Network Utility

Instalación, iniciación y guía del usuario

GA10-5247-00

Network Utility

Instalación, iniciación y guía del usuario

GA10-5247-00

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información general bajo el “Apéndice A. Avisos” en la página 361 y la información de seguridad del “Apéndice B. Información de seguridad” en la página 365.

Tercera edición (Junio de 1999)

Este manual es la traducción del original inglés *Network Utility Installation, Getting Started, and User's Guide*, (GA27-4167-02).

Esta edición se aplica al Network Utility Modelos TN1 y TX1, y a Multiprotocol Access Services (MAS) V3.3.

Puede solicitar publicaciones a través de su representante de IBM o de la sucursal local de IBM. En la dirección indicada más abajo no hay stock de publicaciones.

Al final de esta publicación se proporciona un formulario para comentarios del lector. Si dicho formulario se hubiera extraído, dirija sus comentarios a:

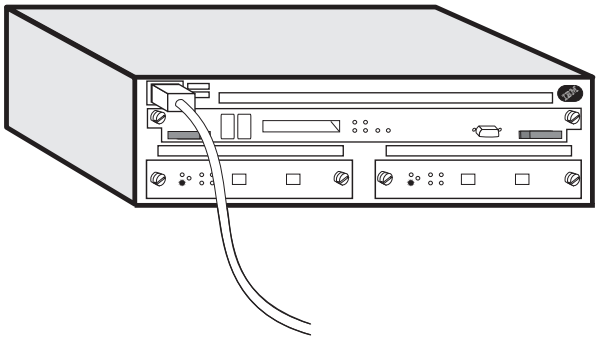
IBM, S.A.
National Language Solutions Center
Av. Diagonal, 571
″Ed. L'Illa″
08029 Barcelona
España

Cuando se envía información a IBM, se otorga a IBM un derecho no exclusivo de utilizar o distribuir la información del modo que estime apropiado sin incurrir por ello en ninguna obligación con el remitente.

Contenido

Acerca de esta guía

Esta guía explica cómo poner a punto el Network Utility de IBM, realizar la configuración inicial, corregir problemas que pueden producirse durante la instalación y utilizar el Network Utility. También contiene ejemplos de configuración detallados para algunas configuraciones de red comunes de Network Utility.



Existen dos modelos del Network Utility de IBM: el Servidor TN3270E de Network Utility (Modelo TN1) y el Transporte de Network Utility (Modelo TX1). A no ser que se indique de forma explícita, el término *Network Utility* se aplica tanto al Modelo TN1 como al Modelo TX1.

Esta guía forma parte de la documentación para el Network Utility que se describe en el apartado “Visión general de la biblioteca” en la página xii. Esta guía le ayuda a familiarizarse con la información de consulta más detallada que se documenta en los demás manuales.

Quién debe utilizar esta guía

Esta guía está dirigida a la persona responsable de la instalación, configuración y gestión del Network Utility.

Cómo proceder

Instalación y configuración inicial

1. Instale el chasis y los cables (consulte el Capítulo 1) utilizando el manual *Installation and Initial Configuration Guide* proporcionado con el producto. (Alternativamente, la instalación puede realizarla el personal de servicio de IBM. Póngase en contacto con el representante de IBM para obtener información adicional).

   Nota: La instalación de los cables para el Adaptador de Canal Paralelo (FC 2299) debe realizarla el servicio de IBM o personal técnico con experiencia en canales.
2. Conecte un terminal o una estación de trabajo para poder configurar y operar el producto (consulte el Capítulo 2) utilizando el puerto serie de la tarjeta del sistema para una conexión local o conecte una línea telefónica al Módem PCMCIA que se enchufa a la tarjeta del sistema para la conexión remota.
3. Decida qué método de configuración desea utilizar y efectúe una configuración inicial del 2216 Modelo 400 o Network Utility (consulte el Capítulo 3).

Aprendizaje

- Si ya tiene experiencia con la interfaz de la línea de mandatos de los productos de direccionamiento de IBM o si prefiere probar las tareas sin seguir una guía de aprendizaje, utilice el Capítulo 4 para repasar algunos de los conceptos básicos de la navegación en la interfaz de la línea de mandatos. Ojee los demás capítulos de la Parte 2. Introducción al Network Utility, para saber dónde encontrar información adicional que puede necesitar.

  Si la interfaz de la línea de mandatos de los productos de direccionamiento de IBM es algo nuevo para usted, utilice el Capítulo 5 como guía de aprendizaje para conocer los conceptos básicos e introducirse en la navegación.
- Si está familiarizado con la configuración básica y las funciones de operación, efectúe una selección en los escenarios de configuración que proporcionamos en la Parte 3. Datos específicos de configuración y gestión. Seleccione una configuración que se asemeje a las características de red:
  - Usuarios del Modelo TN1 — consulte el “Capítulo 12. Servidor TN3270E” en la página 133.
  - Usuarios del Modelo TX1 — consulte el “Capítulo 14. Pasarela de canal” en la página 203, el “Capítulo 16. Conmutación de enlace de datos” en la página 237 o el “Capítulo 19. Redes privadas virtuales” en la página 275.
  - Todos los usuarios — consulte el “Capítulo 18. Definiciones de sistema principal de ejemplo” en la página 259 si la configuración incluye productos de red de sistema principal de IBM.

