producirse la conmutación de vías de acceso. A continuación encontrará una explicación de los parámetros implicados en la determinación de si ha fallado una conexión y el momento de iniciar una conmutación de vías de acceso.

Cuando se alcanza el valor de **Tiempo de espera de desocupación** especificado, se envía una trama de latencia. El valor por omisión para **Tiempo de espera de desocupación** es de 30 segundos.

El valor especificado para **Tiempo de espera de respuesta de sondeo** determina el tiempo que el dispositivo espera una respuesta para la trama de latencia. El valor por omisión para **Tiempo de espera de respuesta de sondeo** es de ocho segundos (8 000 milisegundos). La trama de latencia se reintenta 10 veces. El recuento de reintentos no se puede cambiar.

Si no hay ninguna respuesta a la trama de latencia, se envían los mandatos TEST al sistema asociado. El valor especificado para **Intervalo de reintentos de prueba** determina el tiempo entre los intentos del mandato TEST y el valor especificado para **Límite de reintentos de prueba** determina el número máximo de intentos del mandato TEST. El valor por omisión **Intervalo de reintentos de prueba** es de 8 segundos y el valor por omisión de **Límite de reintentos de prueba** es de cinco intentos.

El siguiente cálculo indica el tiempo necesario para determinar si una conexión ha fallado e iniciar una conmutación de vías de acceso:

```
(Tiempo de espera de desocupación)
+ (Tiempo de espera de respuesta de sondeo * 10 reintentos)
+ (Intervalo de reintentos de prueba * Límite de reintentos de prueba)
+ 1
```

Utilizando los valores por omisión para los parámetros, el tiempo necesario para determinar que una conexión ha fallado e iniciar una conmutación de vías de acceso puede ser de un máximo de 151 segundos.

```
(30 segundos) + (8 segundos * 10 reintentos) +
           (8 segundos * 5 intentos) + 1 = 151 segundos
```

Si experimenta tiempos largos de conmutación de vías de acceso (o anomalías) con HPR cuando falla una conexión, puede reducir el tiempo disminuyendo los valores para los parámetros del cálculo.

Planificación de la pasarela SNA

La pasarela SNA da soporte a:

- Varios protocolos SNA
- Varias estaciones de trabajo en sentido descendente
- Varios tipos de enlace entre la pasarela y el sistema principal
- Agrupación de LU (sesiones) en la pasarela
- Definición de estaciones de trabajo implícitas
- Cambio o adición dinámicamente de definiciones para estaciones de trabajo inactivas
- Múltiples sistemas principales simultáneamente
- Varios tipos de enlace (que pueden combinarse) entre las estaciones de trabajo y la pasarela

Consulte la publicación *Quick Beginnings* para obtener instrucciones de cómo configurar una pasarela SNA utilizando **Configuración de nodos**.

Conexiones soportadas para estaciones de trabajo

La pasarela SNA da soporte a las estaciones de trabajo conectadas por:

- Conectividades LAN
  - Red en anillo
  - Ethernet
  - ATM (emulación de LAN)
- Frame Relay
- SDLC
  - Asíncrono
  - Síncrono
  - Hayes Autosync
  - Primario multipunto
- Red X.25
- AnyNet TCP/IP (para conectividades soportadas por Microsoft TCP/IP)
- Conexiones ISDN

La pasarela SNA puede dar soporte a un máximo de 254 LU para cada PU definida. Puede definir una PU diferente para cada una de las conexiones del sistema principal. Las estaciones de trabajo en sentido descendente utilizan las LU para conectarse al sistema principal. El número de estaciones de trabajo en sentido descendente soportadas depende de varios factores, incluyendo el tipo de conectividad y el número de adaptadores de la pasarela. Por ejemplo, si tiene un adaptador de la LAN en la pasarela, un enlace con el sistema principal con 254 LU se puede utilizar por 253 estaciones de trabajo en sentido descendente simultá-

© Copyright IBM Corp. 1989, 1996

neamente. Con dos adaptadores, puede doblar el número de estaciones de trabajo en sentido descendente.

Conexiones de estación de trabajo SDLC

Puede elegir conectarse utilizando SDLC en configuraciones de punto a punto y Multipunto. Después de haber completado la configuración, no es necesaria ninguna consideración para ejecutar SDLC entre la estación de trabajo y la pasarela.

Cuando configure estaciones secundarias multipunto, tome en consideración los distintos factores que controlan el tiempo de cambio de sentido del sondeo. Hay limitaciones físicas que afectan a la rapidez con la que el primario puede sondear el secundario situado a mayor distancia. La definición de todas las estaciones de trabajo secundarias utilizando los mismos parámetros simplificará el cálculo siguiente.

Para calcular el tiempo de inactividad mínimo en segundos, utilice la fórmula:

```
     NS * (SW + RW) * (IS + 2) / (LS / 8)
donde:
     NS  =  Número de estaciones
     SW  =  Tamaño de ventana de envío
     RW  =  Tamaño de ventana de recepción
     IS  =  Tamaño de campo-i
     LS  =  Velocidad de línea (bps)
```

Si estos valores no son los mismos para todas las estaciones de trabajo secundarias, debe realizarse el cálculo para cada grupo o estación de trabajo y sumarse para encontrar el valor correcto para el temporizador de inactividad.

Por ejemplo, para un enlace multipunto con 16 estaciones de trabajo secundarias a 14,4 Kbps, que tenga cada estación de trabajo establecida para un tamaño de ventana de envío de 7, un tamaño de ventana de recepción de 7, y un tamaño de campo-i de 521, el cálculo del temporizador de inactividad sería:

```
16 * (7 + 7) * (521 + 2) / (14400 / 8) = 65,1 segundos
```

Nota: Añada siempre unos segundos más para el almacenamiento intermedio.

Conexiones de estación de trabajo X.25

Si configura la pasarela SNA para que utilice solamente conexiones de circuito virtual permanente (PVC) X.25 entre la pasarela y las estaciones de trabajo, es aconsejable configurar todas los PVC de estación de trabajo y pasarela con funciones de estación de enlace negociable. Si no configura los PVC de pasarela y estación de trabajo con funciones de estación de enlace negociables, es posible que las estaciones de trabajo no puedan establecer los enlaces PVC X.25 con la pasarela.

Consulte el apartado Planificación de X.25 para obtener más información acerca de las conexiones PVC y la configuración.

Conexiones soportadas con sistemas principales

La pasarela SNA da soporte a las siguientes conexiones con un sistema principal:

- Conectividades LAN
  - Red en anillo
  - Ethernet
  - ATM (emulación de LAN)
- Frame Relay
- SDLC
  - Síncrono
  - Hayes Autosync
- Red X.25
- Twinaxial (para AS/400)
- AnyNet TCP/IP (para conectividades soportadas por Microsoft TCP/IP)
- Enterprise Extender (para conectividades soportadas por Microsoft IP)
- Canal (CDLC)
- Canal (MPC) con una conexión DLUR
- Conexiones ISDN

Si hay conexiones con múltiples sistemas principales desde la pasarela que utiliza el tráfico de LU dependiente, sólo el enlace con el sistema principal con el nombre de PU de punto de control puede realizar lo siguiente:

- Actuar como un punto focal del sistema principal
- Mantener sesiones CP-CP con el sistema principal
- Ser utilizado para funciones APPN

Los enlaces que están definidos con un nombre de PU que no es el mismo que el nombre de punto de control sólo se pueden utilizar para conexiones adicionales de LU dependiente con un sistema principal.

Si un enlace con el sistema principal de pasarela está definido como un enlace de recurso limitado, se enviará una petición de descontactar al sistema principal después de que la última sesión LU-LU se haya desvinculado. Entonces la pasarela pasa las DACTLU a la estación de trabajo y una DACTPU a las estaciones de trabajo que sólo tienen sesiones con ese enlace con el sistema principal. Cuando la estación de trabajo conectada a la pasarela está definida como un recurso limitado, el enlace de estación de trabajo se desconecta si no hay otras sesiones. En Communications Server puede designar una estación de trabajo como un recurso limitado cuando se define la conexión cliente explícita.

Sin embargo, si la estación de trabajo tiene una aplicación (o emulador) que reactiva automáticamente su enlace con el sistema principal, la pasarela reactivará el enlace de pasarela con su sistema principal cuando la estación de trabajo active su enlace con la pasarela. Esto significa que las definiciones de estaciones de trabajo incompatibles inhibirían de manera efectiva la función de recurso limitado en la pasarela.

Consideraciones de sistema principal

Tome en consideración los puntos siguientes al planificar la conexión del sistema principal:

- Si el entorno utiliza un punto de control de red (NCP), la macro **LINE** de 37*xx* NCPGEN, el valor **MAXLU**, debe ser como mínimo igual al número de LU de Communications Server.
- Los usuarios VTAM pueden controlar el intervalo de tiempo durante el cual VTAM colocará datos en almacenamientos intermedios antes de enviarlos al controlador (flecos). Cuando se especifica el parámetro de flecos de VTAM **DELAY = 0** en cualquier definición de PU, debe proporcionar un tiempo de respuesta de envío al sistema principal más rápido a costa de más trabajo para el procesador del sistema principal.

  Cuando se especifica un valor que no es cero para DELAY, se ahorra al procesador del sistema principal instrucciones a costa de un tiempo de respuesta de recepción incrementado en la estación de trabajo de Communications Server.

  Para los flecos, empiece por el valor por omisión 0,2. Un retardo de 0,2 de segundo tiene un efecto moderado en el tiempo de respuesta, pero si la velocidad es aproximadamente de una transacción por segundo o mayor, se producen los flecos.
- Aunque cada estación de trabajo SNA en sentido descendente de la LAN implante una PU con su propio conjunto de LU, la pasarela SNA se implanta para que el sistema principal vea sólo la PU de pasarela. Por lo tanto, solo se codifica una definición de PU en el sistema principal. Esta definición de PU contiene las LU para ***todas*** las estaciones de la LAN que se van a conectar al sistema principal a través de la pasarela.

  Si VTAM del sistema principal da soporte a las LU dependientes de definición propia (SDDLU), es posible que desee aprovechar las ventajas de la función. Cuando configure las LU de sistema principal, especifique el tipo de modelo de LU o proporcione un nombre de modelo de LU que coincida con el valor de operando LUSEED definido en el nodo principal conmutado VTAM y utilizado por la rutina de salida de SDDLU VTAM.

Configuración de dirección de destino de LAN

Es necesario proporcionar una dirección de destino si utiliza una de las conexiones de la LAN soportadas entre la pasarela y el sistema principal o entre la pasarela y las estaciones de trabajo definidas explícitamente. Cuando determine la dirección de destino correcta para entrar en cada perfil, recuerde que la perspectiva correcta para ambas direcciones es ver el destino desde la pasarela SNA. La Figura 32 en la página 119 muestra esta vista.

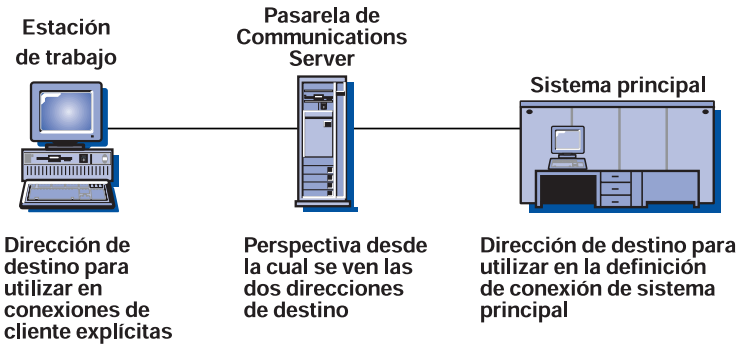


Figura 32. Perspectiva para utilizar entradas de dirección de destino

Planificación de las definiciones de LU de pasarela

La pasarela SNA da soporte a las LU de sistema principal ***agrupadas*** y a las LU de sistema principal ***dedicadas***. Cuando se configuran las LU para cada conexión de sistema principal en la pasarela SNA, pueden agruparse en agrupaciones. La creación de agrupaciones es con frecuencia beneficiosa por las siguientes razones:

- Si ninguna sesión de ninguna estación de trabajo necesita comunicarse con el sistema principal a la vez, la agrupación puede ahorrar recursos del sistema. Las sesiones de estación de trabajo de la LAN pueden compartir las mismas LU, pero no a la vez. Esta función permite que el número de LU configuradas en la pasarela SNA para sesiones de estación de trabajo sea mayor que el número de LU configuradas entre el sistema principal y la pasarela, reduciendo los requisitos de recursos de sistema principal y la definición de estación de trabajo del sistema principal, y acelerando los reinicios.
- Las agrupaciones son más fáciles de administrar y configurar. Puede ajustar el tamaño de la agrupación añadiendo más LU a la misma o suprimiendo LU de la misma sin afectar a otras definiciones.

  Las LU agrupadas no están dedicadas a ninguna estación de trabajo en particular, ni su utilización tiene que estar dedicada a los usuarios de la pasarela en sentido descendente. Una sola agrupación puede compartirse por usuarios TN3270 en sentido descendente y estaciones de trabajo de pasarela SNA, así como clientes API SNA y sesiones de emulador local. Si desea configurar una agrupación (por ejemplo, PUBLIC) para todas las utilizaciones de LU dependientes, no necesita conocer cómo se distribuirán los usuarios entre estos tipos.
- Las agrupaciones pueden proporcionar una mejor disponibilidad para las estaciones de trabajo en sentido descendente si define las LU de múltiples conexiones en la misma agrupación. Si una de las conexiones está activa pero la otra no, los usuarios pueden acceder a las LU del enlace activo.

Tome en consideración los escenarios siguientes:

- Communications Server tiene dos conexiones de sistema principal con 100 LU definidas en cada conexión, todas ellas pertenecientes a la agrupación A. El primer enlace se configura como *activar en el arranque* y es operativo. Todas las estaciones de trabajo utilizan este enlace con sus LU. El segundo enlace está configurado como *activar automáticamente*. Esta combinación de agrupaciones con la configuración de enlace puede proporcionar una mejor dispo-

nibilidad de dos maneras. Si falla el primer enlace, las sesiones dependientes de recuperación activan automáticamente el segundo enlace. Si el primer enlace agota las LU definidas, se activará automáticamente el enlace de reserva cuando se necesite la siguiente LU (la número 101).

- También puede utilizar la combinación de agrupaciones y configuración de enlace para proporcionar el equilibrio de la carga para las estaciones de trabajo en sentido descendente entre las conexiones de sistema principal disponibles. Un ejemplo de esto sería para que el Communications Server tenga dos conexiones de sistema principal con 100 LU definidas en cada conexión, todas ellas pertenecientes a la agrupación A. Ambos enlaces se configuran como *activar en el arranque* y son operativos. Las estaciones de trabajo que se correlacionan con la agrupación de LU se distribuirán entre ambas conexiones para compartir la carga entre ellas.

La pasarela SNA asigna las LU agrupadas a las sesiones de estación de trabajo cuando la estación de trabajo en sentido descendente se conecta a la pasarela. Las sesiones de estación de trabajo se pueden definir para que utilicen las LU de diferentes sistemas principales con LU dedicadas o agrupadas.

Las LU dedicadas no pertenecen a ninguna agrupación. Se puede configurar una LU dedicada para que la utilice un cliente definido explícitamente.

La Figura 33 muestra una configuración sencilla con estaciones de trabajo que utilizan LU dedicadas, LU agrupadas o ambas. (Las líneas de conexión representan las LU.)

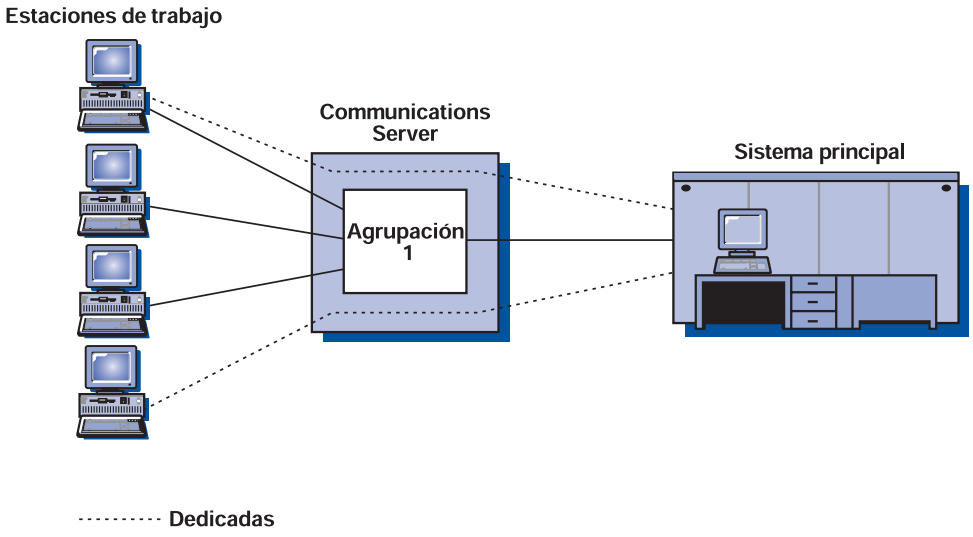


Figura 33. Un escenario sencillo que utiliza LU agrupadas y dedicadas

Utilización de conexiones explícitas e implícitas

Hay dos tipos de estaciones de trabajo en sentido descendente soportadas por la pasarela: explícitas e implícitas. Las estaciones de trabajo explícitas son estaciones de trabajo que tienen direcciones de destino definidas en un tipo de DLC en particular (por ejemplo, red en anillo y SDLC). Para configurar estaciones de trabajo explícitas, debe conocer la dirección de destino o el nombre completamente calificado del punto de control adyacente o el ID de nodo adyacente de cada estación de trabajo y también debe definir un enlace lógico con la pasarela

para cada estación de trabajo. Las LU que se definen para estaciones de trabajo explícitas pueden ser agrupadas o dedicadas.

Las estaciones de trabajo implícitas son más fáciles de configurar, pero sólo pueden utilizar LU agrupadas. En lugar de definir un enlace con cada estación de trabajo que utilice la pasarela, defina una agrupación (o agrupaciones) de LU de sistema principal y configure los dispositivos (DLC) utilizados por las conexiones de estación de trabajo. Configure una plantilla de cliente implícito para utilizarla como modelo para la definición de LU para cada estación de trabajo que se conecte a la pasarela y no coincida con una definición explícita. Por ejemplo, si cada estación de trabajo de una LAN Ethernet tiene configuradas dos sesiones 3270 con las direcciones NAU 2 y 3, configuraría una plantilla de cliente con dos LU (una para la dirección 2 y otra para la dirección 3). Si se utilizan ambas direcciones para sesiones con un solo sistema principal, correlacione ambas direcciones con la misma agrupación del sistema principal. Sin embargo, si se utiliza la dirección 2 para ir a HOST_A y se utiliza la dirección 3 para ir a HOST_B, correlacione cada una para la agrupación de sistema principal adecuada. En este ejemplo, cada vez que una estación de trabajo se conecta con la pasarela en Ethernet, que no coincide con una definición explícita, se crea dinámicamente un enlace y las dos LU para NAU 2 y 3 se asignan desde la agrupación o agrupaciones de LU del sistema principal.

En el caso de estaciones de trabajo implícitas, los usuarios que se conectan a la pasarela sólo necesitan conocer la dirección del adaptador de DLC de pasarela que está configurado para las estaciones de trabajo implícitas y los valores de NAU que se han definido en la pasarela. Deben utilizar estos valores de NAU al definir sus sesiones 3270 y las impresoras lógicas.

Una estación de trabajo Personal Communications en sentido descendente que se conecta con Communications Server puede utilizar el descubrimiento de LAN, para buscar el nombre de grupo `IG02HOST`, para encontrar la dirección de adaptador.

Rendimiento de la pasarela SNA

El rendimiento de cualquier pasarela depende de muchos factores, entre los que se incluyen:

- Configuración de la pasarela
- Conexión con el sistema o sistemas principales
- Demanda de proceso general en cada sistema principal
- Conexiones con las estaciones de trabajo soportadas
- Configuraciones de las estaciones de trabajo soportadas
- Número de estaciones de trabajo soportadas
- Número de sesiones con cada estación de trabajo
- Prioridad de transmisión SNA
- Control de flujo
- Ventana de ritmo para todas las sesiones
- Tráfico en las sesiones sin pasarela

La utilización de una estación de trabajo que implanta una pasarela de software para otras funciones también puede deteriorar el rendimiento de la pasarela.

Si ninguno de los factores mencionados previamente está causando un impacto negativo en el rendimiento, una estación de trabajo individual que utilice los protocolos SNA soportados no debe experimentar ninguna diferencia de rendimiento evidente entre una conexión directa con el sistema principal y una conexión indirecta por medio de una LAN a través de una pasarela SNA conectada al sistema principal. De hecho, si los enlaces del sistema principal están activos en la pasarela, la activación de la estación de trabajo puede mejorar mediante la eliminación del retardo de la actividad general del sistema principal. Sin embargo, debido a que hay muchas variables implicadas, es aconsejable realizar pruebas de rendimiento en el entorno operativo para que pueda atender el equilibrio deseado entre función y rendimiento.

Consideraciones acerca de DLUR

Mediante la utilización de DLUR para la conexión con el sistema principal, se gana flexibilidad en donde puede colocarse la pasarela SNA. La conexión con el sistema principal puede atravesar cualquier red APPN y no se limita a ser adyacente a un HOST/NCP. Se crea un conducto DLUR a DLUS para VTAM DLUS que se utiliza para los flujos de control de sesión dependiente.

La configuración recomendada para tener una conexión DLUR con el sistema principal es definir la pasarela para que sea un nodo de red y configurar la información de DLUS. Durante la configuración de clientes explícitos e implícitos, correlaciónelos con el DLUS. Esta configuración es más fácil porque no necesita ningún conocimiento de las LU en sentido descendente en la pasarela y proporciona la visibilidad más elevada de los dispositivos en sentido descendente para VTAM, ya que VTAM tiene conocimiento de la PU.

Si no desea que VTAM tenga conocimiento de las PU en sentido descendente, puede configurar una PU interna en la pasarela (en lugar de una conexión de sistema principal) y correlacionar las estaciones de trabajo en sentido descendente con esa PU interna.

Si una estación de trabajo en sentido descendente como, por ejemplo, Personal Communications, tiene la posibilidad de DLUR, es aconsejable que la estación de trabajo realice el direccionamiento a través de Communications Server utilizando la posibilidad de nodo de red en lugar de la función de pasarela SNA.

Planificación del servidor TN3270E

La función del servidor TN3270E le permite configurar la red tal como se muestra en la Figura 34 o en la Figura 35 en la página 124.

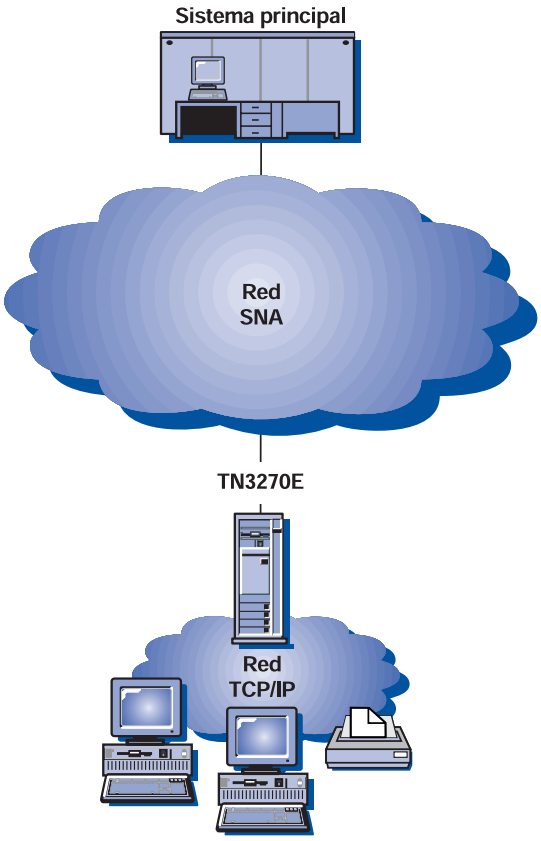


Figura 34. Communications Server configurado como un servidor TN3270E con red SNA de área amplia

© Copyright IBM Corp. 1989, 1996

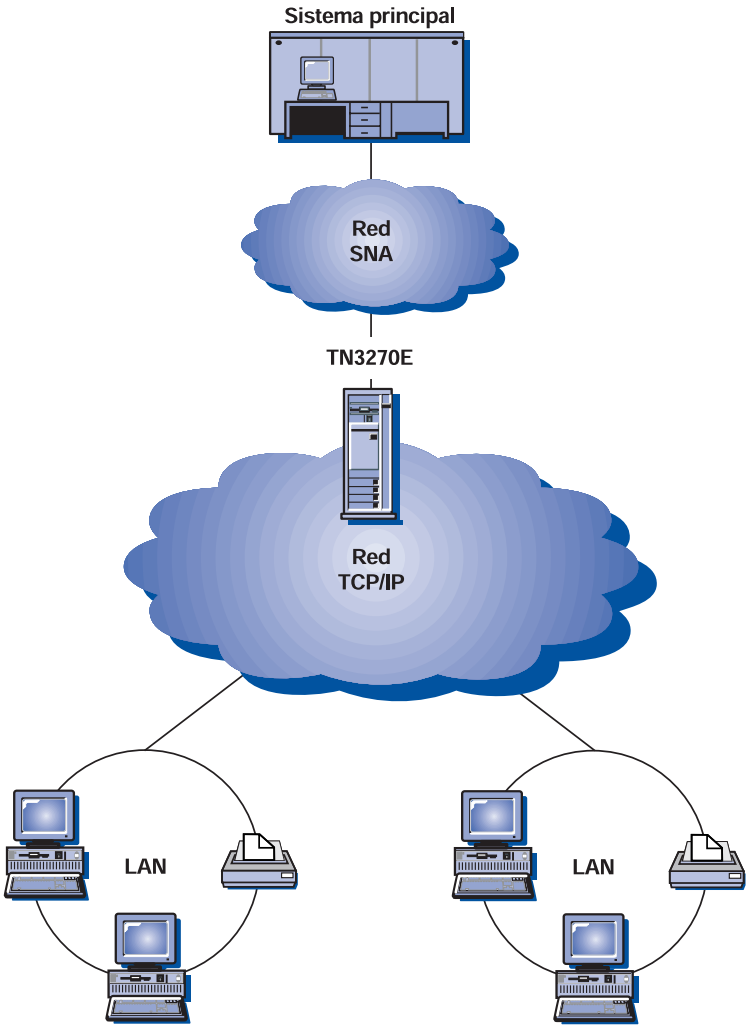


Figura 35. Communications Server configurado como un servidor TN3270E con red TCP/IP de área amplia

La función del servidor TN3270E da soporte a:

- La emulación de LU

  El servidor TN3270E da soporte a la LU 2, que permite a los usuarios ejecutar los programas de aplicación del monitor 3270 interactivo.

- Impresión del sistema principal

  Las ampliaciones estándar de Telnet 3270 (TN3270E) permiten a los usuarios imprimir desde aplicaciones del sistema principal en impresoras conectadas a su estación de trabajo. Estas impresoras pueden estar conectadas localmente o conectadas a la red. Se da soporte a las sesiones de LU 1 y LU 3.

  El servidor TN3270E implanta los protocolos indicados en RFC 1646 y RFC 1647, permitiendo que el servidor pase datos de sesión LU 1 y LU 3 a los clientes habilitados por TN3270E, espere la confirmación del cliente de la petición de impresión y responda al sistema principal.

- filtro de IP

  Communications Server da soporte a la especificación de filtros de cliente TCP/IP, utilizando direcciones IP, subredes, nombres de sistemas principales o

nombres de dominios. Esta función permite la administración central de los clientes que tienen permitido conectarse al servidor TN3270E y la especificación de los nombres de LU y las agrupaciones a las que pueden acceder los clientes.

- Manejo de respuestas

  Los clientes habilitados por TN3270E pueden enviar respuestas tanto positivas como negativas, que el servidor TN3270E envía al sistema principal. El servidor TN3270E genera respuestas a las peticiones para los clientes TN3270 estándar.