Configuración final y operación

1. Utilice las operaciones y las tareas de gestión que se introducen en la Parte 2. Introducción al Network Utility y los escenarios que se documentan en la Parte 3. Datos específicos de configuración y gestión, para depurar y completar la configuración inicial.
2. Realice la configuración final. Consulte el manual *Guía del usuario del Programa de configuración* y el manual *Guía del usuario de software*.

Visión general de la biblioteca

El Network Utility y el IBM 2216 Modelo 400 comparten muchas publicaciones. La figura siguiente muestra las publicaciones de la biblioteca, ordenadas de acuerdo con las tareas.

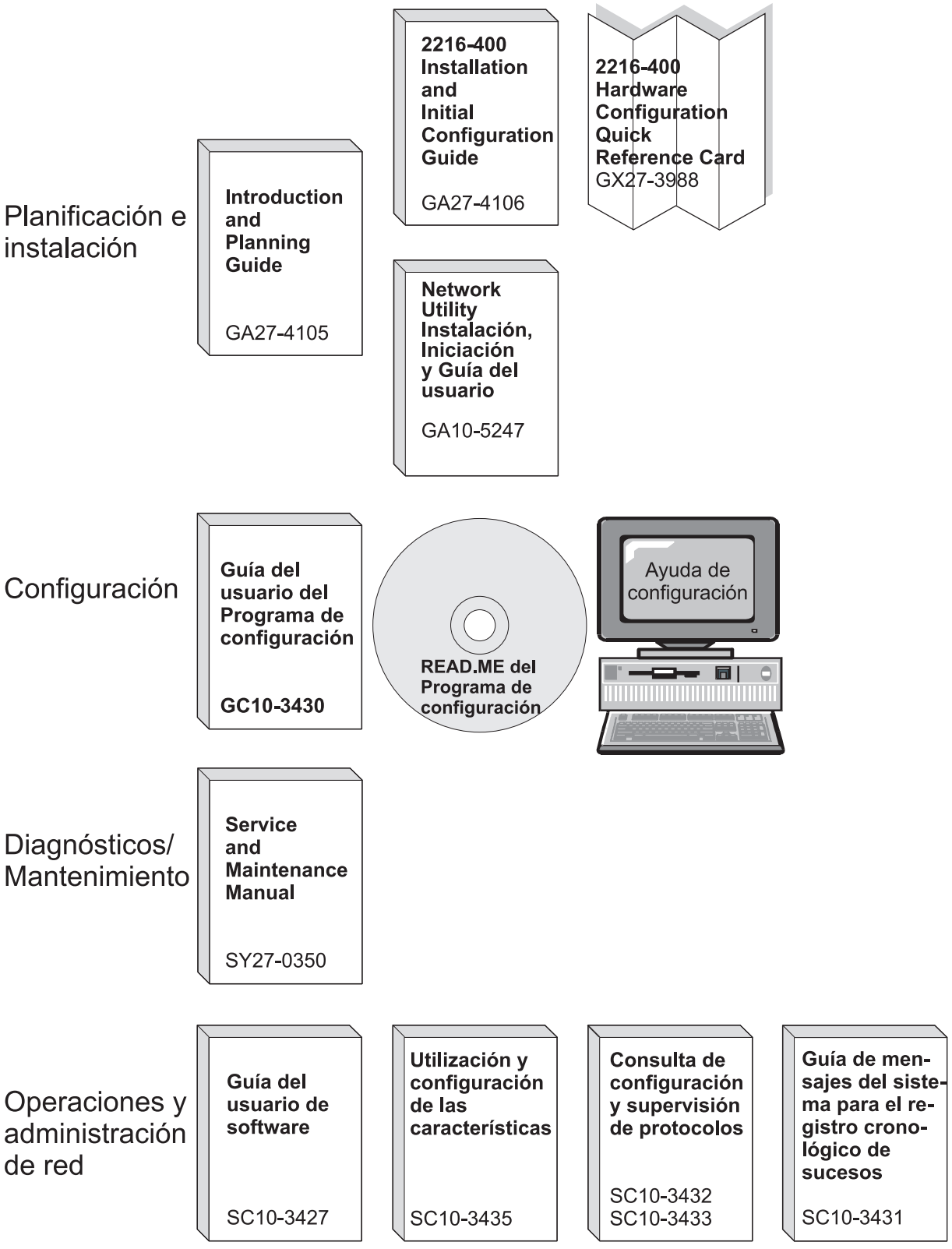


Figura 1. Tareas comunes y la biblioteca para el IBM 2216 Modelo 400 y el Network Utility

Publicaciones impresas que se envían con el producto

Estos documentos se envían en copia impresa y también están contenidos en el CD-ROM de documentación de este producto, SK2T-0405.