- Manejo de teclas ATTN y SYSREQ

  El servidor TN3270E puede convertir y reenviar información al sistema principal cuando el cliente envía una tecla ATTN o SYSREQ. Aunque los clientes que no están habilitados por TN3270E no tienen ninguna definición explícita para ATTN y SYSREQ, el servidor TN3270E utiliza los siguientes mandatos Telnet para implantar estas funciones:

Tabla 6. Equivalentes a mandatos

Telnet	TN3270E	TN3270 estándar
IP	ATTN	SYSREQ
AO	SYSREQ	SYSREQ
BREAK	N/D	ATTN

- Clases de LU

  Communications Server clasifica las conexiones de usuario en clases de LU. Las clases consisten en LU configuradas con características comunes; aquellas que necesitan una conexión específica del sistema principal, por ejemplo. Esto simplifica el acceso de usuarios, agrupa a los usuarios por necesidades de aplicación y maximiza los recursos del sistema principal.

- Seguridad basada en Secure Sockets Layer-based (basada en SSL)

  Las conexiones entre los clientes TN y el servidor TN3270E utilizan SSL Versión 3 para proporcionar el cifrado de datos y la autentificación del servidor mediante la utilización de certificaciones firmadas.

Consulte el manual *Quick Beginnings* para obtener instrucciones de cómo configurar un servidor TN3270E.

Estaciones de trabajo cliente soportadas bajo el servidor TN3270E

El servidor TN3270E da soporte a cualquier cliente TN3270E o TN3270 que cumpla completamente con RFC 1576, 1646 ó 1647.

Características principales

Esta sección proporciona más información acerca de algunas de las características que puede configurar para el servidor TN3270E.

Cambio del número de puerta por omisión

Puede configurar el número de puerta que utiliza el servidor para las nuevas conexiones en la ventana Opciones de TN3270E. El número de puerta por omisión es 23, pero otras aplicaciones Telnet como, por ejemplo, el soporte de servidor TN5250, también pueden utilizar esta puerta. Si otras aplicaciones Telnet están utilizando la puerta 23, debe utilizar otra puerta.

Si cambia el número de puerta, evite los números que sepa que utilizan otras aplicaciones. Si dos aplicaciones utilizan el mismo número de puerta, una de las aplicaciones fallará.

Si cambia el número de puerta, utilice un número mayor que 1 024. Los números inferiores a 1 024 están reservados. Para obtener más información acerca de los números de puerta reservados, consulte la siguiente ubicación en Internet:

http://www.ds1.internic.net

En el momento de la publicación de este documento, el RFC más reciente para los números asignados es RFC1700.

Cuando cambie el número de puerta, notifíquelo a los usuarios del cliente TN3270E, porque tendrán que configurar sus aplicaciones de emulador para que coincidan.

Gestión del tráfico del sistema

Hay dos maneras de controlar la frecuencia con que se desconectan las conexiones no utilizadas: proceso de latencia y de desconexión automática.

Por omisión, el servidor TN3270E no utiliza el proceso de latencia. Si utiliza el proceso de latencia, puede elegir NOP o la marca de sincronismo.

- El proceso NOP envía un mandato Telnet NOP después de una frecuencia de mantener activa especificada. Esto provoca que se transmitan datos en la conexión, lo que hace que TCP/IP detecte que se ha interrumpido la conexión. El servidor no espera una respuesta del cliente. TCP/IP puede tardar un período de tiempo imprevisible en detectar la falta de conexión.
- La marca de sincronismo envía un mandato de marca de sincronismo Telnet al cliente. Si el cliente no responde dentro del período especificado, se cierra la conexión.

El proceso de marca de sincronismo provoca más tráfico en el sistema que el proceso de NOP, pero libera las conexiones no utilizadas más rápidamente.

Si elige una desconexión automática, el servidor desconecta cualquier sesión que no tenga tráfico durante el período especificado. El tráfico del proceso de latencia no mantiene abierta la conexión; deben enviarse datos al sistema principal o desde el mismo. Las sesiones de impresora no se desconectan automáticamente.

Si los emuladores cliente están configurados para realizar el proceso de latencia, es aconsejable desactivarlo en el servidor y si el proceso de latencia se realiza en el servidor, es aconsejable desactivarlo en el cliente para reducir el tráfico de la red.

Filtro de IP

Communications Server le permite configurar filtros TN3270E para especificar qué clientes TCP/IP pueden conectarse al servidor. Se pueden especificar los clientes utilizando direcciones IP individuales, subredes IP o nombres del sistema principal TCP/IP o nombres de dominio.

Soporte de capa de sockets segura (SSL)

Puede configurar un número de puerta segura que el servidor utiliza para las conexiones seguras en la ventana **Parámetros del servidor TN3270E** o en un archivo de respuesta.

Para habilitar la seguridad, Communications Server proporciona el programa de utilidad **Gestión de llamadas clave** para generar certificaciones y claves que son necesarias para SSL. Consulte el apartado “Planificación de la seguridad basada en la capa de sockets segura” en la página 135 para obtener más información.

Cuando haya configurado y habilitado la seguridad, los clientes TN3270E que den soporte a SSL Versión 3 podrán conectarse a un número de puerta segura y establecer conexiones seguras.

Configuración de conexiones SNA

Necesita configurar la conexión del sistema principal y las LU de sistema principal antes de utilizar la función del servidor TN3270E. Para ver una tabla que describe y explica los parámetros del sistema principal, consulte el manual *Quick Beginnings*.

Agrupación

Hay cuatro clases de definiciones de LU específicas para el servidor TN3270E: estación de trabajo implícita, estación de trabajo explícita, impresora implícita e impresora explícita. Estas clases se corresponden con las clases genérica de terminal, específica de terminal, genérica de impresora y específica de impresora especificadas en RFC 1647.

Las definiciones de ***estación de trabajo implícita*** se definen en una agrupación que el servidor TN3270E utiliza para satisfacer las peticiones para las conexiones. Se puede configurar la agrupación por omisión para satisfacer las peticiones en las que el cliente no especifica ningún nombre de LU ni de agrupación. Las demás agrupaciones deben pedirse por el nombre.

También puede definir un conjunto de definiciones de LU utilizadas para satisfacer las peticiones de un nombre de LU específico. Estas definiciones de ***estación de trabajo explícita*** aseguran que un dispositivo de terminal necesario para una aplicación de sistema principal no se asigne a ningún cliente que no la pida específicamente.

Similarmente, puede definir una agrupación de definiciones de impresora que se utilizarán para satisfacer la petición de conexiones que no necesitan nombres específicos de LU (***impresora implícita***) y un conjunto utilizado para satisfacer las peticiones de un nombre de LU específico (***impresora explícita***).

Las definiciones de estación de trabajo explícita e implícita pueden tener varias impresoras asociadas. Cada definición de terminal puede tener asignada una impresora y cada impresora puede tener una definición de terminal asociada. Estas impresoras no se incluyen en las definiciones de impresora explícita o implícita.

Las definiciones de ***impresora asociada*** sólo pueden accederse haciendo referencia al nombre de LU de terminal. Reducen la cantidad de información que necesita el usuario cliente, porque sólo necesita saber el nombre de LU del terminal para conectarse a las sesiones de terminal y de impresora.

Equilibrio de la carga de servidores TN3270E

Communications Server también da soporte al equilibrio de la carga de clientes TN3270 en múltiples servidores TN3270E. Consulte el apartado “Planificación del equilibrio de la carga” en la página 145 para obtener más información.

Planificación del servidor TN5250

La función del servidor TN5250 le permite configurar la red tal como se muestra en la Figura 36 o la Figura 37 en la página 130.

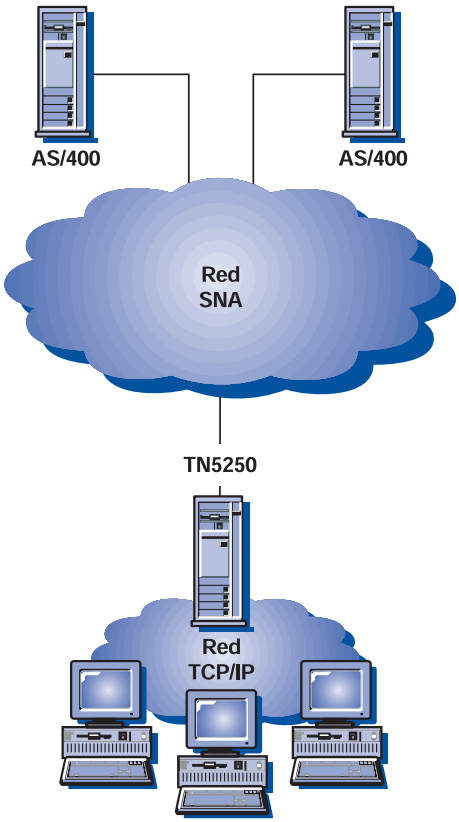


Figura 36. Communications Server configurado como un servidor TN5250 con la red SNA de área amplia

© Copyright IBM Corp. 1989, 1996

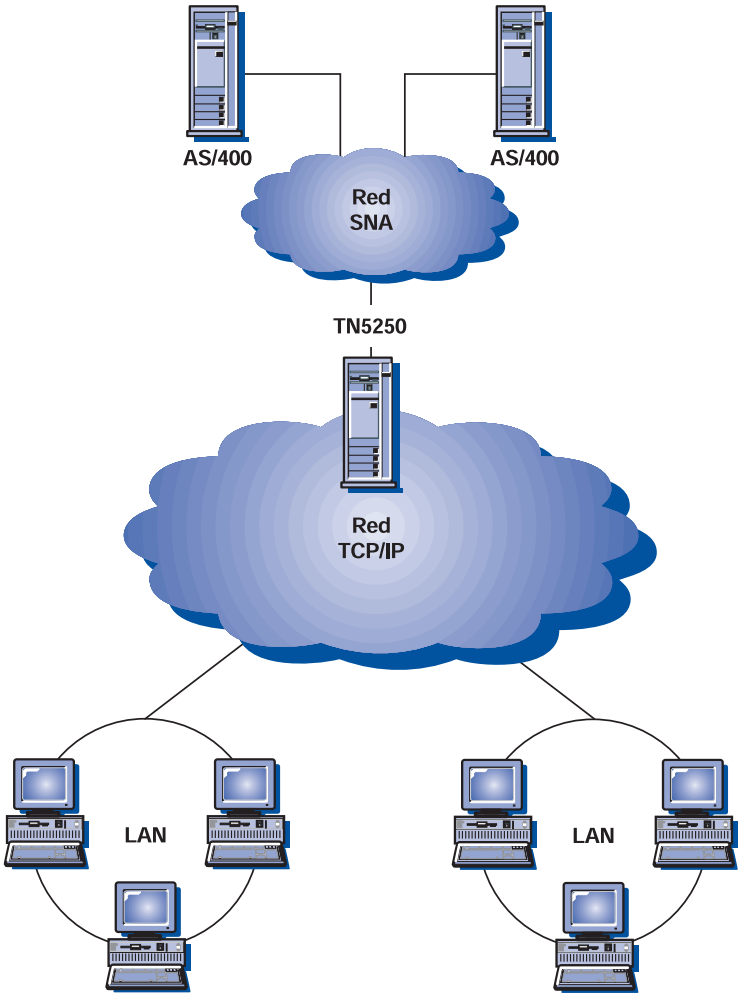


Figura 37. Communications Server configurado como un servidor TN5250 con red TCP/IP de área amplia

La función del servidor TN5250 da soporte a:

- La conexión a clientes TN5250 con corrientes de datos de estación de trabajo 5250

  En la implantación de protocolos indicados en RFC 1205, el servidor pasa los datos de estación de trabajo 5250 a y desde un cliente TCP/IP que emula una estación de trabajo IBM 5250. Este cliente se conoce normalmente como cliente TN5250.

- Acceso a uno o varios AS/400 de un red SNA

  El servidor se conecta a los sistemas principales AS/400 utilizando el protocolo SNA LU 6.2. Se proporciona el soporte para acceder a uno o varios AS/400 desde las mismas estaciones de trabajo cliente o diferentes.

- Filtro de IP

  Communications Server permite la especificación de filtros de cliente TCP/IP, mediante la utilización de direcciones IP, nombres de sistemas principales o nombres de dominio. Esta función permite la administración central de los clientes que tienen permitido conectarse al servidor, así como el soporte para direccionar los clientes a AS/400 específicos.

- Seguridad basada en Secure Sockets Layer (basada en SSL)

  Las conexiones entre los clientes TN y el servidor TN3270E utiliza SSL Versión 3 para proporcionar el cifrado de datos y la autentificación del servidor mediante la utilización de certificaciones con firma.

Consulte el manual *Quick Beginnings* para obtener instrucciones de cómo configurar un servidor TN5250.

Estaciones de trabajo cliente soportadas bajo el servidor TN5250

El servidor TN5250 da soporte a cualquier cliente TN5250 que cumpla completamente con RFC 1205.

Características principales

Esta sección proporciona más información acerca de algunas de las características que puede configurar para el servidor TN5250.

Cambio del número de puerta por omisión

Cuando se configura el soporte de servidor TN5250, se define una puerta por omisión con el número de puerta 23, pero otras aplicaciones Telnet como, por ejemplo, el soporte de servidor TN3270E, pueden utilizar también esta puerta. Si hay otras aplicaciones Telnet que se ejecutan utilizando la puerta 23, debe utilizar otra puerta.

Si cambia el número de puerta, evite los números que sepa que utilizan otras aplicaciones. Si dos aplicaciones utilizan el mismo número de puerta, una de ellas fallará.

Si cambia el número de puerta, utilice un número mayor que 1 024. Los números inferiores a 1 024 están reservados. Para obtener más información acerca de los números de puerta reservados, consulte la siguiente ubicación en Internet:

http://www.ds1.internic.net

En el momento de la publicación de este documento, el RFC más reciente para los números asignados es RFC1700.

Cuando cambie el número de puerta, notifíquelo a los usuarios del cliente TN5250, porque tendrán que configurar sus aplicaciones de emulador para que coincidan.

Gestión del tráfico del sistema

Hay dos maneras de controlar la frecuencia con que se desconectan las conexiones no utilizadas: proceso de latencia y de desconexión automática.

Por omisión, el servidor TN5250 no utiliza el proceso de latencia. Si utiliza el proceso de latencia, puede elegir NOP o la marca de sincronismo.

- El proceso NOP envía un mandato Telnet NOP después de una frecuencia de mantener activa especificada. Esto provoca que se transmitan datos en la conexión, lo que hace que TCP/IP detecte que se ha interrumpido la conexión. El servidor no espera una respuesta del cliente. TCP/IP puede tardar un período de tiempo imprevisible en detectar la falta de conexión.

- La marca de sincronismo envía un mandato de marca de sincronismo Telnet al cliente. Si el cliente no responde dentro del período especificado, se cierra la conexión.

El proceso de marca de sincronismo provoca más tráfico en el sistema que el proceso de NOP, pero libera las conexiones no utilizadas más rápidamente.

Si elige una desconexión automática, el servidor desconecta cualquier sesión que no tenga tráfico durante el período especificado. El tráfico del proceso de latencia no mantiene abierta la conexión; deben enviarse datos al sistema principal o desde el mismo.

Si los emuladores cliente están configurados para realizar el proceso de latencia, es aconsejable desactivarlo en el servidor y si el proceso de latencia se realiza en el servidor, es aconsejable desactivarlo en el cliente para reducir el tráfico de la red.

Especificación del acceso a los AS/400 con múltiples puertas

Communications Server le permite configurar más de un AS/400 y le permite configurar más de una puerta para que el servidor TN5250 escuche las conexiones de entrada. Cuando configure una nueva puerta de servidor TN5250, puede especificar el AS/400 que se ha de asociar con la puerta. Las conexiones TCP/IP de entrada recibidas en esa puerta por el servidor TN5250 accederán al AS/400 asociado con esa puerta.

Notifique a los usuarios del cliente TN5250 los números de puerta que han de configurar para sus aplicaciones de emulador para conectarse a AS/400 específicos.

Filtro de IP

Communications Server le permite configurar los filtros TN5250 para especificar qué clientes TCP/IP pueden conectarse al servidor. Se pueden especificar los clientes utilizando direcciones IP individuales, subredes IP o nombres del sistema principal TCP/IP o nombres de dominio.

También puede configurar un AS/400 con un filtro para especificar un AS/400 diferente del asociado con la puerta. Esto se puede utilizar para direccionar los clientes asociados con un filtro a un AS/400 específico.

Puede especificarse más de un AS/400 en un filtro. Si el intento de una conexión cliente con el primer AS/400 especificado no es satisfactorio, se intenta la conexión con otro AS/400 especificado en el filtro.

Soporte de capa de sockets segura (SSL)

Cuando configure una nueva puerta de servidor TN5250, puede especificar la puerta que se ha de utilizar para las conexiones seguras. Puede especificarse más de una puerta como segura.

Para habilitar la seguridad, Communications Server proporciona el programa de utilidad **Gestión de llamadas clave** para generar certificaciones y claves que son necesarias para SSL. Consulte el apartado “Planificación de la seguridad basada en la capa de sockets segura” en la página 135 para obtener más información.

Cuando haya configurado y habilitado la seguridad, los clientes TN5250 que den soporte a SSL Versión 3 podrán conectarse a un número de puerta segura y establecer conexiones seguras.

Configuración de redes SNA

Necesita configurar la red SNA para permitir que el servidor TN5250 se conecte a los AS/400. Consulte la publicación *Quick Beginnings* para obtener información sobre la configuración de la red SNA para el servidor TN5250.

Equilibrio de la carga de servidores TN5250

Communications Server también da soporte al equilibrio de la carga de clientes TN5250 en múltiples servidores TN5250. Consulte el apartado “Planificación del equilibrio de la carga” en la página 145 para obtener más información.

Planificación de la seguridad basada en la capa de sockets segura

Puede utilizar la seguridad basada en la Capa de sockets segura (basada en SSL) en las conexiones entre los clientes TN y el servidor TN3270E o el servidor TN5250. Esta seguridad utiliza SSL Versión 3 para proporcionar el cifrado de datos y la autentificación del servidor utilizando certificaciones firmadas.

Puede configurar puertas específicas para dar soporte a la seguridad basada en SSL. Si especifica la seguridad, el servidor debe obtener una certificación autentificada proporcionada por una autoridad certificada (CA). Communications Server proporciona un programa de utilidad que genera y gestiona las claves y certificaciones utilizadas por SSL Versión 3.

Este capítulo ofrece una visión general de la planificación de la seguridad basada en la Capa de sockets segura (basada en SSL). La seguridad basada en SSL se proporciona como una opción al configurar el servidor TN3270E y el servidor TN5250.

Cómo funciona la seguridad SSL

La Capa de sockets segura (SSL) es un protocolo estándar de la industria que utiliza tecnología de criptografía claves simétricas y de claves públicas. La criptografía de claves simétricas utiliza la misma clave para cifrar y descifrar los mensajes. La criptografía de clave pública utiliza un par de claves, una clave pública y una clave privada. Todas las claves públicas del servidor se publican y las claves privadas se mantienen en secreto. Para enviar un mensaje seguro al servidor, el cliente cifra el mensaje utilizando la clave pública del servidor. Cuando el servidor recibe el mensaje, lo descifra utilizando su clave privada.

SSL proporciona tres servicios de seguridad básicos:

- Privacidad de mensajes

  La privacidad de los mensajes se consigue a través de un cifrado que combina la clave pública y la clave simétrica. Todo el tráfico entre un cliente SSL y un servidor SSL se cifra utilizando una clave y un algoritmo de cifrado negociado durante la configuración de la sesión.

- Integridad de mensajes

  El servicio de integridad de los mensajes asegura que el tráfico de la sesión SSL no cambia en el direccionamiento a su destino final. SSL utiliza una combinación de claves públicas/privadas y funciones de generación para asegurar la integridad de los mensajes.

- Autentificación

  La autentificación es el proceso por el cual el cliente y el servidor se convencen mutuamente de sus identidades. Las identidades del cliente y del servidor se codifican en las certificaciones de clave pública. La certificación de clave pública se compone de lo siguiente:

  – Nombre diferenciado del sujeto

  – Nombre diferenciado del emisor

© Copyright IBM Corp. 1989, 1996

- Clave pública del sujeto
- Firma del emisor
- Período de validez
- Número de serie

Nota: Communications Server da soporte a la autentificación correspondiente al servidor. Sólo el servidor seguro necesita la autentificación de la autoridad de certificación (CA) para permitir el establecimiento de una conexión de TN3270E o TN5250.

Soporte de SSL de Communications Server

Communications Server da soporte a los siguientes componentes de la seguridad SSL:

- Sesiones SSL seguras entre el servidor TN3270E y cualquier cliente TN3270 y TN3270E que de soporte a SSL Versión 3
- Las sesiones SSL seguras entre el servidor TN5250 y cualquier cliente TN5250 que de soporte a SSL Versión 3
- SSL Versión 3
- Privacidad e integridad de los mensajes
- Autentificación correspondiente al servidor

Configuración de la seguridad SSL

Durante la configuración del servidor TN3270E y del servidor TN5250, se especifican las puertas que la seguridad SSL utilizará para sus conexiones. Consulte el apartado “Planificación del servidor TN3270E” en la página 123 y “Planificación del servidor TN5250” en la página 129 para obtener más información sobre la configuración de puertas seguras.

Para habilitar la seguridad SSL con la autentificación del servidor, se necesita un conjunto de claves públicas/privadas y una certificación de clave pública autentificada asociada. Communications Server proporciona el programa de utilidad **Gestión de llamadas clave** para crear, gestionar y almacenar claves públicas/privadas y certificaciones necesarias para SSL.

Utilizando el programa de utilidad **Gestión de llamadas clave**, debe llevar a cabo una de las siguientes acciones:

- Crear un par de claves públicas/privadas y obtener y almacenar una certificación de las autoridades de certificaciones (CA) predefinidas (conocidas).

  Este procedimiento necesita menos configuración porque el archivo de base de datos de claves está preconfigurado con las certificaciones raíz CA necesarias para identificar las CA desde las que se emite la certificación.
- Cree un par de claves públicas/privadas, defina una CA desconocida obteniendo y almacenando la certificación raíz de CA en el archivo de base de datos de claves , y obtenga y almacene una certificación de la CA desconocida.

- Cree una certificación de firma propia y almacénela en el archivo de base de datos de claves .

  Nota: Para asegurar la seguridad adecuada para su sitio, debe utilizar la certificación de firma propia sólo con el propósito de comprobación controlada.

Programa de utilidad de gestión de llamadas clave

El programa de utilidad **Gestión de llamadas clave** de Communications Server, le permite crear, gestionar y almacenar las claves públicas/privadas y las certificaciones necesarias para las comunicaciones SSL entre Communications Server y el cliente. Antes de empezar la configuración de las comunicaciones SSL, debe abrir el archivo de base de datos de claves de Communications Server. Utilice los pasos siguientes para abrir el archivo:

1. Seleccione **Archivo de base de datos de claves** en el menú principal y seleccione **Abrir** para abrir una base de datos de claves existente.
2. En la ventana **Abrir**, seleccione el subdirectorio **private** del directorio en el que ha instalado el producto (por ejemplo, C:\IBMCS\PRIVATE).
3. Elija **ibmcs.kdb** como base de datos de claves
4. En la solicitud de contraseña, entre la suya.

   Nota: La contraseña se establece inicialmente en **ibmcs**. Para la seguridad adecuada, ***debe*** cambiar la contraseña antes de realizar cualquiera de las tareas de **Gestión de llamadas clave**.

Cambio de contraseña

Utilice los pasos siguientes para cambiar la contraseña de la base de datos actual:

1. Seleccione **Archivo de base de datos de claves** en el menú y seleccione **Cambiar contraseña** para cambiar la contraseña de la base de datos de claves para la base de datos actual. Aparece el diálogo de archivo **Cambiar contraseña**.
2. Entre la nueva contraseña que desee utilizar.
3. Entre la misma contraseña de nuevo para verificarla.
4. Si desea que la contraseña tenga una fecha de caducidad, pulse en **Establecer tiempo de caducidad**. Para asegurar una seguridad adecuada, la contraseña debe tener una fecha de caducidad.
5. Si elige permitir que caduque la contraseña, especifique el número de días que han de pasar para que la contraseña caduque.
6. Pulse en **Ocultar la contraseña** para ocultar la contraseña de la base de datos actual.

Configuración de SSL utilizando una CA fiable conocida

Siga los procedimientos de esta sección para configurar la seguridad SSL utilizando una certificación emitida por una CA conocida. Las siguientes certificaciones firmadas de CA ya están almacenadas en la base de datos de claves y marcadas como certificaciones fiables:

- Integrion Certification Authority Root

- IBM World Registry Certification Authority
- CA Thawte Personal Premium
- CA Thawte Personal Freemail
- CA Thawte Personal Basic
- CA Thawte Premium Server
- CA de servidor seguro Thawte Server CA RSA (también se obtiene de VeriSign)
- CA primaria pública VeriSign clase 4
- CA primaria pública VeriSign clase 3
- CA primaria pública VeriSign clase 2
- CA primaria pública VeriSign clase 1

Para configurar la seguridad SSL utilizando una CA conocida, son necesarios los siguientes procedimientos:

- Crear una petición de certificación y clave
- Someter una petición de certificación a la CA
- Obtener y almacenar una certificación en la base de datos de claves del servidor

Creación de una petición de certificación y clave

Siga los pasos siguientes del programa de utilidad **Gestión de anillo de claves** para crear las claves públicas/privadas y la petición de certificación:

1. Seleccione **Peticiones de certificaciones personales** en la lista desplegable del menú principal y pulse en **Nueva** para crear un par de claves nuevas y una petición de certificación. Aparece el diálogo **Crear nueva clave y petición de certificación**.
2. Entre el nombre (etiqueta) que se utiliza para identificar la clave y la certificación dentro de la base de datos.
3. Entre el número de tamaño de clave que desea utilizar. La elección de un tamaño de clave mayor da como resultado una seguridad más fuerte, pero necesita un proceso mayor en el cliente y en el servidor para establecer una conexión.
4. Entre el nombre de sistema principal TCP/IP del servidor de comunicaciones como el nombre común (por ejemplo, wtr05306.raleigh.ibm.com).
5. Entre un nombre de organización.
6. Entre una unidad de organización (opcional).
7. Entre una ciudad o localidad (opcional).
8. Entre un estado o provincia (opcional).
9. Entre un código postal (opcional).
10. Entre un código de país. Debe especificar un mínimo de 2 caracteres (por ejemplo, US).
11. Entre un nombre de archivo de petición de certificación o utilice el nombre de archivo por omisión.

Cuando pulse en **Aceptar**, se procesará la información que ha suministrado. Se producen dos archivos:

ibmcs.rdb Archivo de clave privada

certreq.arm Es el nombre por omisión del archivo de petición de certificación. Si ha asignado un nombre de archivo, se crea un nombre de archivo con este nombre. El archivo de petición de certificación es un archivo de tipo PKCS 10 en formato 64 blindado.

No trate de editar ni mover estos archivos. Si no se puede encontrar el archivo **ibmcs.rdb** o se ha dañado cuando ha tratado de entrar la certificación en la base de datos de claves , tendrá que volver a someter la petición de certificación a la CA.

Sumisión de una petición de certificación

Inicie un navegador Web y el acceso de página Web para la CA. Siga las instrucciones proporcionadas para someter la petición de certificación. Las siguientes son URL de algunas CA conocidas:

- VeriSign: **http://www.verisign.com/**
- Thawte: **http://www.thawte.com/**

Dependiendo de la CA que elija, envíe por correo electrónico la petición de certificación generada por el programa de utilidad **Gestión de anillo de claves** o incorpore la la petición de certificación en el formato o archivo proporcionado por la CA.

Después de someter una petición de certificación a una CA, puede habilitar la seguridad SSL creando y almacenando una certificación con firma propia. Sólo debe utilizarse una certificación con firma propia con propósito de prueba controlada. Consulte el apartado “Creación de una certificación con firma propia” en la página 142 para obtener más información.

Almacenamiento de una certificación en la base de datos de claves

Cuando reciba una certificación de una CA, utilice el programa de utilidad **Gestión de anillo de claves** para poner la certificación en el archivo de base de datos de claves , **ibmcs.kdb**, ubicado en el servidor.

1. Seleccione **Certificaciones personales** en la lista desplegable del programa de utilidad **Gestión de llamadas clave** y pulse en **Recibir** para recibir el par de claves y la petición de certificación. Aparece el diálogo **Recibir certificación de un archivo**.
2. Asegúrese de que el tipo de datos es **datos ASCII blindados BASE64** (formato 64 blindado).
3. Entre el nombre de archivo de certificación.
4. Entre la ubicación (nombre de vía de acceso) de la certificación. Pulse en **Aceptar**. Se visualiza la certificación almacenada como el primer elemento.
5. Resalte la certificación almacenada y pulse en **Ver/Editar**. Aparece el diálogo **Información de clave**.
6. Pulse en **Establecer certificación como valor por omisión**. La clave seleccionada se convierte en el valor por omisión.

Configuración de SSL utilizando una CA desconocida

Para configurar la seguridad SSL utilizando una CA desconocida (que todavía no se ha definido en la base de datos), son necesarios los siguientes procedimientos:

- Crear una petición de certificación y clave
- Someter una petición de certificación a la CA
- Obtener una certificación raíz de CA y su certificación y almacenarlas en la base de datos de claves .

Creación de una petición de certificación y clave

Siga los pasos siguientes del programa de utilidad **Gestión de anillo de claves** para crear las claves públicas/privadas y la petición de certificación:

1. Seleccione **Peticiones de certificaciones personales** en la lista desplegable del menú principal y pulse en **Nueva** para crear un par de claves nuevas y una petición de certificación. Aparece el diálogo **Crear nueva clave y petición de certificación**.
2. Entre el nombre (etiqueta) que se utiliza para identificar la clave y la certificación dentro de la base de datos.
3. Entre el número de tamaño de clave que desea utilizar. La elección de un tamaño de clave mayor da como resultado una seguridad más fuerte, pero necesita un proceso mayor en el cliente y en el servidor para establecer una conexión.
4. Entre el nombre de sistema principal TCP/IP del servidor de comunicaciones como el nombre común (por ejemplo, wtr05306.raleigh.ibm.com).
5. Entre un nombre de organización.
6. Entre una unidad de organización (opcional).
7. Entre una ciudad o localidad (opcional).
8. Entre un estado o provincia (opcional).
9. Entre un código postal (opcional).
10. Entre un código de país. Debe especificar un mínimo de 2 caracteres (por ejemplo, US).
11. Entre un nombre de archivo de petición de certificación o utilice el nombre de archivo por omisión.

Cuando pulse en **Aceptar**, se procesará la información que ha suministrado. Se producen dos archivos:

ibmcs.rdb Archivo de clave privada

certreq.arm Es el nombre por omisión del archivo de petición de certificación. Si ha asignado un nombre de archivo, se crea un nombre de archivo con este nombre. El archivo de petición de certificación es un archivo de tipo PKCS 10 en formato 64 blindado.

No trate de editar ni mover estos archivos. Si no se puede encontrar el archivo **ibmcs.rdb** o se ha dañado cuando ha tratado de entrar la certificación en la base de datos de claves , tendrá que volver a someter la petición de certificación a la CA.

Sumisión de una petición de certificación

Siga los procedimientos de la CA desconocida para someter la petición de certificación.

Dependiendo de la CA que elija, envíe por correo electrónico la petición de certificación generada por el programa de utilidad **Gestión de anillo de claves** o incorpore la la petición de certificación en el formato o archivo proporcionado por la CA.

Después de someter una petición de certificación a una CA, puede habilitar la seguridad SSL creando y almacenando una certificación con firma propia. Sólo debe utilizarse una certificación con firma propia con propósito de prueba controlada. Consulte el apartado “Creación de una certificación con firma propia” en la página 142 para obtener más información.

Almacenamiento de una certificación en la base de datos de claves

Cuando reciba una certificación de una CA, póngase en contacto con la CA para obtener la certificación raíz de la CA. Debe almacenar la certificación raíz de la CA en la base de datos de claves antes de almacenar la certificación que ha solicitado. La certificación raíz de CA valida la certificación que ha solicitado. Utilice el programa de utilidad **Gestión de llamadas clave** para almacenar la certificación raíz de CA.

1. Seleccione **Firmante de certificaciones** en la lista desplegable y pulse **Recibir** para recibir el par de claves y la petición de certificación. Aparece el diálogo **Recibir certificación de un archivo**.
2. Asegúrese de que el tipo de datos es **datos ASCII blindados BASE64** (formato 64 blindado).
3. Entre el nombre de archivo de certificación.
4. Entre la ubicación (nombre de vía de acceso) de la certificación. Pulse en **Aceptar**. El archivo se marca como ***fiable*** y se almacena.

Para almacenar la certificación que ha solicitado, utilice el programa de utilidad **Gestión de anillo de claves** para poner la certificación en el archivo de llamadas clave , **ibmcs.kdb**, ubicado en el servidor.

1. Seleccione **Certificaciones personales** en la lista desplegable del menú principal y pulse **Recibir** para recibir el par de claves y la petición de certificación. Aparece el diálogo **Recibir certificación de un archivo**.
2. Asegúrese de que el tipo de datos es **datos ASCII blindados BASE64** (formato 64 blindado).
3. Entre el nombre de archivo de certificación.
4. Entre la ubicación (nombre de vía de acceso) de la certificación. Pulse en **Aceptar**. Se visualiza la certificación almacenada como el primer elemento.
5. Resalte la certificación almacenada y pulse en **Ver/Editar**. Aparece el diálogo **Información de clave**.
6. Pulse en **Establecer certificación como valor por omisión**. La clave seleccionada se convierte en el valor por omisión.

Creación de una certificación con firma propia

La recepción de una certificación de una CA fiable conocida puede tardar hasta tres semanas. Hasta que reciba la certificación de servidor público, puede crear una certificación con firma propia para habilitar las sesiones SSL entre los clientes y el servidor. Sólo debe utilizarse una certificación con firma propia con propósito de prueba controlada. Para asegurar seguridad adecuada para su sitio, no debe utilizar la certificación de firma propia en un entorno de producción. Para configurar el sitio para utilizar una certificación con firma propia utilizando el programa de utilidad **Gestión de llamadas clave**, siga estos pasos:

1. Seleccione **Nueva certificación con firma propia** en la opción de menú **Crear** para crear una nueva certificación con firma propia. Aparece el diálogo **Crear nueva certificación con firma propia**.
2. Entre el nombre (etiqueta) que se utiliza para identificar la clave y la certificación dentro de la base de datos. Seleccione **X509 V3** como la versión de la certificación.
3. Entre el número de tamaño de clave que desea utilizar. La elección de un tamaño de clave mayor da como resultado una seguridad más fuerte, pero necesita un proceso mayor en el cliente y en el servidor para establecer una conexión.
4. Entre el nombre de sistema principal TCP/IP del servidor de comunicaciones como el nombre común (por ejemplo, wtr05306.raleigh.ibm.com).
5. Entre un nombre de organización.
6. Entre una unidad de organización (opcional).
7. Entre una ciudad o localidad (opcional).
8. Entre un estado o provincia (opcional).
9. Entre un código postal (opcional).
10. Entre un código de país. Debe especificar un mínimo de 2 caracteres (por ejemplo, US).
11. Entre el número de días de validez de la certificación con firma propia.
12. Pulse en **Aceptar**.
13. Pulse en **Sí** para establecer la clave como la clave por omisión en la base de datos de claves.

Si utiliza IBM eNetwork Host On-Demand o algún otro cliente SSL para el que sea necesario asignar una certificación de firma propia, utilizando el programa de utilidad **Gestión de llamadas clave**, siga estos pasos:

1. Seleccione **Certificaciones personales** en la lista desplegable, resalte la certificación con firma propia y pulse en **Extraer certificación**. Aparece el diálogo **Extraer certificación a un archivo.**.
2. Seleccione **Datos DER binarios** como el tipo de datos.
3. Entre el nombre de archivo de certificación. El archivo debe tener un tipo de archivo **der** (por ejemplo, ibmcs.crt).
4. Entre la ubicación (nombre de vía de acceso) de la certificación.
5. Pulse en **Aceptar**.

Debe suministrarse el archivo de certificación a cada cliente autorizado para conectarse con el servidor. Consulte la documentación del cliente para obtener instrucciones sobre el almacenamiento de la certificación con firma propia como una certificación raíz de CA en el archivo de clase de cliente o en la base de datos de claves .

Planificación del equilibrio de la carga

Este capítulo ofrece una visión general de la planificación del equilibro de la carga. Describe la planificación del equilibrio de la carga de LU dependientes y de LU 6.2.

Equilibrio de la carga de LU dependientes

El equilibrio de la carga le permite equilibrar las sesiones de sistemas principales dependientes en los servidores. Se da soporte al equilibrio de la carga para aplicaciones API LUx a través de clientes API SNA, emuladores 3270 y emuladores TN3270.

Cuando Communications Server responde a las peticiones de clientes, clasifica los servidores que dan soporte a la agrupación pedida por la carga.

La carga de las LU dependientes representa un porcentaje de recursos disponibles de un servidor en particular. El porcentaje de carga se calcula dividiendo el número de conexiones de aplicación activas por el número total de LU (de 0 a 3) disponibles.

Puede influir en la carga calculada especificando un factor de carga de LU0 a LUO3 (el factor de carga de la sesión del sistema principal) para compensar las diferencias entre dos servidores como, por ejemplo, la memoria disponible, la velocidad del procesador y la utilización de CPU. También puede utilizar el factor de carga LU0 a 3 para equilibrar las cargas entre los servidores Communications Server y Novell IntranetWare para SAA.

Notas:

1. Los servidores que participan en el equilibrio de la carga se determinan por pertenecer al grupo de LU y al ámbito. Todos los servidores Communications Server con LU en sus agrupaciones del mismo nombre están sujetos al equilibrio de la carga.
2. Los clientes que utilizan el protocolo TCP/IP pueden participar en el equilibrio de la carga. Sin embargo, los clientes TCP/IP sólo pueden realizar el equilibrio de la carga entre servidores IBM Communications Server. El equilibrio de la carga está determinado por los ámbitos configurados.

En Communications Server, si las agrupaciones de LU de diferentes servidores tienen el mismo nombre, funcionan como una agrupación para el equilibrio de la carga. Cuando asigne LU a una agrupación de LU, seleccione los enlaces con el sistema principal en un servidor y asigne las LU del enlace con el sistema principal seleccionado a la agrupación de LU. Estas LU no necesitan tener el mismo tipo de LU. También, la agrupación resultante puede contener LU de múltiples enlaces.

Equilibrio de la carga de LU 6.2

El equilibrio de la carga le permite equilibrar sesiones de LU 6.2 independientes distribuyéndolas entre múltiples servidores. Se da soporte al equilibrio de la carga para aplicaciones API APPC a través de clientes API SNA y emuladores TN5250.

© Copyright IBM Corp. 1989, 1996

La carga para LU6.2 representa un porcentaje de los recursos disponibles de un servidor en particular. El porcentaje de la carga se calcula dividiendo el número total de conversaciones sobre todas las LU locales de un servidor en particular mediante el límite máximo acumulado de sesiones para todas las LU locales. El límite máximo de sesiones es el límite de sesiones LU 6.2 especificado durante la configuración. Si el límite máximo de sesiones se especifica como cero (0), que indica que no hay ningún límite de sesiones, se utiliza el límite máximo de sesiones de LU local por omisión de 512 por LU local cuando se calcula la carga. El límite máximo de sesiones de LU local por omisión también puede especificarse durante la configuración.

Puede influir en la carga calculada especificando un factor de carga de LU6.2 (factor de carga de sesión APPC) para compensar las diferencias entre dos servidores como, por ejemplo, la memoria disponible, la velocidad de procesador y la utilización de CPU. También pude utilizar el factor de carga LU6.2 para equilibrar las cargas entre los servidores Communications Server y Novell IntranetWare para SAA.

Nota: Los clientes que utilizan el protocolo TCP/IP pueden participar en el equilibrio de la carga de LU 6.2.

Planificación de ámbitos TCP/IP

Ámbito es un parámetro utilizado para controlar y gestionar el acceso de clientes TCP/IP a servidores de una red. Es igual que el ámbito del protocolo de ubicación de servicio (SLP) tal como se hace referencia en RFC 2165. Communications Server utiliza el SLP para implantar el equilibrio de la carga basada en TCP/IP.

El ámbito de control proporcionado es necesario por dos razones:

- Cuando crece la red, el número de clientes y el número de servidores, es necesario particionar el acceso a los servidores entre el número creciente de clientes para reducir el tráfico global de la red.
- El ámbito de control permite a los administradores organizar los usuarios y los servidores en grupos de administración.

El significado de los valores del ámbito los define el administrador de la red. Estos valores pueden representar a cualquier entidad. Normalmente, son las líneas de departamentos, geográficas o de organización.

Una vez configurado, los clientes pueden llegar a la red SNA a través de servidores que están configurados con el mismo ámbito o que no tienen ningún ámbito asociado (servicios o servidores ***sin ámbito***).

Nota: Si se configura un servidor como sin ámbito, responde a las peticiones SLP con ámbito **y** sin ámbito. Si el cliente API SNA está configurado para conectarse con servidores sin ámbito, sólo responderán los servidores sin ámbito.

Ámbitos y seguridad del servidor de clientes

Communications Server permite que los clientes Novell IntranetWare para SAA utilicen la seguridad del dominio Windows NT para autentificar la conexión con el servidor sin volver a entrar el id de usuario y la contraseña. El cliente debe formar parte de un dominio Windows NT, por ser partícipe de un dominio de Communications Server o por conectarse localmente con un id de usuario y una contraseña sincronizados.

Los usuarios autorizados para un servidor de clientes se mantienen en el grupo local IBMCSAPI, que está ubicado directamente en el Communications Server o en el controlador del dominio en el que Communications Server participa. Este grupo de usuarios se crea durante la instalación y puede administrarse utilizando la aplicación Administrador de usuarios de Windows NT.

Los usuarios de clientes Novell IntranetWare para SAA, fuera del dominio Windows NT deben reproducir el id de usuario y la contraseña en todos los servidores configurados con el mismo ámbito.

Dónde está configurado el ámbito

Cada servidor se asigna a un ámbito o ámbitos a través de **Configuración de nodos**. Los clientes que utilicen estos servidores deben estar configurados para conectarse a servidores de un solo ámbito específico o con servidores sin ámbito. Para obtener más información sobre la configuración de clientes, consulte el manual *Client/Server Communications Programming*.

Cómo se relaciona el ámbito con SLP

El ámbito de Communications Server se relaciona directamente con el ámbito del protocolo de ubicación de servicio (SLP). Por lo tanto, los agentes de directorio SLP pueden residir en la red que da soporte a los ámbitos configurados de Communications Server. Si piensa permitir que los clientes localicen los servicios de Communications Server basándose en los ámbitos, tome en consideración la forma en que el ámbito se relaciona con la red como un todo. Si hay servicios sin ámbito en una red en la que también se utilizan ámbitos, los servicios sin ámbito se pueden elegir para satisfacer cualquier petición con ámbito, lo que puede poner potencialmente una carga en los agentes de servicio y los agentes de directorio que dan soporte a los servicios sin ámbito.

Nota: Si el cliente API SNA está configurado para conectarse con servidores sin ámbito, sólo responderán los servidores sin ámbito.

Si se han de utilizar agentes de directorio en la red del local (para el ajuste por arriba), deben estar configurados para manejar los mismos ámbitos que están configurados para el Communications Server. Además, si se han de utilizar servicios sin ámbito en redes con agentes de directorio, debe configurarse como mínimo un agente de directorio sin ámbito.

Communications Server incluye un agente de servicio SLP que está instalado en cada servidor en que está instalado Communications Server. No es necesario instalar ningún soporte SLP adicional en la red para que el equilibrio de la carga TCP/IP y el descubrimiento de Communications Server funcionen correctamente.

Seguimiento de la carga actual

Puede hacer un seguimiento de la carga actual en las LU 6.2 y LU dependientes utilizando el Supervisor de rendimiento de Windows NT. Puede iniciar el supervisor de rendimiento desde la selección en **Herramientas de administración (Común)** del menú **Programas**.

En la pantalla del supervisor de rendimiento, seleccione **Añadir a diagrama** del menú desplegable **Editar**. En el campo **Objeto**, seleccione **Equilibrio de la carga SNA de IBM**. Los dos contadores listados son:

Carga de LU0/LU3 Utilice este contador para hacer un seguimiento de la carga de LU dependientes.

Carga de LU6.2 Utilice este contador para hacer un seguimiento de la carga de LU 6.2.

Los resultados del seguimiento de la carga pueden guardarse para próximas consultas.

Planificación de las conexiones del sistema principal de reserva

Para los entornos en los que puede ser importante proporcionar conexiones del sistema principal de reserva para las conexiones primarias que utilizan las sesiones de emulador de estación de trabajo, Communications Server le proporciona opciones que permiten la configuración de las conexiones del sistema principal que se activan en respuesta a condiciones de anomalía. Las opciones que puede utilizar para ello dependen del nivel de reserva que desee proporcionar:

- Para habilitar un sistema de reserva completo entre los nodos que dan soporte a las sesiones de emulador de estación de trabajo IPX o IP de la LAN, incluya la espera en caliente en el entorno.
- Para habilitar un sistema de reserva completo entre los nodos del servidor que dan soporte a otras sesiones de emulador de la estación de trabajo IP o IPX basadas en la LAN, no incluya la espera en caliente en el entorno. Configure una instalación de Communications Server duplicada en el sistema de reserva.
- Para habilitar la copia de reserva dentro de un nodo del servidor, no utilice la espera en caliente. Utilice las opciones normales en las definiciones de conexión en el entorno de reserva.

Estas opciones se explican en las secciones siguientes.

Planificación de conexiones de reserva entre servidores que utilizan la espera en caliente

En Communications Server, puede configurar enlaces del sistema principal para que se activen automáticamente si falla el servidor crítico. Las conexiones configuradas para un sistema principal pueden continuar funcionando mediante la activación de conexiones alternativas en un servidor de reserva. Esta función se conoce como espera en caliente.

Para el usuario de una sesión de emulador de estación de trabajo con una máquina de sistema principal cuya conexión inicial falla debido a una anomalía de Communications Server, la espera en caliente permite un posterior intento de restablecer la conexión con la máquina de sistema principal, realizando automáticamente el direccionamiento a través de un Communications Server alternativo. El servidor inicial que proporciona la conexión se conoce como el ***servidor crítico***. El servidor alternativo que proporciona una conexión con la máquina de sistema principal después de la anomalía del servidor crítico se conoce como el ***servidor de reserva***. El servidor de reserva proporciona conexiones que se inician automáticamente en respuesta a la detección de una anomalía del servidor crítico y los cargos de licencia relacionados con la conectividad del sistema principal del servidor crítico se gestionan automáticamente en el servidor de reserva.

Un servidor puede ser un servidor crítico y un servidor de reserva a la vez. Los servidores pueden servir de reserva entre sí.

La espera en caliente permite que el servidor de reserva de soporte a sesiones de emulador IP o IPX basadas en la LAN. La espera en caliente no proporciona el soporte de servidor de reserva para el entorno SNA.

© Copyright IBM Corp. 1989, 1996

En la Figura 38 en la página 150, el servidor de reserva está configurado con una conexión de reserva completa para HOSTCON1, que proporciona la conectividad de sistema principal primaria en el servidor crítico. Las líneas de puntos entre el servidor de reserva y los clientes de emulador de estación de trabajo no se activan mientras el servidor crítico esté en funcionamiento.

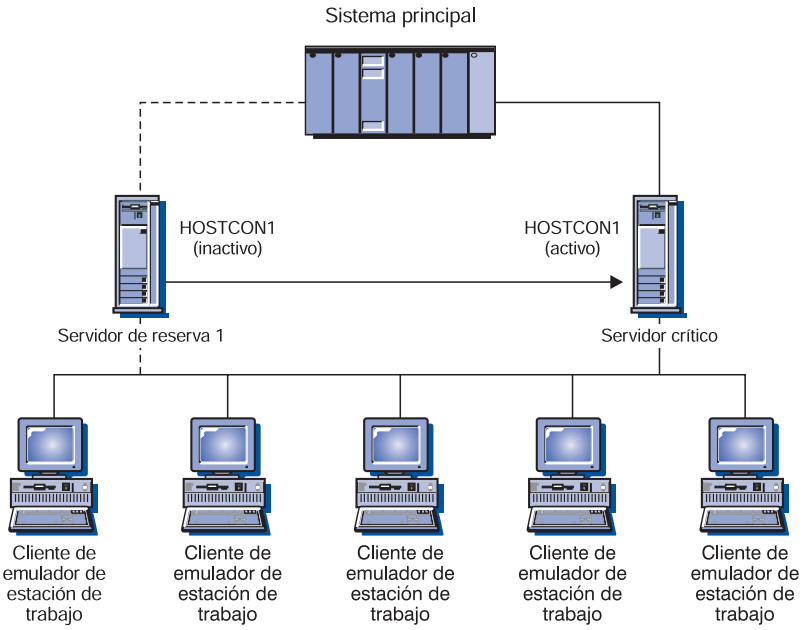


Figura 38. Un servidor crítico con un servidor de reserva

En la Figura 39 en la página 151, cada uno de los servidores de reserva está configurado con una conexión de reserva parcial para HOSTCON1, que proporciona la conectividad del sistema principal primario en el servidor crítico. La combinación de los dos servidores de reserva proporciona una reserva completa para HOSTCON1. Las líneas de puntos entre los servidores de reserva y los clientes de emulador de estación de trabajo no están activos mientras el servidor crítico está funcionando.

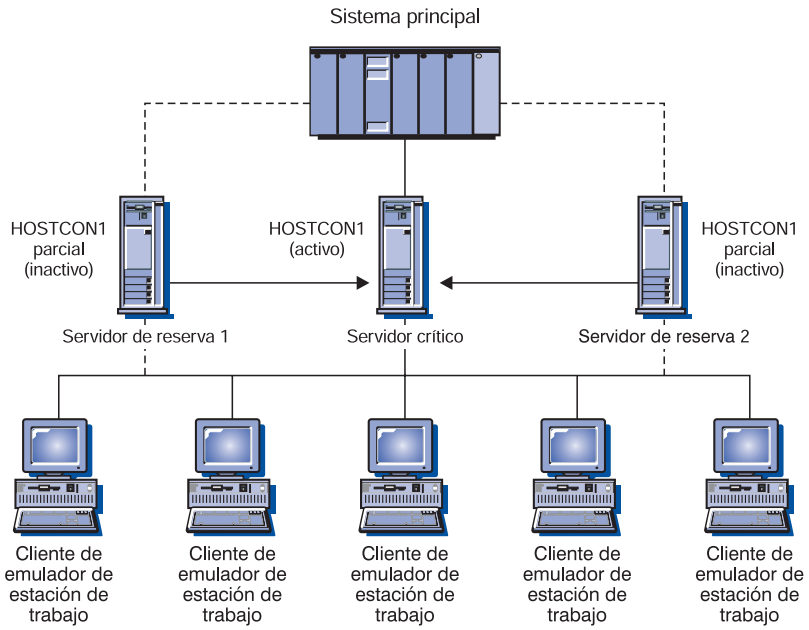


Figura 39. Un servidor crítico con dos servidores de reserva

Si falla el servidor crítico, la recuperación se produce de la manera siguiente:

1. El servidor de reserva, el sistema principal y el software de emulador de estación de trabajo que hay en la estación de trabajo detectan la anomalía prácticamente a la vez.
2. Las conexiones nombradas en la configuración del servidor crítico del servidor de reserva se activan automáticamente y se establece su conectividad con la máquina del sistema principal.
3. La estación de trabajo establece una nueva sesión con el servidor de reserva que acaba de activar sus conexiones de servidor crítico.
4. La estación de trabajo se pone en contacto con la máquina del sistema principal y visualiza una solicitud de conexión para el usuario.

Nota: Cuando el servidor crítico vuelve a estar activo, las conexiones del servidor de reserva activadas no se desactivan automáticamente. Debe desactivar manualmente las conexiones del servidor de reserva.

Utilización de un servidor de reserva de producción o dedicado para la espera en caliente

No puede instalar las mismas licencias de Communications Server en más de un servidor que se ejecute en la misma red. Instale Communications Server en múltiples servidores adquiriendo un paquete adicional de Communications Server para cada servidor adicional.

Antes de configurar Communications Server para la espera en caliente, decida si va a ejecutar Communications Server como servidor de producción y servidor de reserva o sólo como servidor de reserva dedicado.

Utilización de un servidor de producción

Un ***servidor de producción*** es un Communications Server que cuida los requisitos de comunicación diarios. Este entorno configura Communications Server con conexiones de sistema principal que se activan fuera de un escenario de anomalía del servidor crítico. Para la activación y utilización de estas conexiones se necesita adquirir las licencias adecuadas para ellas. No puede instalar las mismas licencias de Communications Server en más de un servidor. Para instalar Communications Server para utilizarlo como servidor de producción en múltiples sistemas, debe adquirir un paquete adicional de Communications Server para cada instalación de servidor adicional.

Cuando se utiliza un Communications Server como servidor de producción y servidor de reserva, no es necesario tomar en consideración la licencia. Se instala Communications Server y las licencias que ha adquirido para utilizar el Communications Server como servidor de producción.

La función del Communications Server como servidor de reserva no necesita ninguna licencia adicional aparte de la licencia básica adquirida para los servidores críticos que está configurado para supervisar. No es necesaria tomar en consideración ninguna licencia especial en el servidor de reserva. Cuando el servidor de reserva detecta una anomalía de un servidor crítico, el servidor de reserva activa automáticamente las conexiones configuradas para el servidor crítico y ajusta las licencias del servidor de reserva basándose en las que están en vigor para el servidor crítico. Communications Server gestiona la licencia de la espera en caliente sin que intervenga el usuario.

Sin embargo, si las conexiones configuradas para el servidor crítico ya se han activado aparte del escenario de anomalía del servidor crítico, no se realiza el ajuste del servidor de reserva para las licencias del servidor crítico y es necesaria una licencia independiente en el servidor de reserva.

Utilización de un servidor dedicado

Un servidor de reserva ***dedicado*** no funciona como servidor de producción y no activa las conexiones fuera de un escenario de anomalía de servidor crítico. No se puede activar ninguna conexión en él en el arranque ni manualmente. Su función es supervisar uno o varios servidores críticos.

Un servidor de reserva dedicado no necesita licencias adicionales aparte de la licencia básica adquirida para los servidores críticos que está configurado para supervisar. Communications Server gestiona la licencia de la espera en caliente sin que intervenga el usuario.

Planificación del entorno completo de espera en caliente

Los escenarios para utilizar la espera en caliente implican los escenarios funcionales normales de Communications Server para dar soporte a los clientes de emulador basados en la LAN sobre IP o IPX, con algunas operaciones específicas de espera en caliente.

Para configurar un entorno de espera en caliente, hay dos dependencias básicas:

- Deben estar configurados dos o más servidores de comunicaciones para proporcionar conexiones compatibles con una máquina del sistema principal. El servidor utilizado como reserva debe estar configurado con la configuración del

servidor crítico que suministra la conectividad primaria a la máquina del sistema principal.

- El software del cliente de emulador de la estación de trabajo utilizado para conectarse a través del servidor para proporcionar a los usuarios las sesiones de emulador en la máquina del sistema principal debe dar soporte a algún medio de efectuar un direccionamiento alternativo al servidor de reserva en el caso de una anomalía del servidor crítico.

Es posible que algunos clientes de emulador no proporcionen el direccionamiento alternativo. La planificación de un entorno de espera en caliente necesita una evaluación cuidadosa del software de emulador y del tipo de conectividad utilizada entre el cliente y el servidor. Algunas opciones de direccionamiento alternativo son las siguientes:

- **Giro activo** - Hace referencia a dar soporte en un cliente de emulador a la configuración de múltiples servidores con nombre con los que se ha de establecer contacto, en un orden específico, para establecer una conexión a través del servidor con la máquina del sistema principal para una sesión de emulador. El giro activo le permite configurar el servidor de reserva con el que ha de contactar cuando los intentos de contactar el servidor crítico no son satisfactorios. Cuando el servidor crítico falla y los recursos del servidor de reserva están activados, el cliente de emulador contacta con el servidor de reserva y establece una ruta alternativa a través del mismo para la conexión con la máquina del sistema principal.
- **Agrupaciones de LU** - Hace referencia a dar soporte, en un cliente de emulador, a establecer dinámicamente la conexión con la máquina del sistema principal para una sesión de emulador, a través del servidor que responde actualmente a las consultas para las LU disponibles de una agrupación con nombre. El soporte de las agrupaciones de LU permite que el servidor de reserva y los servidores críticos proporcionen las LU para la misma agrupación. Inicialmente, el servidor de reserva está definido pero no activo. Cuando el servidor crítico falla y se activan los recursos del servidor de reserva, el servidor de reserva responde a las peticiones del cliente de emulador para una LU de la agrupación y establece una ruta alternativa a través del mismo para la conexión con la máquina del sistema principal. Las agrupaciones de LU incluyen los tipos siguientes de soporte de cliente para las agrupaciones de LU:
  - Soporte de Pre-SLP: Antes que Communications Server diera soporte a SLP, el acceso del cliente a las agrupaciones de LU era aleatorio o en un orden de servidor especificado.
  - Soporte SLP: El soporte de SLP de Communications Server proporciona el acceso del cliente a agrupaciones de LU, equilibrando la carga de sesiones entre los servidores que contribuyen a la agrupación.
- **Múltiples sesiones de emulador** - Hace referencia al soporte en un cliente de emulador para la configuración de múltiples sesiones de emulador, permitiendo al usuario configurar sesiones separadas que utilizan el servidor de reserva y los servidores críticos para conectarse a la máquina del sistema principal. La utilización de múltiples sesiones de emulador no es tan fácil como el giro activo o el soporte de agrupación de LU, porque necesita la intervención manual del usuario del emulador para ayudar en el direccionamiento alternativo cuando se produce una anomalía. Cuando falla la conexión del servidor crítico, el usuario

inicia manualmente la sesión configurada para utilizar el servidor de reserva para restablecer la conexión con la máquina del sistema principal.

El soporte de IBM Personal Communications de los clientes de emulador TN3270E, TN5250, API o QEL/MU proporciona opciones para el direccionamiento alternativo a través de una o varias opciones de giro activo, agrupaciones de LU o múltiples sesiones de emulador. Los clientes de emulador de algunos proveedores proporcionan opciones para un direccionamiento alternativo.

Configuración de espera en caliente en el servidor de reserva

En el panel **Configuración de nodos** avanzada, utilice la opción de configuración Configurar servidores críticos de espera en caliente para configurar la espera en caliente en el servidor de reserva.

No necesita realizar ninguna configuración de espera en caliente en el servidor crítico, pero el servidor de reserva necesita la configuración de espera en caliente. Utilizando la opción avanzada de **Configuración de nodos**, configure el servidor de reserva con las definiciones del servidor crítico. La definición del servidor crítico especifica el nombre del servidor crítico supervisado por el servidor de reserva y los nombres de las conexiones activadas cuando falla el servidor crítico. Se pueden configurar múltiples definiciones de servidor crítico, habilitando un servidor de reserva para supervisar y proporcionar la reserva a múltiples servidores críticos. Después de configurar las definiciones del servidor crítico en el servidor de reserva, reinicie el nodo del servidor de reserva para que los cambios surtan efecto. Para obtener información detallada sobre la configuración de la espera en caliente, consulte la ayuda en línea para **Configuración de nodos**.

Configuración de un entorno de espera en caliente

Siga estos pasos para configurar un entorno de espera en caliente:

1. **Configure el servidor crítico:** El servidor crítico se configura sin ninguna configuración relacionada de espera en caliente. Configure la conectividad del sistema principal para que coincida con la opción de direccionamiento alternativa utilizada con los clientes del emulador.
2. **Configure el servidor de reserva:** La configuración del servidor de reserva implica dos conceptos clave:
   a. La configuración de la conectividad del sistema principal en el servidor de reserva es similar a la del servidor crítico, excepto en que las conexiones del sistema principal están configuradas para la iniciación manual.
   b. La configuración del servidor crítico en el servidor de reserva para definir las conexiones del sistema principal iniciadas cuando se detecta una anomalía del servidor crítico.
3. **Configure los clientes de emulador:** Los clientes de emulador de estación de trabajo se configuran para que coincidan con una opción de direccionamiento alternativo para la conectividad que suministran los servidores.
4. **Inicie los nodos del servidor crítico y del servidor de reserva:** Inicie los nodos normalmente. **Operaciones de nodos SNA** puede verificar el estado de la espera en caliente para los servidores crítico y de reserva.
5. **Anomalía de servidor crítico:** Cuando falla el servidor crítico, la recuperación se produce de la siguiente manera:

a. El servidor de reserva, el sistema principal y el software de emulador de la estación de trabajo del cliente detectan la anomalía prácticamente a la vez.

b. Se activan las conexiones nombradas en la configuración del servidor crítico del servidor de reserva y se establece la conectividad con la máquina del sistema principal.

c. El cliente de emulador de estación de trabajo establece una nueva sesión con el servidor de reserva. El servidor de reserva direcciona las sesiones a la máquina del sistema principal a través de la conexión activada en el servidor de reserva cuando falla el servidor crítico.

d. La estación de trabajo se pone en contacto con la máquina del sistema principal y visualiza una solicitud de conexión para el usuario.

6. **Servidor crítico de nuevo en línea:** Cuando el servidor crítico vuelve a estar activo, las nuevas sesiones de emulador de de estación de trabajo utilizan la conectividad del sistema principal del servidor crítico. Las sesiones de emulador de estación de trabajo existentes direccionadas a través del servidor de reserva continúan funcionando hasta que se cierran las sesiones.

   Debe desactivar manualmente las conexiones con el sistema principal del servidor de reserva. La desactivación manual de las conexiones del servidor de reserva debe realizarse fuera de horas de trabajo. Debe notificarlo a los usuarios de las sesiones de emulador de estación de trabajo con el servidor de reserva antes de la desactivación de las conexiones.

Planificación de las conexiones de reserva entre servidores que no utilizan la espera en caliente

Debido a que la espera en caliente está limitada a entornos que dan soporte a las sesiones de emulador de estación de trabajo IP o IPX basadas en LAN, algunos entornos no pueden utilizar la espera en caliente para la conectividad de reserva. Muchas consideraciones para la planificación de un entorno de reserva sin espera en caliente son similares a la planificación de la reserva que utiliza la espera en caliente. Siga estos pasos para configurar un entorno de reserva que no utiliza la espera en caliente:

1. En el servidor de reserva, instale un paquete de Communications Server adquirido por separado con las licencias adecuadas para proporcionar las conexiones del sistema principal de reserva al servidor primario.
2. En el servidor de reserva, configure las conexiones del sistema principal utilizadas como reservas para activarse bajo petición.
3. Configure los clientes de emulador de estación de trabajo para que proporcionen el direccionamiento automático a los recursos del servidor de reserva cuando falle el servidor primario. Sin embargo, el direccionamiento debe tener limitado el acceso al servidor de reserva a solamente si se detecta una anomalía del servidor primario.
4. Se inician ambos nodos, pero sólo el nodo primario con sus conexiones en sentido ascendente activas suministra inicialmente la conectividad con el sistema principal.
5. Cuando falla el servidor primario, los clientes de emulador de estación de trabajo intentan las conexiones subsiguientes a través del servidor de reserva. Se activan las conexiones de sistema principal del servidor de reserva.

6. La licencia duplicada instalada en el servidor de reserva proporciona la disponibilidad del servidor de reserva a los clientes previamente direccionados a través del servidor primario.
7. Cuando el servidor primario vuelve a estar activo, las conexiones del servidor de reserva se desactivan manualmente.

Planificación de conexiones de reserva en un solo servidor

No puede utilizar la espera en caliente para la conectividad de reserva en un solo servidor, porque la espera en caliente sólo se aplica a entornos con conexiones de reserva entre servidores. Sin embargo, algunas consideraciones para la planificación de un entorno de reserva en un solo servidor son similares a la planificación de reserva que utiliza la espera en caliente. Las diferencias se resumen siguiendo los pasos para las conexiones de reserva de un solo servidor:

1. En el servidor que actúa como pasarela para el sistema principal, configure las conexiones primaria y de reserva que suministran las LU a la misma agrupación de LU, pero con la conexión de reserva configurada para activarse bajo petición.
2. Configure los clientes de emulador de estación de trabajo para que se conecten a través de la agrupación de LU.
3. Cuando falle la conexión primaria, o se agoten las LU de la agrupación, un intento de conexión con la agrupación inicia la activación de la conexión de reserva.
4. Cuando el servidor primario vuelve a estar activo, las conexiones del servidor de reserva se desactivan manualmente.

Planificación de X.25

Es necesario planificar cuidadosamente la configuración X.25. Necesita tomar en consideración lo siguiente:

- Para utilizar un PSDN público, es necesario solicitar una suscripción de red para cada línea (enlace) necesaria. Es posible que el suministro de una línea tarde algún tiempo, compruébelo bien previamente con el proveedor de la red X.25.
- Las funciones que están disponibles en la red X.25 y las funciones que son necesarias. Normalmente el proveedor de la red suministra una guía técnica de la red, que debe obtener y consultar.
- Reúna la información sobre los canales lógicos que necesite para PVC y SVC.
  - Pueden definirse un máximo de 16 grupos de 256 canales lógicos.
  - El número de grupos va de 0 a 15.
  - El número de canal lógico dentro del grupo va de 0 a 255.

    Multiplicando el número de grupos por 256 y sumándole el número de canales lógicos da como resultado un número dentro del rango de 0 a 4095, que identifica de manera exclusiva un canal lógico. A veces se hace referencia a esta combinación como el número de canal lógico.

    Notas:

    1. Si especifica el CCITT como 1984 ó 1988, el número máximo de canales lógicos es 4095.
    2. Si especifica el CCITT como 1980, el número máximo de canales lógicos es 1024.
  - Los grupos de canales lógicos pueden ser de sólo entrada (reservados a las llamadas de otros DTE), de sólo salida (reservados para las llamadas a otros DTE) o de dos direcciones.
- El número de circuitos virtuales que SNA necesita
- Los PVC que necesita
- La combinación de canales lógicos de sólo entrada, de sólo salida y de dos direcciones
- El tamaño máximo de paquete que necesita y lo que la red X.25 da soporte.
- Los detalles de los recursos X.25 opcionales que utilizarán los programas de aplicación X.25.

  Las recomendaciones CCITT X.25 definen la cantidad de recursos opcionales que la red puede soportar.

  Algunos recursos tienen parámetros que un programa de aplicación puede especificar o negociar durante la configuración y borrado de la llamada utilizando los campos de recursos de los paquetes petición de llamada, llamada aceptada y borrar petición.

  La conexión X.25 puede configurarse para dar soporte a los siguientes recursos durante la configuración de la llamada:

  - Grupo cerrado de usuarios

© Copyright IBM Corp. 1989, 1996

- Identificación de usuario de red
- Negociación de tamaño de paquete y ventana
- Cobro revertido

Defina los recursos durante la configuración del DLC X.25.

- Los detalles de cualquier requisito especial de los parámetros de trama y paquete. Los valores por omisión para estos parámetros de configuración se han elegido cuidadosamente para ajustarse a la mayoría de las situaciones. Sin embargo, el proveedor de la red puede requerir o recomendar algunos valores.

  Para evitar problemas, los parámetros de configuración deben coincidir con los detalles de la suscripción de la red. Por ejemplo, si ha configurado 20 canales lógicos SVC pero sólo se ha suscrito a 10, el DCE debería detectar una condición de error al intentar utilizar el undécimo canal lógico.

Posibles conexiones X.25

La Figura 40 muestra cómo una red X.25 puede proporcionar una conexión desde una pasarela SNA con un sistema principal.

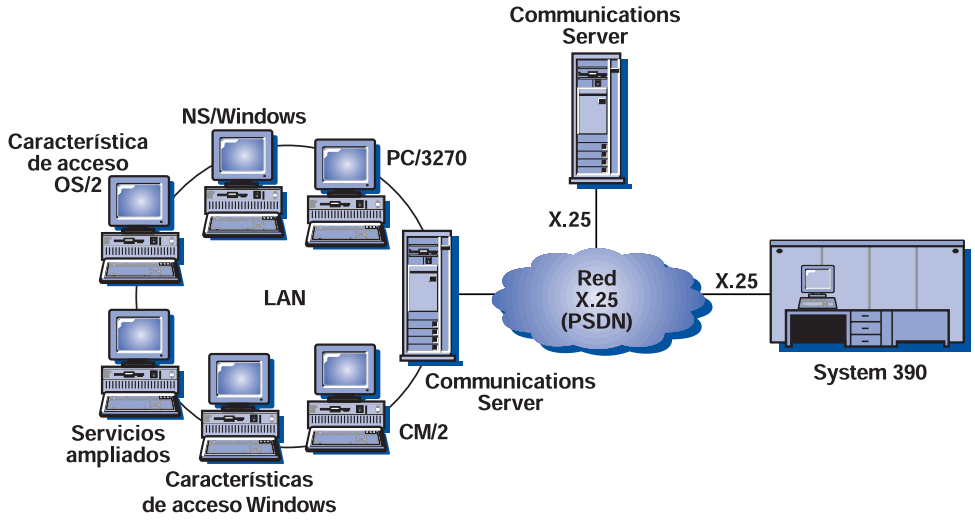


Figura 40. Conectividad de pasarela X.25 y SNA

Cargos de red X.25

Los cargos reales dependen de las prácticas de facturación del proveedor de red X.25, pero normalmente los cargos consisten en algunos o todos los elementos siguientes:

- Cargo de instalación

  Un solo cargo de instalación cuando se suscribe la primera vez a la red X.25.

- Cargo de alquiler periódico

  Este cargo depende de los recursos facilitados por el proveedor de red. Por ejemplo, puede tener que pagar un cargo por cada recurso de red opcional al que se suscriba. También puede tener que pagar un cargo por cada canal

lógico disponible. Generalmente, los PVC cuestan más que los SVC porque necesitan recursos de red dedicados.

- Cargo por uso

  Este cargo depende del período de tiempo para el cual está conectado lógicamente a la red, posiblemente esté sujeto a un cargo mínimo.

- Cargo por volumen

  Este cargo está relacionado con la cantidad de datos transmitidos en la red durante el período de facturación.

Configuración de la conectividad del sistema principal

Puede conectar estaciones de trabajo que ejecutan Communications Server con los sistemas principales System/390 (incluso el System/370) o AS/400. Muchos de los valores que se especifican para la configuración de Communications Server también se utilizan cuando se configura el sistema principal. Este capítulo describe la correlación entre los parámetros de configuración que especifica durante la configuración de Communications Server y los parámetros que especifica en los sistemas principales. Este capítulo contiene también tablas que listan los parámetros que pueden utilizarse para eliminar los parámetros comunes en cada macro que se ha de emitir entre Communications Server y el sistema principal.

Nota: Muchos de los parámetros NCP emitidos desde las macro LINE, PU y LU pueden especificarse en la macro GROUP para legibilidad y facilidad de codificación. Esta coincidencia de parámetros elimina la necesidad de incluir los parámetros comunes en cada macro subsiguiente y sigue permitiendo la posibilidad de alterarlos temporalmente cuando proceda.

Red en anillo NCP (NTRI) con VTAM y Communications Server

La Tabla 7 compara los parámetros del sistema principal con los parámetros de Communications Server para las conexiones de red en anillo IBM.

Tabla 7. Referencia cruzada de los parámetros del sistema principal/PC: Definición de NTRI de red en anillo IBM

NTRI/NCP	Perfil/Parámetros de Communications Server	Observaciones
GROUP ECLTYPE = PHY	Tipo de DLC: LAN	
LINE LOCADDR	Configurar conexiones LAN **Dirección de destino**	El valor establecido para este parámetro bajo Communications Server debe ser la dirección del adaptador de red en anillo IBM en el controlador del sistema principal.

Red en anillo con red conmutada VTAM y Communications Server

La Tabla 8 compara los parámetros del sistema principal con los parámetros de Communications Server para la conexión de Red en anillo IBM que utilizan una red conmutada VTAM.

Tabla 8 (Página 1 de 2). Referencia cruzada de los parámetros del sistema principal/PC: Red conmutada VTAM de Red en anillo IBM

VTAM	Perfil/Parámetros de Communications Server	Observaciones
IDBLK=	Configurar nodo ID de nodo local **ID de bloque**	El IDBLK de bloque debe coincidir con los 3 primeros caracteres hexadecimales del **ID de nodo local**, que toma por omisión X'05D' para Communications Server. Especifique este parámetro cuando utilice líneas conmutadas u omita este parámetro si utiliza CPNAME=.

© Copyright IBM Corp. 1989, 1996

Tabla 8 (Página 2 de 2). Referencia cruzada de los parámetros del sistema principal/PC: Red conmutada VTAM de Red en anillo IBM

VTAM	Perfil/Parámetros de Communications Server	Observaciones
IDNUM=	Configurar nodo ID de nodo local **ID de unidad física**	El IDNUM del sistema principal debe coincidir con los 5 últimos caracteres hexadecimales del **ID de nodo local**. Especifique este parámetro cuando utilice líneas conmutadas u omita este parámetro si utiliza CPNAME=.
CPNAME=	Definición de nodo Configurar nodo **Nombre CP completamente calificado** (segundo campo)	Especifique este parámetro cuando utilice las líneas conmutadas u omítalo cuando utilice IDBLK= e IDNUM=.
LOCADDR	Configurar LU de sistema principal **Dirección de NAU**	Estos parámetros deben tener el mismo valor. Para las LU independientes, VTAM recomienda la creación de una definición CDRSC o la utilización del operando DYNLU en lugar de codificar LOCADDR=0. Para obtener más información sobre la codificación de definiciones CDRSC para LU independientes, consulte el manual *VTAM Network Implementation Guide* No es necesaria ninguna definición del sistema principal para las LU dependientes si se utiliza la definición SDDLU o dinámica para las LU independientes en VTAM 3.4 o posterior.
MAXDATA	Configurar dispositivo de la LAN **Tamaño máximo de PIU** (265–65535)	No es necesario que estos valores coincidan.
MAXOUT	Configurar dispositivo de la LAN **Cuenta de almacenamiento intermedio de recepción** (2–64)	La **Cuenta de almacenamiento intermedio de recepción** de Communications Server debe ser igual al parámetro MAXOUT del sistema principal.

Adaptador y Communications Server de Red en anillo IBM 9370

La Tabla 9 compara los parámetros del sistema principal 9370 con los parámetros de Communications Server para las conexiones de Red en anillo IBM.

Tabla 9 (Página 1 de 2). Referencia cruzada de los parámetros del sistema principal/PC: LAN VTAM 9370 de Red en anillo IBM

VTAM	Perfil/Parámetros de Communications Server	Observaciones
VBUILD TYPE = LAN	Tipo de DLC: LAN	
PORT MACADDR=	Configurar conexión LAN **Dirección de destino**	La dirección de destino especificada en la personalización de Communications Server debe ser la dirección del adaptador de red en anillo IBM 9370.
PORT SAPADDR=04	Configurar conexión LAN **SAP remoto**	Estos valores deben coincidir.

Tabla 9 (Página 2 de 2). Referencia cruzada de los parámetros del sistema principal/PC: LAN VTAM 9370 de Red en anillo IBM

VTAM	Perfil/Parámetros de Communications Server	Observaciones
ADDR=04 (sólo de salida)	Configurar conexión LAN **SAP local**	Estos valores deben coincidir.

Controlador 3174 y Communications Server

La Tabla 10 compara los parámetros del controlador 3174 con Communications Server para las conexiones de red en anillo IBM.

Tabla 10. Coincidencias de parámetros entre una red en anillo 3174 y Communications Server

3174	Perfil/Parámetros de Communications Server	Observaciones
Dirección de límite superior mayor que 104: CUA	Tipo de DLC: LAN	
Dirección de red en anillo para pasarela	Configurar conexiones LAN **Dirección de destino**	Estos valores deben coincidir.
Definición de transmisión en anillo. W= máx. ventana salida, F=0, W = 1-7, F=1, W = 1-7, F=2, W = 1-4, F=3, W = 1-2	Configurar dispositivos LAN **Cuenta de almacenamiento intermedio de recepción** (1–8)	La **cuenta de almacenamiento intermedio de recepción** de Communications Server debe ser igual a 3174 W.

PU VTAM de Controlador 3174 y Communications Server

La Tabla 11 compara los parámetros de PU VTAM del controlador 3174 con Communications Server para las conexiones de red en anillo IBM.

Tabla 11 (Página 1 de 2). Referencia cruzada de los parámetros del sistema principal/PC: PU VTAM de controlador 3174 de Red en anillo IBM y Communications Server

VTAM	Perfil/Parámetros de Communications Server	Observaciones
CUADDR (local) o ADDR (remota)	(ninguna)	Correlacionado por el controlador 3174 con la dirección de red en anillo IBM
MAXDATA (remoto sólo)	Configurar dispositivos LAN **Tamaño máximo de PIU** (99–65535)	El valor de Tamaño máximo de PIU establecido en la estación de trabajo Communications Server debe coincidir con el valor establecido en el sistema principal.
MAXOUT (remoto sólo)	Configurar dispositivos LAN **Cuenta de almacenamiento intermedio de recepción** (2–64)	La **Cuenta de almacenamiento intermedio de recepción** de Communications Server debe ser igual a MAXOUT.

Tabla 11 (Página 2 de 2). Referencia cruzada de los parámetros del sistema principal/PC: PU VTAM de controlador 3174 de Red en anillo IBM y Communications Server

VTAM	Perfil/Parámetros de Communications Server	Observaciones
LOCADDR	Configurar LU de sistema principal **Dirección de NAU**	Estos parámetros deben tener el mismo valor. Para las LU independientes, VTAM recomienda la creación de una definición CDRSC o la utilización del operando DYNLU en lugar de codificar LOCADDR=0. Para obtener más información sobre la codificación de definiciones CDRSC para LU independientes, consulte el manual *VTAM Network Implementation Guide* No es necesaria ninguna definición del sistema principal para las LU dependientes si se utiliza la definición SDDLU o dinámica para las LU independientes en VTAM 3.4 o posterior.

Ethernet con red conmutada VTAM y Communications Server

La Tabla 12 compara los parámetros del sistema principal con los parámetros de Communications Server para las conexiones de red Ethernet que utilizan una red conmutada VTAM.

Tabla 12 (Página 1 de 2). Referencia cruzada de los parámetros del sistema principal/PC: Red conmutada VTAM de red Ethernet

VTAM	Perfil/Parámetros de Communications Server	Observaciones
IDBLK=	Configurar nodo ID de nodo local **ID de bloque**	El IDBLK de bloque debe coincidir con los 3 primeros caracteres hexadecimales del **ID de nodo local**, que toma por omisión X'05D' para Communications Server. Especifique este parámetro cuando utilice líneas conmutadas u omita este parámetro si utiliza CPNAME=.
IDNUM=	Configurar nodo ID de nodo local **ID de unidad física**	El IDNUM del sistema principal debe coincidir con los 5 últimos caracteres hexadecimales del **ID de nodo local**. Especifique este parámetro cuando utilice líneas conmutadas u omita este parámetro si utiliza CPNAME=.
CPNAME=	Definición de nodo Configurar nodo **Nombre CP completamente calificado** (segundo campo)	Especifique este parámetro cuando utilice las líneas conmutadas u omítalo cuando utilice IDBLK= e IDNUM=.

Tabla 12 (Página 2 de 2). Referencia cruzada de los parámetros del sistema principal/PC: Red conmutada VTAM de red Ethernet

VTAM	Perfil/Parámetros de Communications Server	Observaciones
LOCADDR	Configurar LU de sistema principal **Dirección de NAU**	Estos parámetros deben tener el mismo valor. Para las LU independientes, VTAM recomienda la creación de una definición CDRSC o la utilización del operando DYNLU en lugar de codificar LOCADDR=0. Para obtener más información sobre la codificación de definiciones CDRSC para LU independientes, consulte el manual *VTAM Network Implementation Guide* No es necesaria ninguna definición del sistema principal para las LU dependientes si se utiliza la definición SDDLU o dinámica para las LU independientes en VTAM 3.4 o posterior.
MAXDATA	Configurar dispositivo de la LAN **Tamaño máximo de PIU** (265–65535)	No es necesario que estos valores coincidan.
MAXOUT	Configurar dispositivo de la LAN **Cuenta de almacenamiento intermedio de recepción** (2–64)	La **Cuenta de almacenamiento intermedio de recepción** de Communications Server debe ser igual al parámetro MAXOUT del sistema principal.

VTAM/NCP y Communications Server (SDLC)

La Tabla 13 compara los parámetros del sistema principal VTAM/NCP con los parámetros de Communications Server para las conexiones SDLC.

Tabla 13 (Página 1 de 3). Referencia cruzada de los parámetros del sistema principal/PC: SDLC

VTAM/NCP	Perfil/Parámetros de Communications Server	Observaciones
NETID=	Configurar nodo **Nombre de CP completamente calificado** (primer campo)	Este parámetro se puede utilizar tanto para líneas alquiladas como para líneas conmutadas. Este parámetro identifica la red SNA con la que se conecta utilizando Communications Server.
NAME PU		Utilice siempre un NAME PU. Este nombre de PU debe ser un nombre que no sea igual al nombre de CP local para que pueda definir una LU para el punto de control.
IDBLK=	Configurar nodo ID de nodo local **ID de bloque**	El IDBLK de bloque debe coincidir con los 3 primeros caracteres hexadecimales del **ID de nodo local**, que toma por omisión X'05D' para Communications Server. Especifique este parámetro cuando utilice líneas conmutadas u omita este parámetro si utiliza CPNAME=.

Tabla 13 (Página 2 de 3). Referencia cruzada de los parámetros del sistema principal/PC: SDLC

VTAM/NCP	Perfil/Parámetros de Communications Server	Observaciones
IDNUM=	Configurar nodo ID de nodo local **ID de unidad física**	El IDNUM del sistema principal debe coincidir con los 5 últimos caracteres hexadecimales del **ID de nodo local**. Especifique este parámetro cuando utilice líneas conmutadas u omita este parámetro si utiliza CPNAME=.
CPNAME=	Definición de nodo Configurar nodo **Nombre CP completamente calificado** (segundo campo)	Especifique este parámetro cuando utilice las líneas conmutadas u omítalo cuando utilice IDBLK= e IDNUM=.
LNCTL=SDLC	Tipo de DLC: SDLC-WAC, SDLC-MPA, Puerta COM (depende del hardware utilizado)	SDLC debe seleccionarse aquí. Este parámetro se utiliza para líneas alquiladas y conmutadas.
LOCADDR	Configurar LU de sistema principal **Dirección de NAU**	Estos parámetros deben tener el mismo valor. Para las LU independientes, VTAM recomienda la creación de una definición CDRSC o la utilización del operando DYNLU en lugar de codificar LOCADDR=0. Para obtener más información sobre la codificación de definiciones CDRSC para LU independientes, consulte el manual *VTAM Network Implementation Guide* No es necesaria ninguna definición del sistema principal para las LU dependientes si se utiliza la definición SDDLU o dinámica para las LU independientes en VTAM 3.4 o posterior.
NRZI=YES/NO	Configurar conexiones SDLC-WAC, SDLC-MPA, Puerta COM **Codificación NRZI**	Communications Server utiliza USE_NRZI_ENCODING=0 y USE_NRZI_ENCODING=1. Este parámetro sólo se encuentra en PCM para el tipo de módem: Conmutado síncrono, No conmutado síncrono y AutoSync. El esquema de codificación, NRZI o NRZ, debe configurarse de la misma manera en ambos extremos de una conexión. Si los esquemas de codificación no coinciden, los módems se conectarán pero la transferencia de datos no será satisfactoria y Communications Server desconectará la conexión después de un tipo de espera de nivel de enlace (normalmente 40 segundos). Se recomienda el esquema de codificación NRZ cuando se conecte a una red X.25 utilizando un Conector de área amplia IBM.
DUPLEX= FULL/HALF	Configurar conexiones SDLC-WAC y Sólo puerta COM **Dúplex comunicación**	Los valores establecidos en cada lado deben se coherentes con el tipo de módem y la configuración. Este parámetro se utiliza para líneas alquiladas y conmutadas.

Tabla 13 (Página 3 de 3). Referencia cruzada de los parámetros del sistema principal/PC: SDLC

VTAM/NCP	Perfil/Parámetros de Communications Server	Observaciones
(TRANSFR * BFRS) –47	Configurar dispositivos SDLC-WAC, SDLC-MPA, Puerta COM **Tamaño máximo de PIU** (265–4105)	El valor de Tamaño máximo de campo I debe ser inferior o igual a (TRANSFR * BFRS) - 47 indicado en el sistema principal. Este parámetro se utiliza para líneas alquiladas y conmutadas.
MAXDATA=	Configurar dispositivos SDLC-WAC, SDLC-MPA, Puerta COM **Tamaño máximo de PIU** (265–4105)	No es necesario que estos valores coincidan. Este parámetro se utiliza para líneas alquiladas y conmutadas. Se utilizará el valor inferior.
MAXOUT=	Configurar dispositivos SDLC-WAC, SDLC-MPA, Puerta COM **Cuenta de ventana de recepción** (1–30)	La **Cuenta de ventana de recepción** de Communications Server debe ser igual al parámetro MAXOUT del sistema principal. Este parámetro se utiliza para líneas alquiladas y conmutadas.
ADDR=	Configurar dispositivos SDLC-WAC, SDLC-MPA, Puerta COM **Dirección de estación de enlace** (01–FE)	Estos parámetros deben tener el mismo valor. Se codifica en hexadecimal para Communications Server y VTAM/NCP. Este parámetro se utiliza para líneas alquiladas y conmutadas.

VTAM y Communications Server (APPC)

La Tabla 14 compara los parámetros del sistema principal VTAM con los parámetros de Communications Server para las conexiones APPC.

Tabla 14 (Página 1 de 2). Referencia cruzada de los parámetros del sistema principal/PC: APPC

VTAM	Perfil/Parámetros de Communications Server	Observaciones
LU NAME	Configurar LU de sistema principal **Nombre de LU local** o: Configurar nodo **Nombre de CP completamente calificado** (segundo campo)	
LOCADDR	Configurar LU de sistema principal **Dirección de NAU**	Estos parámetros deben tener el mismo valor. Para las LU independientes, VTAM recomienda la creación de una definición CDRSC o la utilización del operando DYNLU en lugar de codificar LOCADDR=0. Para obtener más información sobre la codificación de definiciones CDRSC para LU independientes, consulte el manual *VTAM Network Implementation Guide* No es necesaria ninguna definición del sistema principal para las LU dependientes si se utiliza la definición SDDLU o dinámica para las LU independientes en VTAM 3.4 o posterior.
NETID APPL	Configurar LU 6.2 asociada **Nombre de LU asociada**	

Tabla 14 (Página 2 de 2). Referencia cruzada de los parámetros del sistema principal/PC: APPC

VTAM	Perfil/Parámetros de Communications Server	Observaciones
Tabla de interpretación VTAM	Configurar LU 6.2 asociada **Nombre de LU asociada**	Esto sólo es para LU dependientes.
Tabla LOGMODE LOGMODE=	Configurar modalidad **Nombre de modalidad**	Estos parámetros deben coincidir.
Tabla LOGMODE RUSIZES=	Configurar modalidad **Tamaño máximo de RU** (256–32767)	Los valores finales se negocian.

VTAM y Communications Server (MPC)

La Tabla 15 y la Tabla 16 comparan los parámetros de IOCP/HCD y VTAM con los parámetros de Communications Server para las conexiones de Canal de múltiples vías (MPC).

Tabla 15. Referencia cruzada de los parámetros IOCP/HCD: MPC

IOCP/HCD	Perfil/Parámetros de Communications Server	Observaciones
IOCP IODEVICE UNIT=SCTC	Tipo de DLC: IBM-MPC	
HCD Tipo de dispositivo SCTC	Tipo de DLC: IBM-MPC	

Tabla 16 (Página 1 de 2). Referencia cruzada de los parámetros VTAM: MPC

Sentencia de definición VTAM	Operando	Perfil/Parámetros de Communications Server	Observaciones
VBUILD,TYPE=TRL	LNCTL=MPC	Tipo de DLC: IBM-MPC	
	MPCLEVEL=HPDT		Las conexiones IBM-MPC de Communications Server IBM-MPC necesitan HPR/HPDT
	MAXBFRU	Configurar DLC MPC **Tamaño máximo de PIU**	Puede afectar al rendimiento y/o utilización del almacenamiento VTAM
	MAXREADS	Configurar DLC MPC **Recuento de almacenamiento intermedio de recepción**	Puede afectar al rendimiento y/o utilización del almacenamiento VTAM
	READ	Configurar DLC MPC	La lista de direcciones VTAM READ IODEVICE debe corresponder a la lista de DLC MPC de Communications Server de subcanales READ
	WRITE	Configurar DLC MPC	La lista de direcciones VTAM WRITE IODEVICE debe corresponder a la lista de DLC MPC de Communications Server de subcanales WRITE

Tabla 16 (Página 2 de 2). Referencia cruzada de los parámetros VTAM: MPC

Sentencia de definición VTAM	Operando	Perfil/Parámetros de Communications Server	Observaciones
VBUILD,TYPE=LOCAL	CONNTYPE=APPN	Configurar conexiones IBM-MPC **Soporte APPN**	La conexión IBM-MPC de Communications Server IBM-MPC necesita APPN.
	XID=YES	Configurar conexiones IBM-MPC **Soporte APPN**	La conexión IBM-MPC de Communications Server IBM-MPC necesita PU2.1.
	CPCP=YES	Configurar conexiones IBM-MPC **Soporte APPN**	La conexión IBM-MPC de Communications Server IBM-MPC necesita APPN.
	HPR=YES	Configurar conexiones IBM-MPC **Soporte de HPR**	La conexión IBM-MPC de Communications Server IBM-MPC necesita HPR.
	NN	Configurar nodo **Tipo de nodo**	El tipo de nodo de PU VTAM debe coincidir con la definición de Communications Server.
	DELAY		Puede afectar al rendimiento y/o a la utilización de CPU VTAM

ES/9000 y Communications Server (SDLC)

La Tabla 17 compara los parámetros del Sistema de información 9370 con los parámetros de Communications Server para las conexiones SDLC.

Tabla 17 (Página 1 de 2). Referencia cruzada de los parámetros del sistema principal/PC: Sistema de información 9370 vía SDLC

9370/VTAM	Perfil/Parámetros de Communications Server	Observaciones
QFI: Sin retorno a cero invertido (configuración de microcódigo)	Configurar conexiones SDLC-WAC, SDLC-MPA, Puerta COM **Codificación NRZI**	Estos parámetros deben coincidir. Este parámetro se utiliza para líneas alquiladas y conmutadas. Communications Server utiliza USE_NRZI_ENCODING=0 y USE_NRZI_ENCODING=1. Esta es la corriente síncrona de datos.
QFI: Protocolo (configuración de microcódigo) VTAM: GROUP LNCTL = SDLC	Tipo DLC SDLC-WAC, SDLC-MPA Puerta COM	Los parámetros del microcódigo y VTAM deben coincidir. Este parámetro se utiliza para líneas alquiladas y conmutadas.
MAXDATA	Configurar dispositivos SDLC-WAC, SDLC-MPA, Puerta COM **Tamaño máximo de PIU** (265–4105)	No es necesario que estos valores coincidan. Este parámetro se utiliza para líneas alquiladas y conmutadas.
Tamaño de MAXBFRU * IOBUF	Configurar dispositivos SDLC-WAC, SDLC-MPA, Puerta COM **Tamaño máximo de PIU** (265–4105)	El valor de Tamaño máximo de campo I debe ser igual o inferior a MAXBFRU multiplicado por el tamaño de IOBUF indicado en el sistema principal. Este parámetro se utiliza para líneas alquiladas y conmutadas.

Tabla 17 (Página 2 de 2). Referencia cruzada de los parámetros del sistema principal/PC: Sistema de información 9370 vía SDLC

9370/VTAM	Perfil/Parámetros de Communications Server	Observaciones
MAXOUT=	Configurar dispositivos **Cuenta de ventana de recepción** (1–30)	La **Cuenta de ventana de recepción** de Communications Server debe ser igual al parámetro MAXOUT del sistema principal. Este parámetro se utiliza para líneas alquiladas y conmutadas.
ADDR=	Configurar dispositivos **Dirección de estación de enlace** (01–FE)	Los valores establecidos para estos parámetros deben coincidir. Este parámetro se utiliza para líneas alquiladas y conmutadas.
IDBLK=	Configurar nodo ID de nodo local **ID de bloque**	El IDBLK de bloque debe coincidir con los 3 primeros caracteres hexadecimales del **ID de nodo local**, que toma por omisión X'05D' para Communications Server. Especifique este parámetro cuando utilice líneas conmutadas u omita este parámetro si utiliza CPNAME=.
IDNUM=	Configurar nodo ID de nodo local **ID de unidad física**	El IDNUM del sistema principal debe coincidir con los 5 últimos caracteres hexadecimales del **ID de nodo local**. Especifique este parámetro cuando utilice líneas conmutadas u omita este parámetro si utiliza CPNAME=.
CPNAME=	Configurar nodo **Nombre de CP completamente calificado** (segundo campo)	Especifique este parámetro cuando utilice líneas conmutadas u omita la utilización de IDBLK= o IDNUM=.
LOCADDR	Configurar LU de sistema principal **Dirección de NAU**	Los parámetros LOCADDR y NAU deben tener el mismo valor. Para las LU independientes, VTAM recomienda la creación de una definición CDRSC o la utilización del operando DYNLU en lugar de codificar LOCADDR=0. Para obtener más información sobre la codificación de definiciones CDRSC para LU independientes, consulte el manual *VTAM Network Implementation Guide*. Este parámetro se utiliza para líneas alquiladas y conmutadas.

Sistema principal y Communications Server (DLUR)

La Tabla 18 compara los parámetros del sistema principal con los de Communications Server para las conexiones VTAM sobre DLUR.

Tabla 18 (Página 1 de 2). Referencia cruzada de los parámetros de Communications Server VTAM: Utilización de DLUR

VTAM	Communications Server	Observaciones
IDBLK=	Configurar PU DLUR **ID de bloque**	El IDBLK debe coincidir con los 3 primeros caracteres hexadecimales del ID de nodo que toma por omisión X'05D' para Communications Server Especifique este parámetro cuando NO utilice CPNAME=.

Tabla 18 (Página 2 de 2). Referencia cruzada de los parámetros de Communications Server VTAM: Utilización de DLUR

VTAM	Communications Server	Observaciones
IDNUM=	Configurar PU DLUR **ID de unidad física**	El IDBLK debe coincidir con los 5 últimos caracteres hexadecimales del ID de nodo. Especifique este parámetro cuando NO utilice PNAME=.
CPNAME=	Configurar PU DLUR **Nombre de PU**	El CPNAME debe coincidir con el nombre de PU local. Especifique este parámetro cuando NO utilice IDNUM= ni IDBLK=.

La Tabla 19 lista los siguientes parámetros de la sentencia PATH que se utilizan al establecer una conexión desde el sistema principal con la estación de trabajo.

Tabla 19. Coincidencia de parámetros DLUR de Communications Server VTAM en conexión de sistema principal a estación de trabajo

VTAM	Communications Server	Observaciones
DLURNAME=	Configurar nodo **Nombre de CP completamente calificado** (segundo campo)	El DLURNAME proporciona el nombre del nodo DLUR que es propietario de la PU DLUR. Para Communications Server, es el nombre de CP completamente calificado.
DLCADDR= (1,C,INTPU)		Necesario. Este parámetro indica al DLUR que la conexión es para una PU interna.
DLCADDR= (2,X,zzzzzzzz)	Configurar PU DLUR **ID de bloque y ID de unidad física**	zzzzzzzz de DLCADDR=(2,X,zzzzzzzzz) debe coincidir con el ID de nodo. Especifique este parámetro cuando NO utilice DLCADDR=(3,C,nombrepu).
DLCADDR= (3,C,nombrepu)	Configurar PU DLUR **Nombre de PU**	El nombre de PU de DLCADDR=(3,C,nombrepu) debe coincidir con el nombre de PU local. Especifique este parámetro cuando NO utilice DLCADDR=(2,X,zzzzzzzz).

NPSI y Communications Server (X.25)

El soporte de Communications Server X.25 permite la transmisión de tramas SNA a través de una red X.25. X.25 trata las tramas SNA como datos sin formato y las transmite como paquetes de datos dentro de datos. Los dos nodos de red no se conectan directamente, sino que se conectan a un intermediario denominado red de datos de conmutación de paquetes (PSDN). La red X.25 puede componerse de cualquiera de las conectividades de X.25.

El software que interactúa con PSDN y empaqueta los datos SNA en paquetes y los extrae intactos es una parte íntegra de Communications Server. En la parte correspondiente al sistema principal S/370, las funciones de X.25 se manejan por un producto de software separado denominado Interfaz de conmutación del programa de control de red X.25 (NPSI). Las definiciones de NPSI se generan junto con el NCP y el software NPSI se ejecuta en armonía con el NCP en el mismo controlador 3705, 3725, 3720 ó 3745.

La mayor parte de los parámetros de X.25 especificados en Communications Server y en NPSI toman los valores que se acuerdan entre el usuario y el pro-

veedor de la red X.25 en lugar de entre los dos nodos. Por ejemplo, con una conexión SDLC de una línea no conmutada, el controlador del sistema principal (NCP) se configura para sondear una dirección secundaria en particular. Communications Server se configura para responder a esta dirección en un enlace físico entre la estación de trabajo Communications Server y el sistema principal.

Conexiones NPSI sobre X.25

La Tabla 20 compara los parámetros del sistema principal y de Communications Server para las conexiones NPSI sobre X.25.

Tabla 20. Referencia cruzada de los parámetros de sistema principal/PC: Conexiones NPSI sobre X.25

NPSI	Perfil/Parámetros de Communications Server	Observaciones
X25.LINE TYPE=	Tipo DLC Puerta COM X.25, X.25-WAC	Especifique **TYPE=P** para los PVC y **TYPE=S** para los SVC para la definición de línea X.25 NPSI.
CALL= (sólo para tipo = S)	Configurar dispositivos Puerta COM X.25, X.25-WAC **Rangos de circuito virtual**	Los rangos de circuito virtual deben coincidir con la suscripción de red X.25.
MAXDATA=	Configurar dispositivos Puerta COM X.25, X.25-WAC **Tamaño máximo de PIU** (256–4105)	No es necesario que estos valores coincidan.
VWINDOW	Configurar dispositivos Puerta COM X.25, X.25-WAC **Tamaño de ventana** (1–7)	El **Tamaño de ventana SVC/PVC** debe coincidir con las suscripciones de X.25.
MWINDOW	Configurar dispositivos Puerta COM X.25, X.25-WAC Valores de trama **Tamaño de ventana** (1–7)	
FRMLGTH	Configurar dispositivos Puerta COM X.25, X.25-WAC Secuencia de trama **Módulo**	El valor **FRMLGTH** del sistema debe ser como mínimo MAXPKT +3 cuando se ejecute el Módulo 8 o MAXPKT +4 cuando se ejecute el Módulo 128. El tamaño de Módulo y los tamaños de paquetes del sistema principal y de Communications Server deben coincidir con la suscripción de X.25.
MAXPKTL	Configurar dispositivos Puerta COM X.25, X.25-WAC **Tamaño de paquete**	Los **tamaños de paquete SVC/PVC** debe coincidir con el valor de suscripción de X.25.

VTAM/NCP y Communications Server (X.25)

La Tabla 21 compara los parámetros del sistema principal y Communications Server para X.25 (VTAM/NCP).

Tabla 21. Referencia cruzada de los parámetros de sistema principal/PC: X.25 (VTAM/NCP)

VTAM/NCP	Perfil/Parámetros de Communications Server	Observaciones
NETID=	Configurar nodo **Nombre de CP completamente calificado** (primer campo)	Esto identifica la red SNA a la que se conecta utilizando Communications Server.
PU NAME		Utilice siempre un nombre de PU. Este nombre de PU no debe ser igual al nombre de CP local para que pueda definir una LU para el punto de control.
IDBLK=	Configurar nodo ID de nodo local **ID de bloque**	Los 3 primeros dígitos hexadecimales del **ID de nodo local**, que toman por omisión X'05D' para Communications Server. Especifique este parámetro cuando utilice líneas conmutadas u omita este parámetro si utiliza CPNAME=.
IDNUM=	Configurar nodo ID de nodo local **ID de unidad física**	El IDNUM del sistema principal debe coincidir con los 5 últimos caracteres hexadecimales del **ID de nodo local**. Especifique este parámetro cuando utilice líneas conmutadas u omita este parámetro si utiliza CPNAME=.
CPNAME=	Configurar nodo **Nombre de CP completamente calificado** (segundo campo)	Especifique este parámetro cuando utilice las líneas conmutadas u omítalo cuando utilice IDBLK= e IDNUM=.
(TRANSFR * BFRS) - 47	Configurar dispositivos Puerta COM X.25, X.25-WAC **Tamaño máximo de PIU** (265–4105)	El **Tamaño máximo de PIU** debe ser igual al valor establecido en el sistema principal.
MAXDATA=	Configurar dispositivos Puerta COM X.25, X.25-WAC **Tamaño máximo de PIU** (265–4105)	No es necesario que estos valores coincidan.
LOCADDR	Configurar LU de sistema principal **Dirección de NAU**	Estos parámetros deben tener el mismo valor. Para las LU independientes, VTAM recomienda la creación de una definición CDRSC o la utilización del operando DYNLU en lugar de codificar LOCADDR=0. Para obtener más información sobre la codificación de definiciones CDRSC para LU independientes, consulte el manual *VTAM Network Implementation Guide* No es necesaria ninguna definición del sistema principal para las LU dependientes si se utiliza la definición SDDLU o dinámica para las LU independientes en VTAM 3.4 o posterior.

APPC sobre X.25

La Tabla 22 correlaciona los parámetros para una estación de trabajo de Communications Server que ejecuta las comunicaciones avanzadas programa a programa (APPC) conectando con un sistema principal mediante X.25.

Tabla 22. Referencia cruzada de parámetros del sistema principal/PC: APPC en una red en anillo IBM que utiliza X.25 para un sistema principal

NCP	Perfil/Parámetros de Communications Server	Observaciones
LU NAME	Configurar LU 6.2 local **Nombre de LU local** o: Configurar nodo **Nombre de CP completamente calificado** (segundo campo)	
LOCADDR	Configurar LU de sistema principal **Dirección de NAU**	Estos parámetros ***deben*** tener el mismo valor. Para las LU independientes, VTAM recomienda la creación de una definición CDRSC o la utilización del operando DYNLU en lugar de codificar LOCADDR=0. Para obtener más información sobre la codificación de definiciones CDRSC para LU independientes, consulte el manual *VTAM Network Implementation Guide* No es necesaria ninguna definición del sistema principal para las LU dependientes si se utiliza la definición SDDLU o dinámica para las LU independientes en VTAM 3.4 o posterior.
NETID APPL	Configurar LU 6.2 asociada **Nombre de LU asociada**	
Tabla de interpretación VTAM	Configurar LU 6.2 asociada **Nombre de LU asociada**	Esto sólo es para LU dependientes.
Tabla LOGMODE LOGMODE=	Configurar modalidad **Nombre de modalidad**	Estos parámetros ***deben*** coincidir.
Tabla LOGMODE RUSIZES=	Configurar modalidad **Tamaño máximo de RU** (256–32767)	Estos valores deben coincidir.

Definiciones de línea de sistema principal AS/400

Las definiciones de línea de sistema principal AS/400 incluyen la correlación de los parámetros de programa de sistema principal OS/400 con los parámetros Communications Server. La Tabla 23 en la página 175 contiene los parámetros de línea SDLC.

Tabla 23. Referencia cruzada de los parámetros de Communications Server AS/400: Definición de línea de programa del sistema principal OS/400

OS/400	Perfil/Parámetros de Communications Server	Observaciones
Codificación de datos NRZI=	Configurar conexiones SDLC-WAC, SDLC-MPA, Puerta COM **Codificación NRZI**	Communications Server utiliza USE_NRZI_ENCODING=0 y USE_NRZI_ENCODING=1. Este parámetro sólo se encuentra en PCM para el tipo de módem: Conmutado síncrono, No conmutado síncrono y AutoSync.
Selección de velocidad de datos de módem	Configurar dispositivos Sólo puerta COM **Configurar módem**	Los parámetros deben coincidir en ambos sistemas para los tipos de conexión de módem, conmutado asíncrono.
Tamaño máximo de trama (MAXFRAME)	Configurar dispositivos SDLC-WAC, SDLC-MPA, Puerta COM **Cuenta de ventana de recepción** (1–30)	Los valores no conmutados asíncronos no es necesario que coincidan.
Número máximo de tramas pendientes (MAXOUT)	Configurar dispositivos SDLC-WAC, SDLC-MPA, Puerta COM **Cuenta de ventana de recepción** (1–30)	La **Cuenta de ventana de recepción** de Communications Server debe ser igual al parámetro MAXOUT del sistema principal AS/400.

Definiciones de controlador de sistema principal AS/400

La definición del controlador de sistema principal AS/400 incluye la correlación de los parámetros del programa del sistema principal OS/400 con los parámetros de Communications Server.

La Tabla 24 muestra los parámetros del programa del sistema principal OS/400.

Tabla 24 (Página 1 de 2). Referencia cruzada de los parámetros de Communications Server de AS/400: Parámetros de controlador

OS/400	Perfil/Parámetros de Communications Server	Observaciones
Tipo de enlace: *SDLC	Tipo DLC SDLC-WAC, SDLC-MPA Puerta COM	El tipo de enlace debe coincidir en ambos sistemas. Este parámetro está en la descripción de la línea, pero inclúyalo para que esté completo.
Línea no conmutada conectada	Configurar dispositivos SDLC-WAC, SDLC-MPA, Puerta COM **Línea conmutada**	Este parámetro es para conexiones no conmutadas. Este valor debe coincidir con una definición de línea de sistema principal definida previamente.
Lista de líneas conmutadas	(ninguna)	Este parámetro es para conexiones conmutadas. Este valor debe coincidir con una definición de línea de sistema principal definida previamente.
Tamaño máximo de trama	Configurar dispositivos SDLC-WAC, SDLC-MPA, Puerta COM **Tamaño máximo de PIU** (265–4105)	No es necesario que estos valores coincidan.

Tabla 24 (Página 2 de 2). Referencia cruzada de los parámetros de Communications Server de AS/400: Parámetros de controlador

OS/400	Perfil/Parámetros de Communications Server	Observaciones
Identificador de red remota	Configurar nodo **Nombre de CP completamente calificado** (primer campo)	Estos valores deben coincidir.
Nombre de punto de control remoto	Configurar nodo **Nombre de CP completamente calificado** (segundo campo)	Estos valores deben coincidir.
Función de enlace de datos:	Configurar conexiones SDLC-WAC, SDLC-MPA, Puerta COM **Función de la estación de enlace**	Los parámetros de ambos sistemas son complementarios. Si la función del sistema principal es primaria, la estación de trabajo Communications Server debe configurarse como secundaria o negociable. A menos que se utilice multipunto (*MP), es mejor establecer la función de enlace de datos en negociable (*NEG).
Dirección de estación	Configurar dispositivos SDLC-WAC, SDLC-MPA, Puerta COM **Dirección de estación de enlace** (01–FE)	Estos valores deben coincidir.
Soporte de sesión CP APPN: (Sí/No)	Configurar conexiones SDLC-WAC, SDLC-MPA, Puerta COM **Soporte APPN**	Deben coincidir si se desean sesiones CP-CP.
Tipo de nodo APPN:	Configurar conexiones SDLC-WAC, SDLC-MPA, Puerta COM **Tipo de CP adyacente**	Estos valores deben coincidir.

Definiciones de dispositivo de sistema principal AS/400

El sistema principal AS/400 puede crear una definición de dispositivo cuando la estación de trabajo Communications Server se conecta sin una definición de dispositivo definida previamente.

La Tabla 25 contiene los parámetros de dispositivo de programa de sistema principal OS/400.

Tabla 25 (Página 1 de 2). Referencia cruzada de los parámetros Communications Server de AS/400: Parámetros de dispositivo

OS/400	Perfil/Parámetros de Communications Server	Observaciones
Nombre de ubicación remota	Configurar LU 6.2 local **Nombre de LU local** o: Configurar nodo **Nombre de CP completamente calificado** (segundo campo)	Estos valores deben coincidir.

Tabla 25 (Página 2 de 2). Referencia cruzada de los parámetros Communications Server de AS/400: Parámetros de dispositivo

OS/400	Perfil/Parámetros de Communications Server	Observaciones
Controlador conectado	(ninguna)	Este parámetro es para conexiones no conmutadas. Este valor debe coincidir con una definición de línea de sistema principal definida previamente.
Nombre de ubicación local		Utilice el valor por omisión proporcionado.
Identificador de red remota	Configurar nodo **Nombre de CP completamente calificado** (primer campo)	Utilice el valor por omisión proporcionado.
Modalidad	Configurar modalidad **Nombre de modalidad**	Utilice el valor por omisión proporcionado.

Descripción de línea de sistema principal AS/400 y Communications Server

La Tabla 26 contiene la descripción de la línea de programa del sistema principal AS/400.

Tabla 26. Referencia cruzada de los parámetros del sistema principal/PC: Descripción de línea

OS/400	Perfil/Parámetros de Communications Server	Observaciones
Dirección de adaptador local:	Configurar conexiones **Dirección de destino de LAN**	Las dos direcciones deben coincidir para establecer la comunicación.

Descripción del controlador del sistema principal AS/400 y Communications Server

La Tabla 27 contiene la descripción del controlador del sistema principal OS/400.

Tabla 27 (Página 1 de 2). Referencia cruzada de los parámetros del sistema principal/PC: Descripción del controlador

OS/400	Perfil/Parámetros de Communications Server	Observaciones
Línea conmutada activa	(ninguna)	Este parámetro es para conexiones no conmutadas. Este valor debe coincidir con una definición de línea de sistema principal definida previamente.
Punto de control remoto	Configurar nodo **Nombre de CP completamente calificado** (segundo campo)	Los nombres deben coincidir.
Identificador de red remota	Configurar nodo **Nombre de CP completamente calificado** (primer campo)	Utilice el valor por omisión o correlacione los parámetros si son diferentes del ID de red local del AS/400.
Descripción del controlador de modelo		Este parámetro debe ser YES si el AS/400 utiliza una red de conexión.

Tabla 27 (Página 2 de 2). Referencia cruzada de los parámetros del sistema principal/PC: Descripción del controlador

OS/400	Perfil/Parámetros de Communications Server	Observaciones
ID de conexión de red y nombre de CP de red de conexión	Configurar redes de conexión **Nombre de red de conexión**	Estos valores deben coincidir para todos los nodos que participan en una red de conexión.

Descripciones de AS/400 Twinaxial

La Tabla 28 contiene la descripción de AS/400 twinaxial.

Tabla 28. Referencia cruzada de los parámetros del sistema principal/PC: Descripción del controlador

AS/400	Perfil/Parámetros de Communications Server	Observaciones
Línea no conmutada conectada	(ninguna)	Este parámetro es para conexiones no conmutadas. Este valor debe coincidir con una definición de línea de sistema principal definida previamente.
Punto de control remoto	Configurar nodo **Nombre de CP completamente calificado** (segundo campo)	Los nombres deben coincidir.
Identificador de red remota	Configurar nodo **Nombre de CP completamente calificado** (primer campo)	Utilice el valor por omisión o correlacione los parámetros si son diferentes del ID de red local del AS/400.
Función de enlace de datos=*SEC:	Configurar conexiones SDLC-WAC, SDLC-MPA Puerta COM **Función de la estación de enlace**	Los parámetros de ambos sistemas son complementarios. Si la función del sistema principal es primaria, la estación de trabajo Communications Server debe configurarse como secundaria o negociable. A menos que se utilice multipunto (*MP), es mejor establecer la función de enlace de datos en negociable (*NEG).

Definiciones de línea de sistema principal AS/400 (X.25)

Las definiciones de línea de sistema principal AS/400 incluyen la correlación de los parámetros de programa de sistema principal OS/400 con los parámetros Communications Server. La Tabla 29 contiene los parámetros de línea X.25.

Tabla 29 (Página 1 de 2). Referencia cruzada de los parámetros de Communications Server de AS/400: Definición de línea de programa del sistema principal OS/400 (X.25)

OS/400	Perfil/Parámetros de Communications Server	Observaciones
Dirección de red local	Configurar dispositivos **Dirección local**	Normalmente ambas direcciones se determinan por el proveedor de la red.
Tipo de conexión	Configurar dispositivos Puerta X.25-COM X.25-WAC **Línea conmutada**	El tipo de conexión de ambos sistemas debe coincidir.

Tabla 29 (Página 2 de 2). Referencia cruzada de los parámetros de Communications Server de AS/400: Definición de línea de programa del sistema principal OS/400 (X.25)

OS/400	Perfil/Parámetros de Communications Server	Observaciones
Soporte de DCE X.25	N/D	Debe establecerse en YES, si la conexión entre los dos sistemas es de punto a punto, sin pasar a través de una red X.25.
Tamaño máximo de trama	Configurar dispositivos Puerta X.25-COM X.25-WAC **Tamaño máximo de PIU**	El Tamaño máximo de trama debe coincidir en ambos sistemas.
Tamaño de paquete por omisión	Configurar dispositivos Puerta X.25-COM X.25-WAC **Tamaño de paquete**	Este valor lo determina el proveedor de la red y es el mismo que para Transmitir y Recibir.
Tamaño máximo de paquete	N/D	Este valor lo determina el proveedor de la red.
Módulo	Configurar dispositivos Puerta X.25-COM X.25-WAC **Secuencia**	Este valor lo determina el proveedor de la red.
Tamaño de ventana por omisión	Configurar dispositivos Puerta X.25-COM X.25-WAC **Tamaño de ventana**	Este valor lo determina el proveedor de la red y es el mismo que para Transmitir y Recibir.
Insertar dirección de red	Configurar dispositivos Puerta X.25-COM X.25-WAC	Este valor lo determina el proveedor de la red y debe ser igual para ambos sistemas.
Entradas de canal lógico	Configurar dispositivos Puerta X.25-COM X.25-WAC **Circuito virtual** **Rangos**	Estos valores los determina el proveedor de la red y el tipo de circuito virtual X.25.

Definiciones de controlador de sistema principal AS/400 (PVC X.25)

La definición del controlador de sistema principal AS/400 incluye la correlación de los parámetros del programa del sistema principal OS/400 con los parámetros de Communications Server.

La Tabla 30 muestra los parámetros del programa del sistema principal OS/400 para PVC X.25.

Tabla 30 (Página 1 de 2). Referencia cruzada de parámetros PVC X.25 de Communications Server de AS/400: Parámetros de controlador

OS/400	Perfil/Parámetros de Communications Server	Observaciones
ID de canal lógico X.25	Configurar conexiones Puerta COM X.25, X.25-WAC **Número de canal lógico**	Estos valores los determina el proveedor de la red.
Tipo de enlace: *X25	Configurar conexiones	Los tipos de enlace deben coincidir en ambos sistemas.
Conexiones conmutadas: *NO		Todos los PVC son no conmutados.

Tabla 30 (Página 2 de 2). Referencia cruzada de parámetros PVC X.25 de Communications Server de AS/400: Parámetros de controlador

OS/400	Perfil/Parámetros de Communications Server	Observaciones
Tamaño máximo de trama	Configurar dispositivos Puerta X.25-COM X.25-WAC **Tamaño máximo de PIU**	Los valores de Tamaño máximo de trama no es necesario que coincidan.
Función de estación de enlace	Configurar dispositivos Puerta X.25-COM X.25-WAC **Función de estación de enlace**	Los parámetros de ambos sistemas son complementarios. Si la función del sistema principal es primaria, la estación de trabajo de Communications Server debe configurarse como secundaria o negociable.
Nivel de red X.25	Configurar dispositivos Puerta X.25-COM X.25-WAC **Cumplimiento de CCITT**	Estos valores los determina el proveedor de la red.
Protocolo de nivel de enlace X.25: *QLLC		Este valor debe ser QLLC.

Definiciones de controlador de sistema principal AS/400 (SVC X.25)

La definición del controlador de sistema principal AS/400 incluye la correlación de los parámetros del programa del sistema principal OS/400 con los parámetros de Communications Server.

La Tabla 31 muestra los parámetros del programa del sistema principal OS/400 para SVC X.25.

Tabla 31. Referencia cruzada de parámetros SVC X.25 de Communications Server de AS/400: Parámetros de controlador

OS/400	Perfil/Parámetros de Communications Server	Observaciones
Tipo de enlace: *X25	Configurar conexiones	Los tipos de enlace deben coincidir en ambos sistemas.
Conexiones conmutadas: *YES		Todos los SVC están conmutados.
Tamaño máximo de trama	Configurar dispositivos Puerta X.25-COM X.25-WAC **Tamaño máximo de PIU**	Los valores de Tamaño máximo de trama no es necesario que coincidan.
Número de conexión	Configurar dispositivos Puerta X.25-COM X.25-WAC **Dirección de DTE local**	Este valor lo determina el proveedor de la red.
Función de estación de enlace	Configurar dispositivos Puerta X.25-COM X.25-WAC **Función de estación de enlace**	Los parámetros de ambos sistemas son complementarios. Si la función del sistema principal es primaria, la estación de trabajo de Communications Server debe configurarse como secundaria o negociable.
Nivel de red X.25	Configurar dispositivos Puerta X.25-COM X.25-WAC **Cumplimiento de CCITT**	Estos valores los determina el proveedor de la red.
Protocolo de nivel de enlace X.25: *QLLC		Este valor debe ser QLLC.

Implantación de las configuraciones de Communications Server

A continuación encontrará el procedimiento sugerido para instalar y configurar la red:

1. Planificación del hardware.
2. Planificación de las aplicaciones de software.
3. Creación de los convenios de denominación.
4. Definición de las direcciones de red.
5. Selección de las herramientas de configuración e instalación.
6. Definición de la configuración modelo.
7. Creación de configuraciones e instalación.
8. Creación de materiales de usuario.
9. Mantenimiento de la red.

Este capítulo proporciona la información necesaria para completar el procedimiento sugerido.

Introducción

Una configuración modelo define la información de configuración común a un grupo de servidores. Es aconsejable crear una o varias configuraciones modelo. Cada archivo de configuración de servidor empieza con la configuración modelo y puede contener los pocos parámetros necesarios para personalizar la configuración para ese servidor. Esto da como resultado una configuración de servidor simplificada.

La configuración modelo también puede utilizarse para especificar las opciones de configuración que no pueden especificarse utilizando archivos de respuesta.

Para obtener información sobre la utilización de archivos de respuesta y de archivos modelo para la configuración e instalación, consulte el apartado “Configuración con archivos modelo y de respuesta” en la página 192.

Recuerde sumar los totales para los requisitos de RAM y de espacio de disco fijo para cada estación de trabajo a medida que vaya reuniendo la información de los pasos siguientes. De esta manera, puede asegurarse de tener el hardware adecuado para los usuarios cuando empiecen a utilizar el software que ha elegido para ellos.

Paso 1. Planificación del hardware

Si ya ha determinado que puede utilizar servidores existentes, necesita asegurarse de que el hardware existente tiene la memoria y el espacio de disco fijo adecuados. El hardware existente debe tener también las unidades del sistema correctas, así como, los monitores, impresoras, teclados, adaptadores, módems y cables para el software que se va a instalar.

© Copyright IBM Corp. 1989, 1996

Si va a adquirir nuevos servidores, anote el hardware en las hojas de trabajo que prepare para estos usuarios.

Almacenamiento

Consulte el manual *Quick Beginnings* para ver los requisitos de almacenamiento para Communications Server.

Capacidad de memoria

Cuando planifique el hardware para ejecutar Communications Server, es importante evaluar la forma en que va a utilizarse el servidor en cuanto a lo que se refiere a capacidad. Determine el tipo de sesiones a las que Communications Server dará soporte. Estas incluyen, pero no se limitan a, sesiones TN3270E, sesiones de cliente API SNA y sesiones SNA tradicionales con un sistema principal. Basándose en este número, puede calcular la carga promedio del servidor y determinar la cantidad correcta de memoria para el servidor.

Nota: Estas estimaciones son adicionales a los requisitos del sistema operativo base (Windows NT Server) y de cualquier otra aplicación que se ejecute simultáneamente en el mismo sistema.

Utilice la tabla siguiente para determinar cual va a ser el promedio de carga del servidor:

Tabla 32. Capacidad de memoria

Tipo de sesión cliente	Uso de memoria por sesión
Pasarela SNA (tradicional)	29,9 KB
Cliente API SNA	25,2 KB
TN3270E	15,8 KB

El consumo de memoria estimado de un Communications Server activo sin ningún enlace ni sesión activos es 21 MB. Para minimizar la pérdida de rendimiento, es mejor reducir la cantidad de paginación (intercambio de segmentos de memoria a disco) que se produce. Intente tener la cantidad de memoria real disponible en el sistema necesaria por el software en ejecución, dejando de 5 a 10 MB adicionales como almacenamiento intermedio. Por ejemplo, una instalación de Communications Server que de soporte a sesiones cliente 1000 TN3270E necesitarían las siguientes cantidades de memoria (basándose en los valores de la Tabla 32).

Sistema operativo de Microsoft Windows NT Server	19,0 MB (estimada)
Communications Server para Windows NT	21,0 MB
Sesiones TN3270E (1 000 X 15,8 KB)	15,8 MB
Contingencia	10,0 MB
Memoria total recomendada	65,8 MB

Nota: 65,8 MB no es una cantidad necesaria de memoria para 1 000 sesiones TN3270E. Es una recomendación para el mejor rendimiento.

Velocidad de CPU

Cuando determine la velocidad mínima de procesador necesaria, necesita comprender el número promedio de transacciones que tendrá que procesar el servidor cada minuto. Una transacción es cualquier intercambio de información entre el cliente y el sistema principal a través del servidor, ya sea una renovación de pantalla o una entrada de base de datos solicitada.

Cuando calcule la carga de CPU promedio, multiplique el número de sesiones por el número de transacciones promedio por minuto y por sesión y el factor de escala de la tabla siguiente (basándose en el tipo de sesión).

Tipo de sesión cliente	Factor de carga de CPU (100 Mhz)	Factor de carga CPU (166 Mhz)
Pasarela SNA (tradicional)	,004	,002
Cliente API SNA	,021	,011
TN3270E	,011	,006

Por ejemplo, para dar soporte a 1 000 sesiones TN3270E simultáneas, con un promedio de 6,7 transacciones por minuto, la carga promedio en la CPU de 166 Mhz sería 1 000 X 6,7 X ,006, ó 40.2%. El rendimiento se degrada rápidamente cuando la utilización de la CPU excede el 80%. Una CPU más rápida mejoraría el rendimiento de Communications Server y del sistema. Podría haber más usuarios y transacciones que aprovechasen las ventajas del servidor simultáneamente. Si bien no hay ninguna velocidad máxima de CPU soportada por Communications Server, 100 Mhz es la velocidad mínima recomendada.

Paso 2. Planificación de las aplicaciones de software

Las aplicaciones de software tienen requisitos adicionales a los requisitos de Communications Server. Para obtener más información, consulte la documentación de la aplicación de software.

Paso 3. Creación de los convenios de denominación

Para las redes creadas con Communications Server es necesario crear y utilizar numerosos nombres para múltiples objetos de la red. Algunos de estos nombres pueden ser los mismos en un servidor que en otro, pero otros nombres deben ser exclusivos en la red para evitar conflictos entre los servidores que intentan acceder a los recursos de red.

Por ejemplo, dos LAN pueden tener definidos algunos de los nombres del mismo dominio. Siempre que no se conecten estas LAN, no se producen conflictos. Sin embargo, si deben conectarse más adelante a una LAN principal, sus nombres entrarían en conflicto en la LAN.

Esto significa que debe crear convenios de denominación. Los convenios de denominación son normas y estándares que se utilizan para asignar nombres a los distintos recursos de la red.

Las secciones siguientes listan los convenios de denominación que es necesario planificar. Si ya conoce los convenios de denominación que va a utilizar en la planificación, anótelos cuando planifique la red.

Criterios de denominación

Cuando cree convenios de denominación, debe determinar:

- Los criterios que se han de utilizar para crear nombres y direcciones de la red
- Cómo va a mantener la coherencia de estos nombres y direcciones y, cuando sea necesario, su exclusividad en la red

Si conecta un servidor a una red de sistema principal, por ejemplo, puede encontrarse que la mayoría de los nombres que utilice en la red los elija el personal del sistema principal. En este caso, para las unidades físicas y lógicas necesarias por el sistema principal, debe registrar esos nombres dados para los archivos de configuración del servidor.

Otro ejemplo podría ser denominar los servidores de la red como los nombres de las personas que los utilizan. En una red pequeña, puede funcionar siempre que la cantidad de nombres sea pequeño y puedan continuar siendo exclusivos. Sin embargo, esto no podría funcionar para una red grande porque, generalmente, los nombres de las personas no son exclusivos. Tiene que crear otro convenio para los nombres de estación de trabajo de una red grande.

Cualquiera que sea el criterio que elija para los nombres, asegúrese de anotarlo. De esta manera, puede consultar la información adecuada en el momento en que añada nuevos recursos a la red.

Tipos de nombres y sus restricciones

La mayoría de nombres tienen que ser exclusivos en la red en la que los utiliza. Las secciones siguientes listan los tipos de nombres que puede encontrar cuando planifica la instalación y configuración de una red. Debe consultar estos nombres con anterioridad a la planificación de la red para familiarizarse con ellos.

Se proporciona la siguiente información para cada nombre:

- Una definición
- Si el nombre debe ser exclusivo dentro de una red
- Restricciones de denominación

Nombres utilizados por más de un componente

Los nombres utilizados por más de un componente son:

- ID de red
- Contraseñas
- ID de usuario
- Nombres de unidades direccionables de red (NAU)

ID de red: Los ID de red son nombres dados a las redes y los utilizan todos los servidores y estaciones de trabajo (nodos) dentro de la red específica para mantener una identidad exclusiva en todas las redes conectadas. El ID de red se utiliza

también en los registros de errores y en las alertas de gestión de red asociadas con los errores del sistema de redes.

Hay dos maneras ver las redes. Una manera es como una red física que consiste en un “anillo” en un entorno de red en anillo o en una “serie” en un entorno de red Ethernet o PC. La otra manera es como una red lógica que puede no ser igual a la red física. Dos o más redes físicas (por ejemplo, dos redes en anillo y una serie Ethernet) podrían conectarse con la intención de mantenerlas en la misma red lógica.

Los ID de red son exclusivos entre las redes lógicas; de lo contrario, las redes serían lógicamente la misma red. Dentro de una red lógica, los nombres de LU deben ser exclusivos para evitar conflictos de denominación. Entre redes lógicas, el ID de red garantiza los nombres exclusivos. Un nombre de LU puede ser igual en dos redes lógicas; sin embargo, el ID de red para cada red lógica hace que los nombres de LU completamente calificados sean exclusivos. Incluso si las redes no están conectadas actualmente, los ID de red deben ser exclusivos si piensa puentear las redes en el futuro.

Debe registrar los ID de red en IBM. Esto asegura que las redes SNA puedan interconectarse más adelante sin conflictos de direccionamiento. Póngase en contacto con la Sucursal de IBM para obtener más información acerca del registro de los ID de red.

Las restricciones para los ID de red son:

- **Longitud**: De 1 a 8 caracteres
- **Caracteres permitidos**: A a Z, 0 a 9, $, @, #

Contraseñas: Las contraseñas son funciones de seguridad necesarias para las aplicaciones y servicios configurados correctamente para proteger los datos y para restringir el acceso a recursos.

Las contraseñas no tienen que ser exclusivas en la red. Las contraseñas son específicas del usuario.

Las restricciones para las contraseñas de LU-LU son:

- **Longitud**: De 1 a 8 caracteres
- **Caracteres permitidos**: Cualquier serie hexadecimal

Las restricciones para otras contraseñas como, por ejemplo, las de conexiones CPI-C y AS/400, son:

- **Longitud**: De 1 a 10 caracteres
- **Caracteres permitidos**: Cualquier serie ASCII

ID de usuario: Los ID de usuario son nombres exclusivos de identificación que se dan a los usuarios de los recursos de la red para que puedan acceder a la base de datos, LAN o recursos del sistema principal con emulación.

Los ID de usuario deben ser exclusivos en la red.

Las restricciones para los ID de usuario son:

- **Longitud**: De 1 a 8 caracteres

- **Caracteres permitidos**: A a Z, a a z, 0 a 9, $, @, #

Nombres de unidades direccionables de red (NAU)

Los tipos de nombres que puede tener que especificar en Communications Server son:

- Nombres de punto de control (CP)(nombres de nodos locales)
- Nombres de unidad lógica (LU)

Nombres de punto de control (CP) (nombres de nodos locales): El punto de control (CP) es responsable de gestionar el nodo y sus recursos. En un nodo final APPN, el punto de control debe comunicarse con el punto de control de un nodo de red adyacente para obtener los servicios de red APPN. En un nodo de red APPN, el punto de control debe comunicarse con los puntos de control de los nodos de red adyacentes para gestionar la red. El punto de control direcciona las funciones como, por ejemplo, la activación y desactivación del adaptador y la activación y desactivación del enlace y ayuda a las LU en el inicio y la terminación de las sesiones.

El nombre de punto de control es la segunda mitad del nombre de CP completamente calificado de la definición de NODO de Communications Server.

Los nombres de punto de control deben ser exclusivos en la red. Sin embargo, un nodo puede tener múltiples nombres de PU que se definen en la definición de conexión (**LINK_STATION**) y se intercambian en XID3 a diferentes sistemas principales. Estos múltiples nombres de PU deben ser exclusivos en el nodo y en el sistema principal con el que se conecta.

La PU y el punto de control no son iguales para VTAM de subárea. En ese VTAM, se define un nombre de PU para cada nodo periférico de un dominio VTAM y representa la visión que VTAM tiene de los nodos periféricos. Los nodos periféricos no conocen los nombres de PU en VTAM; es decir, VTAM no envía los nombres de PU a los nodos periféricos. Si desea que el nombre de PU en un nodo periférico sea el mismo que el definido en VTAM, debe coordinarlo. Se recomienda hacerlo, pero para SNA no es necesario.

Para VTAM, el punto de control es una LU, utilizada para activar las sesiones de LU 6.2 entre el punto de control y una LU VTAM (por ejemplo, CICS). El nombre de punto de control definido en el nodo periférico debe coincidir con una definición de LU en VTAM, si VTAM inicia sesiones LU 6.2 con el punto de control. De lo contrario, VTAM conoce el nombre de punto de control cuando el nodo periférico inicia una sesión con una LU VTAM.

Para Communications Server, el nombre de punto de control (que no incluye el ID de red) se trata como nombre de punto de control de nodo local y su nombre de PU. El único flujo que contiene el nombre de PU de nodo periférico es una alerta. Sin embargo, cuando Communications Server (APPC/APPN) envía una alerta, incluye el nombre de punto de control (el tipo de recurso es CP) en la alerta, no un nombre de PU. Si los emuladores envían un nombre de PU en las alertas, el nombre es el mismo que el nombre de punto de control (de nuevo, porque Communications Server utiliza el nombre de punto de control como nombre de PU de nodo). El punto focal del sistema principal sólo puede definirse en un enlace en el que el nombre de PU sea igual al nombre de punto de control. Además, los enlaces de sistema principal con un nombre de PU que no sea el nombre de punto

de control no pueden tener sesiones CP-CP con el sistema principal ni direccionar el tráfico APPN en el enlace. Todas las alertas incluyen el nombre de punto de control incluso si la alerta está provocada por una condición de un enlace que utiliza otra PU.

Las restricciones para los nombres de nodos locales son:

- **Longitud**: De 1 a 8 caracteres
- **Caracteres permitidos**: A a Z, 0 a 9, $, @, #
- **Primer carácter**: A a Z, $, @, #

Nombres de unidad lógica (LU): Los nombres de unidad lógica (LU) son nombres dados a entidades lógicas SNA en un nodo que proporciona funciones de soporte para el proceso de transacciones. Esto les permite comunicarse con otras LU de la red, incluyendo las aplicaciones del sistema principal.

Las restricciones de los nombres de LU son:

- **Longitud**: De 1 a 8 caracteres
- **Caracteres permitidos**: A a Z, 0 a 9, $, @, #

Nombres de LU de Sockets sobre SNA: La pasarela Sockets sobre SNA debe tener configurado un nombre de LU para que la pasarela se inicialice satisfactoriamente. La pasarela Sockets sobre SNA definirá dinámicamente el nombre de LU configurado para Communications Server en la inicialización.

La utilización de un convenio de denominación predefinido para nombres de LU de Sockets sobre SNA, puede ayudarle a:

- Controlar los nombres que son LU de la pasarela Sockets sobre SNA y los que representan otras LU de la red.
- Analizar y resolver cualquier error de correlación y direccionamiento que ocurra.
- Habilitar la correlación algorítmica que se ha de utilizar cuando se correlacionan direcciones IP con nombres de LU de Sockets sobre SNA.

Para obtener más información sobre la correlación de direcciones IP con nombres de LU, consulte el apartado “Configuración de AnyNet Sockets sobre SNA” en la página 86.

Paso 4. Definición de direcciones de red

Asegúrese de la coherencia y exclusividad de las direcciones de la red. Cada dirección debe ser exclusiva. Las direcciones que defina dependerán de cómo configure la red. Las secciones siguientes describen las direcciones para:

- LAN
- SDLC
- X.25

Anote las direcciones que utilice para asegurarse, cuando sea necesario, de que ninguna de ellas entra en conflicto y que son coherentes con los convenios de denominación que ha elegido.

Direcciones de adaptadores de la LAN

Las direcciones de los adaptadores de la LAN son números hexadecimales de 12 caracteres codificadas en la tarjeta adaptadora por el fabricante (dirección de adaptador administrada universalmente) o asignada por el administrador de la red (dirección administrada localmente). Cada tarjeta adaptadora de red de la estación de trabajo que está configurando para las comunicaciones de la LAN debe tener una dirección exclusiva.

Puede utilizar las direcciones administradas universalmente, a las que también se hace referencia como “direcciones grabadas”, para las tarjetas adaptadoras de red o puede asignar direcciones administradas localmente. Las direcciones de adaptador de la LAN deben ser exclusivas en la red. Si utiliza direcciones administradas localmente, asegúrese de que las direcciones son exclusivas en la red.

Las direcciones administradas localmente ofrecen una ventaja significativa cuando se produce una anomalía del adaptador que necesita la sustitución del mismo. Puede transferir la dirección existente al adaptador de sustitución y evitar tener que cambiar cualquiera de las configuraciones que haga referencia a esta dirección. Si utiliza direcciones administradas universalmente, tiene que cambiar la dirección de la tarjeta adaptadora de red para todas las estaciones de trabajo que acceden a la tarjeta adaptadora defectuosa.

Las limitaciones para la configuración de direcciones del adaptador de la LAN son:

- **Longitud**: 12 caracteres
- **Caracteres permitidos**: A, B, C, D, E, F, 0-9
- **Rango**: de X'400000000000' a X'7FFF FFFF FFFF'

En la LAN, puede elegir utilizar las direcciones de adaptador de la LAN administradas localmente. Por lo tanto, asignará números hexadecimales como direcciones de adaptador de la LAN a cada uno de los adaptadores de la LAN en lugar de utilizar las direcciones universales de adaptador de la LAN incorporadas en ellos. Puede decidir utilizar un convenio con los siguientes criterios:

- Los primeros 4 dígitos son siempre X'4000'
- Los 3 dígitos siguientes son siempre X'268' que representan el departamento
- Los dígitos finales están dentro del rango de X'01000' a X'FFFFF' que representan las estaciones de trabajo individuales de la red

Las direcciones administradas universalmente en Ethernet están en formato Ethernet. Puede especificar el tipo de formato (Ethernet o red en anillo) cuando utilice direcciones administradas localmente. Cuando configure la dirección de destino en conexiones SNA, asegúrese de que el formato de la dirección es igual al especificado en el remoto. Con el puenteado, es posible estar en una red en anillo localmente y tener una estación de trabajo remota en una Ethernet y utilizar una dirección en formato Ethernet (con intercambio de bytes).

Direcciones de estaciones secundarias SDLC

Las direcciones de las estaciones se utilizan para identificar una estación secundaria en la red.

Las direcciones de las estaciones secundarias deben ser exclusivas en una red. La estación primaria se comunicará con una estación secundaria utilizando la dirección de estación secundaria. La secundaria se comunicará con la primaria utilizando su propia dirección.

Para conexiones de punto a punto, si la estación secundaria da soporte a la dirección de difusión X'FF', la primaria conocerá la dirección secundaria remota. La secundaria puede especificar cualquier valor entre X'01' y X'FE'.

Para las primarias que no dan soporte a la dirección de difusión, la estación secundaria debe establecerse en el mismo valor que está definido en la primaria. El valor debe estar entre X'01' y X'FE'.

Nota: La mayoría de estaciones darán soporte a la dirección de difusión, de modo que la dirección de estación secundaria en la primaria debe utilizar X'FF'.

Las estaciones negociables tienen direcciones de estaciones secundarias locales configuradas entre X'01' y X'FE'. Se utilizará la dirección secundaria de la estación negociada para secundaria.

Para las secundarias en una conexión multipunto, la dirección debe coincidir con el valor especificado en el nodo que proporciona la función de servidor primario multipunto. La dirección estará en el rango de X'01' a X'FE'.

Direcciones X.25

Las direcciones X.25 se utilizan para identificar los recursos en comunicación en redes X.25. Las redes X.25 implantan la recomendación CCITT que define la interfaz entre el equipo terminal de datos y las redes de conmutación de paquetes. Las direcciones X.25 deben ser exclusivas en una red. Puede obtener estas direcciones del proveedor de red X.25.

Direcciones de Internet

Las direcciones del Protocolo de Internet (IP) se utilizan para direccionar los datos a través de la red. Se asigna una dirección IP como mínimo a cada sistema principal TCP/IP. La dirección IP asignada al sistema principal no define ningún sistema principal en la red; define una interfaz de red en ese sistema principal para una red.

Un nodo de Communications Server debe tener una dirección IP exclusiva para cada interfaz de red que direcciona datos TCP/IP a través del nodo. Por ejemplo, un nodo Communications Server que está direccionando tráfico TCP/IP en una red SNA (utilizando la función de pasarela Sockets sobre SNA) necesita direcciones IP exclusivas para la red SNA y la red TCP/IP. La dirección IP de la interfaz TCP/IP identifica la conexión de pasarela Sockets sobre SNA en la red IP, mientras que la dirección IP identifica la conexión en la red SNA, que al sistema le parece una red TCP/IP "virtual".

Una dirección IP consta de un campo de dirección de 32 bits, dividido en dos partes:

- La primera parte del campo de dirección contiene la dirección de red; la segunda parte contiene la dirección de sistema principal.
- El número de bits utilizados para las partes correspondientes a la red y al sistema principal de una dirección IP son variables, según la clase de dirección de la dirección IP.
- Una máscara de red le permite utilizar la parte correspondiente al sistema principal de la dirección IP como una dirección de subred.

La clase de dirección IP se determina leyendo los 3 primeros bits (superiores) de la dirección. Tal como se muestra en la Tabla 33, Communications Server da soporte a las clases de direcciones A, B y C. Para obtener más información, consulte el manual *Guide to Sockets over SNA*.

Tabla 33. Clases de dirección IP soportadas por Communications Server

Clase de dirección	**Máscara de red por omisión**	**Distribución de bits para las direcciones de red y de sistema principal**	**En el caso de una dirección IP decimal con puntos con el formato *a.b.c.d*, el rango de valores para *a* es:**
A	255.0.0.0	Dirección de red de 8 bits; dirección de sistema principal de 24 bits	1–127 Por ejemplo, 9.0.0.0 es una dirección de red IP de Clase A.
B	255.255.0.0	Dirección de red de 16 bits; dirección de sistema principal de 16 bits	128–191 Por ejemplo, 132.11.0.0 es una dirección de red IP de Clase B.
C	255.255.255.0	Dirección de red de 24 bits; dirección de sistema principal de 8 bits	192–223 Por ejemplo, 220.11.44.0 es una dirección de red IP de Clase C.

Paso 5. Selección de las herramientas de configuración e instalación

Communications Server utiliza las herramientas de configuración explicadas en las secciones siguientes. Consulte el manual *Quick Beginnings* para obtener más información acerca de estas herramientas.

Aplicación Configuración de nodos

La aplicación **Configuración de nodos** es una aplicación de ventanas gráficas que le permite gestionar la información de configuración SNA. La aplicación utiliza una vista en árbol para organizar los datos de la configuración SNA para mostrar las relaciones entre las definiciones. Se proporciona al usuario ayuda para las tareas cuando crea una configuración a través de una lista de tareas integradas, en la *Guía de Aprendizaje* en línea y ayuda sensible al contexto. La aplicación es responsable de crear los archivos de configuración para el usuario y de verificar los datos proporcionados.

Configuración remota

Configuración de nodos también puede utilizarse para conectar un Communications Server remoto y configurar directamente sus recursos. El usuario puede gestionar remotamente la configuración para un Communications Server en cualquier lugar de la red.

Un cliente de administración remota sólo instala las aplicaciones de administración en un cliente, incluyendo **Configuración de nodos**. Desde este cliente, un usuario puede administrar y configurar completamente cualquier Communications Server de la red.

Los clientes de administración remota Windows 95 y Windows NT utilizan la seguridad del dominio Windows NT para autentificar la conexión cliente con el servidor sin volver a entrar el id de servidor y la contraseña. El cliente debe formar parte de un dominio Windows NT, por ser partícipe de un dominio de Communications Server o por conectarse localmente con un id de usuario y una contraseña sincronizados.

Es necesario que los usuarios de clientes de administración remota externos al dominio Windows NT proporcionen el id de usuario y la contraseña, a través de una solicitud o almacenando estos valores en el archivo de configuración del cliente.

Los usuarios autorizados para los clientes de administración remota se mantienen en el grupo local IBMCSADMIN, que está ubicado directamente en el Communications Server o en el controlador del dominio en el que Communications Server participa. Este grupo de usuarios se crea durante la instalación y puede administrarse utilizando la aplicación Administrador de usuarios de Windows NT. Los usuarios de los clientes de administración remota deben tener derechos en el grupo IBMCSADMIN para conectarse localmente al servidor.

Archivo de configuración ASCII

Configuración de nodos de Communications Server almacena sus datos de configuración en un archivo de configuración ASCII que el hombre puede leer. Esto permite al usuario modificar los archivos de configuración sin utilizar **Configuración de nodos**. (Consulte el manual *Configuration File Reference* para obtener más información acerca de este archivo y sus sintaxis.) Mediante la utilización de este archivo, un administrador de red puede realizar cambios rápidamente en la configuración utilizando las tareas automatizadas como, por ejemplo, la creación de un script o los servicios de distribución de software como Tivoli TME10 o Microsoft System Management Server.

Al crear configuraciones para que un gran número de servidores las implanten, el administrador de la red puede crear un archivo de configuración modelo que represente los elementos de configuración comunes a todos los servidores. Mediante la utilización de un archivo de respuesta con sólo los cambios necesarios para cada servidor, el administrador puede distribuir el modelo y el archivo de respuesta y fusionar los dos para crear la configuración de destino. Para obtener información detallada sobre cómo utilizar los archivos modelo y de respuesta para la configuración e instalación, consulte el apartado “Configuración con archivos modelo y de respuesta” en la página 192.

Administración de la web

A través de la administración de la Web, un usuario puede modificar el archivo de configuración de un Communications Server cargando el archivo en una ventana de edición. Los cambios se envían al servidor, se verifican y se guardan para utilizarlos inmediatamente. El usuario puede detener y reiniciar el servidor utilizando los cambios realizados o puede aplicar los cambios en la configuración a un sistema en ejecución.

Configuración con archivos modelo y de respuesta

Los archivos modelo y de respuesta de Communications Server le permiten crear o modificar una configuración utilizando un editor. Puede configurar todas las palabras claves y parámetros de configuración de Communications Server con los archivos de respuesta. Tanto los archivos de respuesta como los archivos modelo tienen el mismo formato que los archivos de configuración de Communication Server (.ACG).

Nota: El formato de los archivos .ACG se documenta en el archivo OCDNTS50.DAT contenido en el directorio de instalación de Communications Server (por ejemplo, C:\IBMCS). Consulte el manual *Configuration File Reference* para obtener más información sobre las palabras clave y parámetros utilizados en los archivos .ACG.

Los archivos modelo pueden facilitar la distribución múltiple de configuraciones a servidores remotos. Un archivo modelo puede especificar las palabras clave que son comunes a varios servidores. Por ejemplo, si tiene que configurar múltiples servidores como pasarelas SNA con el soporte de cliente implícito, habrá muchas palabras clave idénticas. Puede crear un archivo de configuración modelo que refleje estas palabras clave comunes.

Puede utilizar los archivos de respuesta para añadir, modificar o suprimir palabras clave de un archivo modelo. El archivo original de configuración modelo no se cambia. Un archivo de respuesta se fusiona con un archivo modelo especificando la palabra clave INCLUDE al final del archivo modelo. Por ejemplo, si un archivo de respuesta se llama *miconfig.rsp*, la última línea del archivo modelo que utilizará el archivo de respuesta es `INCLUDE = miconfig.rsp`. Cuando el archivo modelo y el archivo de respuesta se fusionan, puede dar al archivo de configuración resultante un nombre con la extensión .ACG que lo distinga de otros archivos .ACG.

Cuando se crean configuraciones utilizando los archivos modelo y de respuesta, el programa de utilidad de verificación busca en los directorios en el orden siguiente:

1. El directorio local en el que se está invocando el programa de utilidad de verificación
2. El subdirectorio PRIVATE en el directorio de instalación de Communications Server.

Para asegurarse de que el programa de verificación puede localizar los archivos modelo y de respuesta, debe almacenarlos en el subdirectorio PRIVATE. En el subdirectorio PRIVATE también se almacenan los archivos de configuración (.ACG).

Campos de clave

El campo de clave es el parámetro de una palabra clave que nombra la palabra clave y la identifica de forma exclusiva entre otras palabras clave del mismo tipo. El parámetro @KEY_NAME especifica el campo de clave para la palabra clave.

El campo de clave siempre es el primer parámetro de una palabra clave que tiene un campo de clave (por ejemplo, **MODE_NAME** en la palabra clave **MODE**).

Algunas palabras clave no tienen campos de clave porque sólo pueden especificarse una vez en un archivo de configuración. Un ejemplo de palabra clave que sólo puede especificarse una vez es la palabra clave **TN3270E_DEF**.

Adición de palabras clave a un archivo modelo

Cuando se utiliza el archivo de respuesta para añadir una nueva definición de palabra clave, debe proporcionarse toda la palabra clave. Debe proporcionarse el campo de clave junto con un valor exclusivo. Si se omite cualquier subcampo de la palabra clave, se utilizan los valores por omisión para estos campos. Por ejemplo, para añadir la palabra clave **MODE** a la configuración, el archivo de respuesta puede contener la siguiente palabra clave:

```
MODE=(
     MODE_NAME=MIMODALIDAD
     COS_NAME=#INTER
     CRYPTOGRAPHY=NONE
     DEFAULT_RU_SIZE=1
     MAX_NEGOTIABLE_SESSION_LIMIT=8192
     MAX_RU_SIZE_UPPER_BOUND=4096
     MIN_CONWINNERS_SOURCE=4096
)
```

El contenido del archivo de respuesta supone que no existe la palabra clave **MODE** con el parámetro `MODE_NAME=MIMODALIDAD` en el modelo. Si existe, los parámetros se habrían actualizado con los valores proporcionados en el archivo de respuesta.

Si se ha omitido el parámetro `MODE_NAME` en el archivo de respuesta, se produciría un error durante la verificación de la configuración porque el parámetro `MODE_NAME` no podría identificarse exclusivamente. No se han especificado todos los parámetros disponibles para la palabra clave **MODE** en el archivo de respuesta. Los restantes parámetros utilizan los valores por omisión asignados por el archivo OCDSNT50.DAT. La adición resultante a la configuración sería parecida a esta:

```
MODE=(
     MODE_NAME=MIMODALIDAD
     AUTO_ACT=0
     COMPRESSION=PROHIBITED
     COS_NAME=#INTER
     CRYPTOGRAPHY=NONE
     DEFAULT_RU_SIZE=1
     MAX_NEGOTIABLE_SESSION_LIMIT=8192
     MAX_RU_SIZE_UPPER_BOUND=4096
     MIN_CONWINNERS_SOURCE=4096
     PLU_MODE_SESSION_LIMIT=8192
     RECEIVE_PACING_WINDOW=20
)
```

Modificación de una palabra clave en un archivo modelo

Cuando se utiliza un archivo de respuesta para modificar una definición de palabra clave existente, la palabra clave original debe existir en el archivo modelo. Si no existe en el archivo modelo, el archivo de respuesta añade una entrada a la nueva configuración. Debe especificarse el parámetro de clave en el archivo de respuesta para identificar la palabra clave de destino. Sólo aquellos parámetros especificados en la palabra clave del archivo de respuesta se actualizan en la palabra clave del archivo modelo. Los parámetros no especificados en el archivo de respuesta no se cambian. Por ejemplo, si está la palabra clave **MODE** siguiente en el archivo modelo:

```
MODE=(
     MODE_NAME=#INTER
     AUTO_ACT=0
     COMPRESSION=PROHIBITED
     COS_NAME=#INTER
     CRYPTOGRAPHY=NONE
     DEFAULT_RU_SIZE=1
     MAX_NEGOTIABLE_SESSION_LIMIT=8192
     MAX_RU_SIZE_UPPER_BOUND=4096
     MIN_CONWINNERS_SOURCE=4096
     PLU_MODE_SESSION_LIMIT=8192
     RECEIVE_PACING_WINDOW=20 )
```

y se especifica la siguiente palabra clave en el archivo de respuesta:

```
MODE=(
     MODE_NAME=#INTER
     AUTO_ACT=10
)
```

la configuración resultante tendría la siguiente definición de palabra clave **MODE**:

```
MODE=(
     MODE_NAME=#INTER
     AUTO_ACT=10
     COMPRESSION=PROHIBITED
     COS_NAME=#INTER
     CRYPTOGRAPHY=NONE
     DEFAULT_RU_SIZE=1
     MAX_NEGOTIABLE_SESSION_LIMIT=8192
     MAX_RU_SIZE_UPPER_BOUND=4096
     MIN_CONWINNERS_SOURCE=4096
     PLU_MODE_SESSION_LIMIT=8192
     RECEIVE_PACING_WINDOW=20
)
```

Supresión de una palabra clave de un archivo modelo

Cuando se utiliza el archivo de respuesta para suprimir una palabra clave del modelo, deben especificarse el parámetro de clave y el valor que identifica la palabra clave, junto con la palabra clave `DELETE`. Por ejemplo, si el archivo modelo especifica la siguiente palabra clave:

```
MODE=(
     MODE_NAME=#INTER
     AUTO_ACT=0
     COMPRESSION=PROHIBITED
     COS_NAME=#INTER
     CRYPTOGRAPHY=NONE
     DEFAULT_RU_SIZE=1
     MAX_NEGOTIABLE_SESSION_LIMIT=8192
     MAX_RU_SIZE_UPPER_BOUND=4096
     MIN_CONWINNERS_SOURCE=4096
     PLU_MODE_SESSION_LIMIT=8192
     RECEIVE_PACING_WINDOW=20
)
```

y el archivo de respuesta contiene la siguiente palabra clave:

```
MODE=(
     MODE_NAME=#INTER
            DELETE
)
```

la configuración resultante no contiene la definición de modalidad `#INTER`.

La palabra clave **DELETE** puede aparecer después de la especificación de un *parámetro=valor* o en una línea por sí sola, precediendo o a continuación del parámetro. Por ejemplo, son válidas la siguientes utilizaciones de la palabra clave **DELETE**:

```
MODE=(
     MODE_NAME=#INTER
            DELETE
)
MODE=(
            DELETE
     MODE_NAME=#INTER
)
MODE=(
     MODE_NAME=#INTER DELETE
)
```

La palabra clave **DELETE** puede **no** aparecer delante de una especificación *parámetro=valor* en la misma línea. Por ejemplo, no es válida la siguiente utilización de la palabra clave **DELETE**:

```
MODE=(
     DELETE MODE_NAME=#INTER
)
```

Para suprimir todas las palabras clave de un tipo en particular o para suprimir una palabra clave que no tiene un campo de clave, sólo son necesarias la palabra clave y la palabra clave **DELETE**. Por ejemplo,

```
TN3270E_DEF=(
            DELETE
)
```

Paso 6. Selección de las características de Communications Server

Las características soportadas para Communications Server se describen más abajo. Es posible que su tipo de conexión de soporte a algunas o todas estas funciones:

Configuración de pasarela SNA Mediante la configuración de una pasarela SNA, puede intercambiar datos entre las estaciones de trabajo cliente en sentido descendente y un sistema principal de Systems Network Architecture (SNA). La pasarela realiza una función de concentrador, haciendo que estén disponibles los recursos de LU de uno o varios sistemas principales y las PU de sistema principal para estaciones de trabajo cliente SNA en sentido descendente, en cualquier medio de comunicación soportado por Communications Server.

Configuración de servidor TN3270E Mediante la configuración de un servidor TN3270E, puede intercambiar datos entre estaciones de trabajo cliente TCP/IP en sentido descendente que ejecutan aplicaciones de TN3270E (o TN3270) y un sistema principal de Systems Network Architecture (SNA). El servidor realiza una función de concentrador, haciendo que estén disponibles los recursos de las LU de uno o varios sistemas principales y las PU de sistema principal para sesiones en sentido descendente TN3270E (o TN3270), en cualquier medio de comunicación soportado por Communications Server.

Configuración del servidor TN5250 Mediante la configuración de un servidor TN5250, puede intercambiar datos entre las estaciones de trabajo cliente en sentido descendente de una red TCP/IP que ejecuta aplicaciones TN5250 y un AS/400 de una red SNA. El servidor realiza la función de pasarela, haciendo que estén disponibles sesiones de visualización AS/400 para clientes TN5250 en sentido descendente, en cualquier medio de comunicación soportado por Communications Server.

Configuración de nodo de red APPN Los nodos de red son responsables del mantenimiento y direccionamiento de la información a través de una red APPN. Mantienen un directorio de todos los recursos (LU) disponibles en los nodos finales conectados directamente, así como una topología de todos los nodos de red de la red APPN. Cuando un nodo de la red pide una sesión LU 6.2 independiente, el nodo de red es responsable de la localización del recurso remoto pedido por la sesión y de establecer y direccionar la sesión entre dos nodos.

Configuración DLUR/DLUS Communications Server da soporte a las sesiones LU dependientes en redes APPN. Esto requiere que Communications Server funcione como una peticionario de LU dependientes (DLUR) que pide los servicios de direccionamiento de un servidor de LU dependientes (DLUS), que reside en un sistema principal.

Communications Server da soporte al DLUR para las sesiones y los dispositivos locales, así como para las sesiones y dispositivos en sentido descendente. En cualquier caso, el nodo local debe estar configurado para conectarse a una red APPN.

Configuración de la pasarela AnyNet SNA sobre TCP/IP La pasarela SNA sobre TCP/IP direcciona el tráfico SNA (LU 6.2 independiente) entre redes TCP/IP y SNA. La pasarela SNA sobre TCP/IP, por ejemplo, permite

que las aplicaciones APPC o CPI-C que se ejecutan en otro nodo de acceso AnyNet SNA sobre TCP/IP se comuniquen con nodos similares SNA en una red SNA.

La pasarela AnyNet SNA sobre TCP/IP debe estar configurada como un nodo de red APPN. Esto permitirá que las sesiones APPC se direccionen a los nodos similares SNA adecuados.

Configuración AnyNet Sockets sobre SNA Hay dos tipos de nodos AnyNet Sockets sobre SNA: nodos de acceso y nodos de pasarela. Los nodos de acceso permiten que las aplicaciones de sockets TCP/IP se ejecuten localmente y se comuniquen con otros nodos de acceso o pasarelas de otros lugares de la red SNA. La pasarela AnyNet Sockets sobre SNA sirve de conversor de protocolo, permitiendo que las aplicaciones de una red TCP/IP se comuniquen con aplicaciones de socket que se ejecutan en un nodo de acceso de la red SNA. Mediante la utilización de dos pasarelas, las redes TCP/IP separadas pueden conectarse a través de una red SNA.

Configuración del cliente API SNA Los clientes API SNA son máquinas separadas del Communications Server que tienen la posibilidad de ejecutar aplicaciones SNA a la vez que utilizan el código SNA en el nodo de Communications Server para gestionar realmente la sesión. Communications Server simplemente establece y gestiona una sesión como si el origen fuese el nodo local, pero reenvía los datos de la aplicación al cliente API SNA en lugar de a sus propias API de aplicación.

Loa clientes API SNA proporcionan la posibilidad de ejecutar aplicaciones SNA sin tener que instalar una pila de comunicaciones SNA como, por ejemplo, Communications Server para Windows NT, en la misma máquina. De esta manera, pueden utilizarse las máquinas más pequeñas y menos poderosas para ejecutar aplicaciones SNA, mientras que una máquina más poderosa centralizada puede dedicarse como servidor SNA para estos clientes API SNA.

Los clientes API SNA dan soporte a dos tipos de aplicaciones: aplicaciones APPC (LU 6.2 independiente) y aplicaciones API LUA como, por ejemplo, los emuladores 3270.

Configuración CPI-C o APPC Communications Server da soporte a aplicaciones CPI-C o APPC (por ejemplo, la emulación APPC3270 o 5250 para un sistema AS/400). La red APPC es muy flexible y versátil y, por lo tanto, puede ser muy complicada. La complejidad de esta configuración depende de cómo vaya a utilizar Communications Server y de cuánto trabajo vaya a realizar la aplicación.

Sesiones de LU 6.2 dependiente con un sistema principal Communications Server da soporte a sesiones LU 6.2 dependientes con una PU de sistema principal.

Configuración de 3270 Communications Server da soporte a sesiones 3270 con un sistema principal.

Configuración de punto focal Communications Server da soporte a las ubicaciones de punto focal remotas para el direccionamiento de la información de alertas para aplicaciones de servicios de gestión específicas. El nodo local localizará los puntos focales remotos a través de una red APPN.

Configuración de carpetas compartidas AS/400 Communications Server le permite crear dispositivos de disco en el servidor que se comunican con las carpetas AS/400 a través del sistema de archivos integrado (IFS) de AS/400. Si el servidor comparte estos dispositivos de disco, los clientes pueden emitir NET USE para los mismos. Se pueden conectar múltiples clientes a las carpetas del sistema AS/400 como si fueran unidades de sus estaciones de trabajo.

Paso 6.1 Planificación de programas de aplicación

Revise las aplicaciones para asegurarse de que cumplirá los requisitos que tienen. Específicamente, compruebe los requisitos para:

- Modalidades
- Programas de transacción (TP)
- Definiciones de LU (sistema principal, LU 6.2)
- LU asociadas

Paso 7. Creación de configuraciones e instalación

Necesita determinar cómo va a configurarse e instalarse Communications Server en los servidores de los usuarios. Puede:

- Dar instrucciones a los usuarios para instalar y configurar Communications Server. Puede preparar sus propias instrucciones o imprimir copias del manual *Quick Beginnings*. También debe proporcionar información específica para cada servidor como, por ejemplo, el ID de red, el nombre de punto de control y la dirección de red.
- Debe dar instrucciones a los usuarios para instalar Communications Server con una configuración existente o un archivo modelo. También debe proporcionar un archivo de respuesta adaptado para cada servidor, así como los CD de Communications Server o el acceso a imágenes del CD.
- Configurar e instalar Communications Server en los servidores de los usuarios usted mismo. A menos que tenga un grupo muy pequeño de usuarios, es aconsejable tomar en consideración la utilización de un producto de ayuda para la configuración, instalación y distribución del software para múltiples estaciones de trabajo. Son ejemplos de este tipo de producto IBM NetView Distribution Manager/2 (NVDM/2), Tivoli TME-10 y Microsoft System Management Server (SMS).

Utilización de la configuración e instalación del archivo de respuesta

Si elige utilizar la configuración e instalación del archivo de respuesta, consulte el apartado “Configuración con archivos modelo y de respuesta” en la página 192.

Paso 8. Creación de materiales de usuario

Después de haber planificado la red y de haber determinado cómo va a implantar la planificación, necesita crear materiales de usuario. Esto significa que debe preparar la documentación para la instalación, configuración y uso diario y preparar procedimientos de copia de seguridad.

Preparación de la documentación

Prepare un conjunto de documentación personalizada para ayudar a los usuarios a instalar, configurar y utilizar Communications Server y las aplicaciones locales para sus necesidades particulares. Las secciones siguientes contienen sugerencias para el tipo de información que debe incluir.

Materiales y procedimientos de configuración e instalación

El manual *Quick Beginnings* y las ayudas de instalación en línea se pueden utilizar para ayudar a los usuarios a instalar Communications Server. Las instrucciones que de al usuario deben indicar cual de los pasos siguientes debe llevar a cabo para realizar la instalación del software:

- Cuándo se ha de hacer una copia de seguridad de los archivos de configuración
- Si han de aceptar los valores por omisión para crear un archivo de configuración de Communications Server

  Es posible que necesite proporcionar información de red como, por ejemplo, direcciones de adaptador de la LAN, nombres de red, etcétera.
- Cuándo ha de realizar una instalación con un archivo de respuesta que le ha proporcionado
- Cuándo ha de realizar una instalación con un archivo de configuración personalizado que le ha proporcionado

Si es necesario, proporcione a los usuarios la documentación adecuada.

Materiales y procedimientos de Communications Server

Los siguientes materiales están recomendados para utilizar las funciones y API de Communications Server:

- *Quick Beginnings*
- Programas escritos por el usuario para las API de Communications Server seleccionadas

Inicio y detención de Communications Server

Para el procedimiento de iniciar o detener Communications Server, consulte el manual *Quick Beginnings*.

Si tiene instrucciones diferentes para el inicio o detención, suministre estas instrucciones a los usuarios.

- El número de teléfono de ayuda del sistema principal para la determinación de problemas (póngase en contacto con el personal del sistema principal)
- Procedimientos de conexión para los sistemas o aplicaciones del sistema principal
- El procedimiento para la detención de la aplicación del sistema principal

  Póngase en contacto con el personal del sistema principal.
- Los procedimientos de desconexión

  Las instrucciones deben incluir cualquier requisito especial para desconectar los sistemas o aplicaciones. Esta información puede obtenerse del personal del sistema principal.

Materiales y procedimientos para programas de aplicación

Debe proporcionar a los usuarios los procedimientos y demás información para los programas de aplicación que pueda utilizar en la red. Generalmente, debe proporcionarles:

- Los procedimientos para iniciar los programas de aplicación
- Los procedimientos para ejecutar los programas de aplicación
- Los procedimientos para responder a los mensajes generados por el programa de aplicación
- Los procedimientos para la determinación de problemas
- Si es necesario, los procedimientos para detener el programa de aplicación

Póngase en contacto con el programador de la aplicación para obtener la información precedente.

Materiales y procedimientos para la determinación de problemas

Para los procedimientos sobre la determinación e informe de problemas, consulte el manual *Quick Beginnings*.

Preparación de procedimientos de copia de seguridad

Ocasionalmente, los usuarios pueden borrar o cambiar los archivos de configuración, el registro, el sistema de archivos, los programas de aplicación y otros programas o archivos creados localmente. También, los servidores pueden experimentar borrados o cambios no aceptables, especialmente cuando hay muchos usuarios que acceden a las estaciones de trabajo del servidor a lo largo de un día de trabajo.

Por eso, es necesario preparar y documentar los procedimientos de copia de seguridad para la red. También es aconsejable cambiar los atributos de los archivos seleccionados en los servidores a Sólo lectura para que los usuarios no puedan cambiarlos.

Paso 9. Mantenimiento de la red

Cuando haya completado la planificación para la instalación y configuración de la red y se ejecute diariamente, la tarea que queda es la del mantenimiento. Debe planificar la adición, cambio o eliminación de recursos y usuarios en la red y planificar la resolución de problemas.

Necesitará realizar el mismo nivel de planificación y los pasos de implantación de cambios en la red que los que ha realizado para la configuración inicial. Debe seguir los mismos pasos para estos cambios en la red que los que ha utilizado para la planificación, instalación y configuración inicial.

Communications Server proporciona estas herramientas para ayudarle a supervisar el rendimiento diario de la red:

- **Operaciones de nodos SNA**
- Programas de utilidad de la línea de mandatos
- Administrador de la web
- Cliente de administración remota

- API de gestión de sistemas
- Subagente SNMP
- Supervisor de rendimiento NT

Los siguientes productos también pueden ayudarle a la gestión diaria de la red:

- IBM NetView
- IBM LAN Network Manager
- Tivoli TME-10

Control y mantenimiento de una red

© Copyright IBM Corp. 1989, 1996

Recursos de gestión de sistemas

Este capítulo proporciona una visión general de los recursos de gestión del sistema Communications Server y describe las posibilidades que son comunes a todos los recursos. Cada recurso tiene también algunas funciones que son exclusivas y estas funciones se describen para cada recurso.

Los recursos de gestión del sistema le permiten supervisar y controlar los recursos de comunicaciones de Communications Server. También le permiten ajustar estos recursos para mejorar la eficacia de los servicios de comunicación SNA o para supervisar y probar estos servicios durante la determinación de problemas.

Consulte la publicación *Quick Beginnings* para ver una lista de recursos que puede gestionar.

Puede gestionar Communications Server con los siguientes recursos:

- **Operaciones de nodos SNA**
- Administración remota
- Programas de utilidad de la línea de mandatos
- Administración basada en la web
- Contros ActiveX de Operaciones de nodos SNA
- Módulo Tivoli Plus
- Soporte APPN MIB
- Soporte de operaciones remotas S/390 (ROPS)

Puede utilizar cualquier combinación de estos recursos para la gestión de Communications Server.

Posibilidades comunes de los recursos de gestión de sistemas

Cada recurso de gestión de sistemas puede realizar las siguientes acciones para los recursos:

- Visualizar información de recursos
- Iniciar recursos
- Detener recursos
- Suprimir recursos
- Iniciar conmutadores de vía de acceso

Puede realizar un subconjunto de estas acciones para cada recurso, tal como se muestra en la Tabla 34 en la página 206.

© Copyright IBM Corp. 1989, 1996

Tabla 34. Acciones de gestión para los recursos de Communications Server

Recurso	Visualizar	Inicio	Detener	Supresión	Conmutación de vía de acceso
Conexiones	X	X	X	X	
Información complementaria CPI-C	X			X	
Dispositivos	X	X	X	X	
PU DLUR	X	X	X		
LU 0 a 3 locales	X			X	
LU 6.2 local	X			X	
Sesiones LU 6.2	X		X		
Pasarela PU 2.0/DLUR	X			X	
Conexiones RTP	X				X
Sesiones TN3270E	X		X		
Sesiones TN5250	X		X		

Operaciones de nodos SNA

Operaciones de nodos SNA es un recurso en línea para la supervisión y control de los recursos de comunicaciones mantenidos por Communications Server. **Operaciones de nodos SNA** le permite detener, iniciar y supervisar los recursos de la red.

Puede utilizar **Operaciones de nodos SNA** para ayudar a gestionar los recursos de la red. Las posibilidades de programación de gestión de sistemas de Communications Server le permiten configurar y gestionar los nodos dentro de la red SNA. **Operaciones de nodos SNA** proporciona un diagrama de vista en árbol de la configuración que le permite seleccionar y modificar los recursos de una interfaz gráfica jerárquica.

Puede gestionar múltiples ventanas de la ventana principal de **Operaciones de nodos SNA**.

Puede definir más de una configuración de Communications Server y conmutar entre configuraciones cuando sea necesario. Cuando se inicia Communications Server, se ofrece la configuración por omisión como la primera opción para la configuración de nodos o la operación de nodo a menos que especifique otra configuración. Una vez completada la nueva configuración, puede sustituir la configuración por omisión por la nueva. Utilice **Operaciones de nodos SNA** para aplicar la nueva configuración y asegurarse de que la parte relevante del producto se ejecuta tal como la ha configurado.

Operaciones de nodos SNA le permite lanzar otros programas de Communications Server como, por ejemplo, **Visor de registros**, **Recurso de rastreo** o **Configuración de nodos**.

Administración remota

Configuración de nodos también puede utilizarse para conectarse con un Communications Server remoto y administrar directamente sus recursos. El usuario puede gestionar remotamente los recursos para un Communications Server en cualquier lugar de la red.

Un cliente de administración remota sólo instala las aplicaciones de administración en un cliente, incluyendo **Operaciones de nodos SNA**. Desde este cliente, un usuario puede administrar completamente cualquier Communications Server de la red.

Los clientes de administración remota Windows 95 y Windows NT utilizan la seguridad del dominio Windows NT para autentificar la conexión cliente con el servidor sin volver a entrar el id de servidor y la contraseña. El cliente debe formar parte de un dominio Windows NT, por ser partícipe de un dominio de Communications Server o por conectarse localmente con un id de usuario y una contraseña sincronizados.

Es necesario que los usuarios de clientes de administración remota externos al dominio Windows NT proporcionen el id de usuario y la contraseña, a través de una solicitud o almacenando estos valores en el archivo de configuración del cliente.

Los usuarios autorizados para los clientes de administración remota se mantienen en el grupo local IBMCSADMIN, que está ubicado directamente en el Communications Server o en el controlador del dominio en el que Communications Server participa. Este grupo de usuarios se crea durante la instalación y puede administrarse utilizando la aplicación Administrador de usuarios de Windows NT. Los usuarios de los clientes de administración remota deben tener derechos en el grupo IBMCSADMIN para conectarse localmente al servidor.

Programas de línea de mandatos

Los programas de línea de mandatos le permiten emitir mandatos desde la ventana del indicador de mandatos de Windows NT. La salida de los mandatos se visualiza en la pantalla, pero la salida se puede direccionar a un archivo.

Consulte la publicación *Quick Beginnings* para ver una lista de los programas de línea de mandatos que puede utilizar.

Administración basada en la web

La función de administración basada en la Web de Communications Server le permite gestionar el servidor en una intranet desde cualquier sistema que tenga instalado un navegador de la Web. Para utilizar la función de administración de la Web, debe estar en ejecución un servidor Web en la misma máquina que Communications Server. Puede gestionar múltiples servidores Communications Server, pero sólo puede acceder a un servidor cada vez. Los usuarios deben conectarse a la administración de la Web como miembros del grupo IBMCSADMIN en la máquina Windows NT que ejecuta Communications Server para realizar las funciones de administración.

Esta función puede instalarse desde el CD-ROM de Communications Server. La mayoría de las funciones de **Operaciones de nodos SNA** están disponibles a través de un navegador de la Web. Puede consultar el estado de nodos, obtener información acerca de los recursos, modificar recursos, visualizar y editar archivos de configuración, visualizar registros de mensajes y realizar otras tareas administrativas. La función de administración de la Web también le permite editar archivos de configuración y visualizar el archivo de registro. Los pasos necesarios para utilizar estas funciones están documentados en la página **Welcome to Communications Server Web Administration** de la Web.

Control ActiveX de Operaciones de nodos SNA

Existe una versión de control ActiveX de **Operaciones de nodos SNA**. Este control le permite incorporar **Operaciones de nodos SNA** en cualquier aplicación que permita controles incorporados como, por ejemplo, Microsoft Management Console (MMC). El nombre del control es CSNTACTX y está ubicado en el directorio de instalación del producto. Este control tiene todas las funciones de **Operaciones de nodos SNA** y proporciona la ventaja de incorporar **Operaciones de nodos SNA** en otras aplicaciones, permitiendo cruzar la gestión del producto.

Módulo Tivoli Plus

Si utiliza el Entorno de gestión Tivoli (TME) para gestionar de manera centralizada los dispositivos y aplicaciones en la red, el módulo Communications Server Tivoli Plus le permite gestionar también Communications Server desde TME. El módulo Communications Server Tivoli Plus puede instalarse en el servidor TME. Hay una imagen instalable de TME en el directorio TME del CD-ROM de Communications Server. Para acceder a las funciones instaladas de TME Plus, pulse dos veces en el icono de TivoliPlus que se ha añadido al panel TME **Escritorio para el administrador**. Cuando se pulsa dos veces en el icono IBM CSPlus, se puede utilizar los iconos del panel para realizar las acciones siguientes:

- Distribuir, instalar y desinstalar Communications Server
- Iniciar, detener y consultar el servidor
- Visualizar y modificar los recursos del servidor
- Listar archivos de configuración
- Direccionar mensajes de error desde Communications Server a una consola Tivoli Enterprise
- Establecer supervisores y umbrales para los atributos clave de Communications Server

Cuando pulse dos veces en cualquier icono del panel IBM CSPlus, entre la información de los campos del recuadro de diálogo presentados. Hay ayuda disponible para los campos en el recuadro de diálogo.

Soporte de MIB APPN

Communications Server da soporte a las peticiones del protocolo simple de gestión de red (SNMP) para la información de gestión APPN de cualquier sistema de gestión SNMP.

El Servicio SNMP se instala desde la pestaña **Servicios** bajo el desplegable **Red** del panel de control de Windows NT. Después de instalar el software del Servicio SNMP en el sistema, debe configurarlo con la información válida para que SNMP funcione.

Debe haberse conectado como miembro del grupo Administrador para que el sistema local configure SNMP.

La información de configuración SNMP identifica las comunidades y los destinos de ruptura.

Soporte de operaciones remotas (ROPS) S/390 para el programa NetView

Cuando se emite RUNCMD desde NetView, el valor para el parámetro APPL se debe especificar como APPL=CSRCMDS.

Cuando se emite el mandato RUNCMD, se transmite toda la información, incluyendo el ID y contraseña, y no se protege de ninguna manera a menos que se utilice el carácter de supresión de NetView cuando se emita el mandato RUNCMD. Esta información se visualiza en la pantalla y se entra en el registro de NetView. Si se transmiten contraseñas al servicio ROPS, el usuario es responsable de proteger el terminal NetView y sus registros NetView para que los datos importantes no se vean comprometidos.

Appendixes

© Copyright IBM Corp. 1989, 1996

Apéndice A. Planificación de Communications Server

Este apéndice proporciona la información que necesita saber para planificar el entorno de Communications Server.

Hardware compatible

Esta sección describe el hardware IBM que da soporte a Communications Server. Estas descripciones incluyen información acerca de:

- Adaptadores de comunicación
- Módems
- Adaptadores de cifrado de nivel de sesión

Adaptadores de comunicación

Para obtener una lista de adaptadores de comunicación a los que Communications Server da soporte, consulte la siguiente URL de Internet:

http://www.software.ibm.com/enetwork/commserver/about/comp_products/comp_csnt.html

Módems

Communications Server da soporte a los siguientes tipos de módems:

- Módems asíncronos:
  - Módems 100% compatibles con el conjunto de mandatos Hayes** AT
  - Módems de IBM que cumplen los estándares de interfaz ITU-T (CCITT) V.24/V.28 (EIA RS-232-D) y V.35
  - También se da soporte a módems asíncronos no IBM, así como la función básica de equipo terminal de datos (DTE) estándar de ITU-T (CCITT) V.24 (EIA RS-232-D) para la interfaz de equipo de terminación de circuito de datos (DCE) para comunicaciones asíncronas
  - Módems que cumplen con el estándar RS-232-D de interfaz DTE a DCE
- Módems síncronos y unidades CSU/DSU que dan soporte al conjunto de mandatos V.24bis
- Módems 100% compatibles con el protocolo Hayes AutoSync

Los usuarios de X.25 necesitarán un módem síncrono y unidades CSU/DSU que den soporte al conjunto de mandatos V.24bis o un módem compatible con el protocolo Hayes AutoSync. Consulte al suministrador de la red para ver el tipo de conexión y módem recomendado.

Para obtener una lista de módems a los que Communications Server da soporte, consulte la siguiente URL de Internet:

http://www.software.ibm.com/enetwork/commserver/about/comp_products/comp_csnt.html

© Copyright IBM Corp. 1989, 1996

Adaptadores de cifrado de nivel de sesión

Para utilizar el cifrado de nivel de sesión, debe tener el programa Programmed Cryptographic Facility y uno de los siguientes adaptadores:

- El adaptador de coprocesador criptográfico IBM SecureWay 4758 PCI
- Otros adaptadores que cumplen con la Arquitectura común de criptografía IBM

Nota: Si utiliza un adaptador que no sea IBM 4758, necesitará utilizar los verbos API de criptografía en su lugar. Consulte el manual *Communications Server Programming Guide and Reference* para obtener más información.

Software de emulador

Para obtener una lista de software de emulador al que Communications Server da soporte, consulte la siguiente URL de Internet:

http://www.software.ibm.com/enetwork/commserver/about/comp_products/comp_csnt.html

Consideraciones sobre la compresión de datos

Antes de utilizar la compresión de datos SNA se han de llevar a cabo varios pasos de configuración en los sistemas implicados. Las compresión de datos SNA se da soporte en:

- VTAM V3R4.1 o posterior
- OS/400 V2R3 o posterior

Cuando se realiza la compresión, cada RU se comprime independientemente y se añade una cabecera de compresión a la RU. El TH y RH no se comprimen. No se realiza ninguna compresión cuando la RU es inferior a 20 bytes o mayor que 64 Kbytes, o , en el caso de RLE sólo, si el tamaño de los datos comprimidos, incluyendo la cabecera de compresión es mayor que los datos originales.

Antes de empezar a configurar las características adecuadas de Communications Server para la compresión de datos, asegúrese de que el sistema asociado puede dar soporte a la compresión de datos y está preparado para ello.

Planificación de la conexión sistema principal/VTAM

Antes de poder pedir la compresión de datos en una sesión para un sistema principal S/370 o S/390* con emulación 3270 o comunicaciones de tipo LU 6.2, VTAM Versión 3 Release 4.1 (VTAM V3R4.1) debe estar instalado y configurado para negociar estas peticiones.

El programador del sistema VTAM del sistema principal debe suministrarle las definiciones adecuadas de VTAM necesarias para la compresión de datos. Aquí encontrará una lista que resume las definiciones necesarias. Se dan ejemplos en la siguiente lista.

- Las opciones de arranque de VTAM deben contener el parámetro **CMPVTAM**=x
- Necesita una entrada LOGMODE con el parámetro **COMPRES=**

- Esta entrada LOGMODE debe estar en la tabla Modalidad que está utilizando
- Debe haber una sentencia VTAM APPL con los parámetros **CMPAPPLI=** y **CMPAPPLO=** para la aplicación que va a utilizar
- La definición de LU VTAM para la sesión debe especificar LOGMODE y la tabla Modalidad que se han definido para la compresión.

CMPVTAM Es el parámetro de las opciones de arranque de VTAM que indica el nivel de compresión máximo permitido para cualquier sesión conectada a este sistema principal. La sintaxis de este parámetro es:

```
CMPVTAM=n
```

donde n es el nivel de compresión permitido para una petición, en el rango de 0 a 4. El valor recomendado es 4, que permite utilizar todos los niveles de compresión de datos.

COMPRES Esta es la entrada de tabla VTAM MODEENT de la definición LOGMODE que la LU utilizará. La sintaxis es:

```
COMPRES=valor
```

donde valor significa SYSTEM, REQUESTED o PROHIBITED. SYSTEM sería codificado para todos los tipos de LU soportados.

CMPAPPLO Es el parámetro de definición de aplicación VTAM (APPL) que establece el nivel de compresión pedido para los datos de Unidad de petición/respuesta (RU) de salida. La sintaxis es:

```
CMPAPPLO=n
```

donde "n" es el nivel de compresión de datos pedido para la dirección de flujo de datos PLU -> SLU, también llamados datos de salida. Para todas las sesiones de tipo LU soportadas por Communications Server, el valor de "n" puede ser igual a 0, 1 ó 2, lo que representa el nivel de compresión de datos nivel 0, nivel 1 y nivel 2. Sin embargo, para las LU de tipo 0, 1, 2 y 3, Communications Server siempre reserva los recursos de compresión en el nivel 2.

CMPAPPLI Es el parámetro de definición de aplicación VTAM (APPL) que establece el nivel de compresión pedido para los datos de la Unidad de petición/respuesta (RU). La sintaxis es:

```
CMPAPPLI=m
```

donde "m" es el nivel de compresión de datos pedido para el flujo de datos SLU -> PLU, también llamado datos de entrada. El valor de m depende del tipo de LU utilizado para la sesión:

- Para las sesiones de tipo LU 3270, "m" puede tener el valor igual a 0 ó 1.
- En las sesiones de tipo LU 6.2, "m" puede tener los valores 0, 1 ó 2.

Nota: VTAM siempre representa la LU primaria (PLU) y Communications Server representa la LU secundaria (SLU) para las LU tipo 0, 1, 2 y 3.

A continuación encontrará ejemplos codificados, que se han extraído de los listados VTAM originales, que señalan la utilización y colocación de los parámetros explicados arriba. Preste una atención especial a las líneas resaltadas.

```
************************************************************
SSCPID=20,HOSTSA=20,XNETALS=YES,                                X
GWSSCP=YES,                                                     X
NODELST=NODES1,                                                 X
CMPVTAM=4,                                                      X
CONFIG=K0,SUPP=NOSUP,                                           X
NETID=USIBMRA,HOSTPU=ISTPUS20,HOSTSA=20,SSCPNAME=RAK,           X
SSCPDYN=YES,SSCPORD=PRIORITY,                                   X
ASYDE=TERM,                                                     X
NOTRACE,TYPE=VTAM,IOINT=0,                                      X
NOTRACE,TYPE=SMS,ID=VTAMBUF,                                    X
PPOLOG=YES,                                                     X
NODETYPE=NN,                                                    X
CPCP=YES,                                                       X
CSALIMIT=0,                                                     X
NOTNSTAT,DYNLU=YES,                                             X
IOBUF=(3500,256,3,,1,58),                                       X
LPBUF=(1100,,2,,1,4),                                           X
LFBUF=(100,,,,1,1),                                             X
CRPLBUF=(2400,,,,1,4),                                          X
SFBUF=(60,,,,1,1)
************************************************************
```

Figura 41. Parámetro de arranque de VTAM. Está permitido un máximo de nivel de compresión de 4 en este VTAM.

```
************************************************************************
* LOGMODE PARA PRUEBA DE COMPRESIÓN - BASADA EN D4C32XX3               *
************************************************************************
*                                                                      *
*              3274 MODELO 1C (SNA REMOTA)                    @OY02946*
*              PANTALLA PRIMARIA 24 X 80 (1920)                        *
*              PANTALLA ALTERNATIVA A DETERMINAR POR LA APLICACIÓN     *
*                                                                      *
************************************************************************
D4C3COMP MODEENT LOGMODE=D4C3COMP,                                    *
                 FMPROF=X'03',                                        *
                 TSPROF=X'03',                                        *
                 PRIPROT=X'B1',                                       *
                 SECPROT=X'90',                                       *
                 COMPROT=X'3080',                                     *
                 RUSIZES=X'87F8',                                     *
                 PSERVIC=X'028000000000000000000300',                 *
                 APPNCOS=#CONNECT,                                    *
                 COMPRES=REQD
```

Figura 42. Tabla Logmode de VTAM. La macro MODEENT configurada con la compresión de datos pedida.

```
   VBUILD TYPE=APPL
*********************************************************************
* SENTENCIAS VTAM APPL PARA CICS/MVS* 3.3                            *
*********************************************************************
RAKAC001 APPL ACBNAME=RAKAC001,                                     *
              MODETAB=MTAPPC,                                       *
              EAS=20,                                               *
              SONSCIP=YES,                                          *
              AUTH=(ACQ,VPACE,PASS),                                *
              PARSESS=YES,                                          *
              VPACING=5,                                            *
              CMPAPPLI=1                                 *
              CMPAPPLO=2
```

Figura 43. Sentencia de aplicación VTAM. Controla los niveles máximos soportados para esta sesión.

```
WTCC1102   PU   ADDR=13,
                IDBLK=05D,
                IDNUM=32289,
           etc.
                DLOGMOD=D4C3COMP
                MODETAB=AMODETAB
           etc.

RACC1102   LU   LOCADDR=2,DLOGMOD=D4C3COMP,MODETAB=AMODETAB
           LU
           etc.
```

Figura 44. Definiciones de PU y LU VTAM. La LU RACC1102 utiliza logmode D4C3COMP, que está en la tabla de modalidades AMODETAB.

Planificación de la compresión de datos de AS/400

Cuando esté conectado a un sistema AS/400, necesitará OS/400 V2R3 para poder utilizar la compresión de datos. Todo lo que necesita realmente es asegurarse de tener una definición de MODE que especifique el soporte de compresión. Son necesarios tres parámetros en el perfil “Crear descripción de modalidad” obtenida a través del mandato CRTMODD o a través de menús. Los tres parámetros son:

DTACPR Este parámetro controla la utilización de la compresión de datos. Los parámetros válidos se muestran más abajo:

- **NETATR** Utilice el valor de red de todo el sistema para este parámetro.
- **NONE** No se permite la compresión de datos.
- **ALLOW** Si el sistema remoto pide la compresión de datos, el sistema local permitirá establecer la sesión.
- **REQUEST** El sistema local pide la compresión de datos.
- **REQUIRE** Es necesaria la utilización de la compresión de datos. Si uno de los sistemas no puede realizar la compresión de datos en el nivel pedido, no se establecerá la sesión.

Siempre que la compresión de datos esté permitida y se pida, los dos sistemas negocian el nivel de compresión de datos que se ha de utilizar

en la sesión de acuerdo a los valores de los parámetros **INDTACPR** y **OUTDTACPR**.

INDTACPR Este valor representa el nivel máximo de compresión utilizado para los datos de entrada.

OUTDTACPR Este valor representa el nivel máximo de compresión utilizado para los datos de salida.

En las sesiones LU 6.2, se da soporte a los niveles de compresión de datos 0, 1 y 2 en ambas direcciones, es decir, para el flujo de datos de salida y de entrada.

Para obtener información acerca de la habilitación de Communications Server para la compresión de datos, consulte el manual *Quick Beginnings*.

Consideraciones sobre el rendimiento

El rendimiento de las comunicaciones del sistema en general y del Communications Server en particular, está sujeto a un gran número de variables. El propósito de la siguiente información es introducir algunos de los factores que influyen en el rendimiento de las comunicaciones en un entorno Communications Server.

El rendimiento de las comunicaciones se ve afectado por la velocidad de la línea de comunicaciones. Esta velocidad se expresa normalmente como el número de bits por segundo (bps) que pueden transmitirse en la línea. Normalmente, cuanto más alto sea bps, mayor será el rendimiento de las comunicaciones que se consigue en la línea.

Además de la velocidad de bits, hay otros factores relacionados con la línea que pueden afectar al rendimiento de las comunicaciones. Por ejemplo, algunas líneas sólo pueden transportar datos en una dirección cada vez. Para cambiar la dirección de las comunicaciones (quién puede enviar), la estación eleva una ***petición de emisión*** (RTS) y espera que se emita ***preparado para transmitir*** (CTS). Esto necesita tiempo adicional para esta ***inversión de línea*** (que depende de módem). Otro factor es la calidad de la transmisión de la línea de comunicaciones. Cuando se produce un error de línea, la mayoría de protocolos lo detectarán y volverán a enviar los datos. Una línea que tiene pocos errores de transmisión ofrecerá una mayor productividad.

También se puede conseguir mayor productividad si los protocolos operan en una modalidad de transmisión de datos ***dúplex***, donde el protocolo puede recibir y transmitir simultáneamente. LAN y X.25 son protocolos dúplex. SDLC puede operar en modalidad dúplex y semidúplex.

Para utilizar dúplex para SDLC, debe utilizar un adaptador adecuado (el adaptador MPA no puede dar soporte a dúplex). La estación remota que también puede dar soporte a dúplex.

A medida que aumenta la velocidad de línea, la capacidad de velocidad de bits de la línea se convierte una menor restricción para el rendimiento. En su lugar, la restricción se relaciona con los retardos en los dispositivos que utilizan la línea de comunicaciones (módems, unidades de control o restricciones internas de los sistemas). A velocidades muy altas, estos retardos pueden impactar en el rendimiento de la comunicación más que en la capacidad de velocidad de bits de la línea.

El análisis de estas situaciones es difícil. Por ejemplo, los retardos de la comunicación más largos de lo esperado pueden estar causados por:

- Una línea de comunicación con carga excesiva
- Un sistema principal con carga excesiva
- Una unidad de control 3X74 con carga excesiva
- Un controlador de red 37*xx* con carga excesiva
- Una definición VTAM o NCP inferior a óptima
- Diseño o gestión de red inadecuados
- Confirmaciones excesivas e intercambio de memoria del sistema operativo

En un entorno de comunicación de alta velocidad como, por ejemplo, una LAN, la velocidad de bits de la línea de comunicación es menos significativa porque la capacidad de comunicación se determina grandemente por la velocidad de los dispositivos de comunicación. Con frecuencia se consigue un mejor rendimiento de la comunicación aumentando la potencia del proceso de la estación de trabajo, sistema principal y de otros componentes de la red. Esto no significa que la velocidad de bits de la red LAN no sea nunca una restricción; sino que es posible que sea necesario ejecutar varios sistemas a su capacidad de comunicación antes de que se degrade significativamente el rendimiento de la LAN.

Para resumir, en muchos casos el rendimiento de Communications Server se determina grandemente por factores que están relacionados con la red de comunicación que se utilice. La proporción del rendimiento de comunicaciones a un coste razonable implica una compresión de la red como un todo y el análisis de sus componentes individuales.

Apéndice B. Avisos

Esta información se ha desarrollado para los productos y servicios ofrecidos en EE.UU. Es posible que IBM no comercialice en otros países, los productos, servicios o dispositivos de los que trata este documento. Consulte al representante local de IBM la información sobre los productos y servicios que están actualmente disponibles en su área. El hecho de que esta publicación incluya referencias a productos, programas o servicios de IBM, no implica que sólo se puedan utilizar los productos, programas o servicios de IBM. Se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente. Puede utilizarse en su lugar, cualquier producto, programa o servicio que no infrinja ningún derecho de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes que afecten a los temas tratados en este documento. La posesión de este documento no confiere ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
Estados Unidos

Para consultas sobre licencias en relación a la información de doble byte (DBCS), póngase en contacto con el Departamento de propiedad intelectual de IBM de su país o envíe las consultas por correo a:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

El siguiente párrafo no se aplica al Reino Unido ni a ningún otro país en el que sus disposiciones no se ajusten a la legislación local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN “TAL CUAL” SIN GARANTÍA DE NINGUNA CLASE, NI EXPRESA NI IMPLÍCITA, INCLUYENDO PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRINGIR LA LEY, DE COMERCIALIZACIÓN O DE IDONEIDAD PARA UN PROPÓSITO EN PARTICULAR. Algunos países no permiten la declaración de limitación de responsabilidad en las garantías expresas o implícitas de determinadas transacciones, por lo tanto, el párrafo anterior puede no aplicarse en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Se realizan modificaciones periódicas a la información contenida en esta publicación; estas modificaciones se incorporarán en las nuevas ediciones de la misma. IBM puede mejorar o modificar el producto o productos y el programa o programas descritos en esta publicación en cualquier momento sin avisar.

Cualquier referencia de esta publicación a algún sitio de la Web que no sea de IBM sólo se proporciona por su conveniencia y no sirve, en manera alguna, de

© Copyright IBM Corp. 1989, 1996

aprobación de estos sitios de la Web. Los materiales de estos sitios de la Web no forman parte de los materiales de este producto IBM y la utilización de estos sitios es bajo su propia responsabilidad.

Los usuarios con licencia para este programa que deseen información acerca del mismo para poder: (i) intercambiar la información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) utilizar, de forma mutua, la información intercambiada, deben ponerse en contacto con:

IBM Corporation
Department TL3B/062
P.O. Box 12195
Research Triangle Park, NC 27709-2195
Estados Unidos

La disponibilidad de esta información puede estar sujeta a términos y condiciones apropiados incluyendo, en algunos casos, el pago de una cuota.

IBM proporciona el programa bajo licencia descrito en este documento y todo el material bajo licencia disponible para el mismo, sujetos a los términos de IBM Customer Agreement, International Programming License Agreement o cualquier contrato equivalente entre las partes.

Cualquier dato del rendimiento contenido en esta publicación se ha calculado en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos operativos pueden variar significativamente. Es posible que algunas mediciones se hayan realizado en sistemas en nivel de desarrollo y no existe ninguna garantía de que estas mediciones vayan a ser las mismas en los sistemas disponibles en general. Además, es posible que algunas mediciones se hayan estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables para su entorno específico.

La información relativa a productos no IBM se ha obtenido de los suministradores de estos productos, sus anuncios publicados u otras fuentes públicas. IBM no ha probado estos productos y no puede confirmar la precisión del rendimiento, la compatibilidad y otras reclamaciones relacionadas con productos no IBM. Las preguntas sobre las posibilidades de productos no IBM deben dirigirse a los suministradores de estos productos.

Marcas registradas

Los términos siguientes son marcas registradas de IBM Corporation en Estados Unidos y/o en otros países:

Red avanzada de igual a igual
AIX
AnyNet
APPN
AS/400
AT
BookManager
CICS
DB2/2
eNetwork
Enterprise System/9000
ESCON
ES/9000
FFST/2
First Failure Support Technology/2
Global Network
IBM
IBMLink
IMS
Micro Channel
NetView
OS/2
OS/400
Personal System/2
Portmaster
Presentation Manager
PS/2
System/370
System/390
SystemView
S/370
S/390
TalkLink
VTAM
WebExplorer

Otros nombres de empresas, productos y servicios pueden ser marcas registradas o de servicios de otros fabricantes.

C-bus es una marca registrada de Corollary, Inc.

Java y HotJava son marcas registradas de Sun Microsystems, Inc.

Microsoft, Windows y el logotipo de Windows 95 son marcas registradas de Microsoft Corporation.

PC Direct es una marca registrada de Ziff Communications Company e IBM IBM Corporation la utiliza bajo licencia.

ActionMedia, LANDesk, MMX, Pentium y ProShare son marcas registradas de Intel Corporation en EE.UU. y en otros países.

Para ver una lista completa de marcas registradas de Intel consulte www.intel.com/tradmarx.htm.

UNIX es una marca registrada en Estados Unidos y en otros países, cuya licencia la otorga exclusivamente X/Open Company Limited.

Índice

Números

A

© Copyright IBM Corp. 1989, 1996

C

D

E

F

G

H

I

L

M

N

P

R

S

T

U

V

W

X

Printed in Denmark by IBM Danmark A/S

SC10-3108-00