Planificación

GA27-4105

2216 Nways Multiaccess Connector and Network Utility Introduction and Planning Guide

Este manual explica cómo prepararse para la instalación y seleccionar el hardware que desea comprar. Incluye especificaciones para el hardware y software para la red. También proporciona información sobre la gestión de redes de direccionamiento.

Instalación y aprendizaje

GA10-5247

Sólo para el Network Utility:

Network Utility Instalación, iniciación y guía del usuario

Este manual explica cómo instalar un Network Utility y verificar su instalación. Además explica cómo utilizar el producto y contiene configuraciones de ejemplo para el producto.

GA27-4106

Sólo para el 2216 Modelo 400:

2216 Nways Multiaccess Connector Modelo 400 Installation and Initial Configuration Guide

Este manual explica cómo instalar el 2216 Modelo 400 y verifica su instalación.

GX27-3988

Sólo para el 2216 Modelo 400:

2216 Nways Multiaccess Connector Hardware Configuration Quick Reference

Este folleto se utiliza para entrar y guardar información de configuración de hardware utilizada para determinar el estado correcto de un IBM 2216 Modelo 400.

Diagnósticos y mantenimiento

SY27-0350

2216 Nways Multiaccess Connector and Network Utility Service and Maintenance Manual

Este manual proporciona instrucciones para diagnosticar problemas del Modelo 400 y del Network Utility así como para realizar reparaciones en los mismos.

Seguridad

SD21-0030

Atención: Información de Seguridad — Lea Esto Primero

Esta publicación proporciona traducciones de avisos de peligro y precaución aplicables a la instalación y al mantenimiento de un dispositivo.

Configuración

GC10-3430

Guía del usuario del Programa de configuración

Este manual describe cómo utilizar el Programa de configuración Nways Multiprotocol Access Services.

Publicaciones enviadas como copia software en el CD-ROM

Estas publicaciones se pueden pedir también por separado como copias impresas.

Operaciones y gestión de red

SC10-3434

Nways Multiprotocol Access Services Guía del usuario de software

Este manual explica cómo:

- Configurar, supervisar y utilizar el software y microcódigo de Nways Multiprotocol Access Services.
- Utilizar la interfaz de usuario de direccionador de línea de mandatos de Nways Multiprotocol Access Services para configurar y supervisar las interfaces de red y los protocolos de la capa de enlace enviados con el 2216 base.

SC10-3435

Nways Multiprotocol Access Services Utilización y configuración de las características

Este manual describe las características de Multiprotocol Access Services (MAS)y explica los mandatos para utilizarlas. Por características se entienden funciones autónomas o que mejoran los protocolos. Ejemplos de estas características son: el Filtro MAC, que filtra tramas basándose en sus direcciones MAC, el Bandwidth Reservation System (Sistema de reserva de ancho de banda), que permite reservar el ancho de banda para tipos de tráfico elegidos por una interfaz serie Frame Relay o PPP o bien la Network Address Translation (Conversión de dirección de red), que permite representar una dirección IP con otra cuando se está ejecutando IP.

SC10-3432

Nways Multiprotocol Access Services Consulta de configuración y supervisión de protocolos, Volumen 1

SC10-3433

Nways Multiprotocol Access Services Consulta de configuración y supervisión de protocolos, Volumen 2

Estos manuales describen cómo acceder y utilizar la interfaz de usuario de la línea de mandatos de Nways Multiprotocol Access Services para configurar y supervisar el software de protocolo de direccionamiento enviado con el producto.

Incluyen información acerca de cada uno de los protocolos que soporta el dispositivo.

SC10-3431

Nways Guía de mensajes del sistema para el registro cronológico de sucesos

Este manual contiene un listado de los códigos de error que pueden producirse, junto con descripciones y acciones recomendadas para corregir los errores.

Cómo solicitar publicaciones de IBM

En EE.UU. puede solicitar publicaciones de IBM llamando al 1-800-879-2755. Dentro o fuera de EE.UU., puede solicitar publicaciones de IBM a través del IBM Publications Direct Catalog en la the World Wide Web en la dirección:

`http://www.elink.ibmlink.ibm.com/pbl/pbl`

IBM traduce muchas publicaciones a diversos idiomas. Puede que las publicaciones que necesite estén disponibles en su idioma.

Visite nuestras ubicaciones Web

Estas páginas web de IBM proporcionan información del producto:

Para el Network Utility: `http://www.networking.ibm.com/networkutility`
Para el Modelo 400: `http://www.networking.ibm.com/216/216prod.html`

Esta página web de IBM proporciona manuales de 2216 base y Network Utility en línea:

`http://www.networking.ibm.com/did/2216bks.html`

Información, actualizaciones y correcciones

Esta página proporciona información sobre cambios técnicos, aclaraciones y arreglos que se han implementado después de que se imprimieran los manuales:

`http://www.networking.ibm.com/216/216changes.html`

Soporte del producto

Estas páginas proporcionan paquetes que se pueden bajar e información de soporte adicional:

Para el Network Utility:
`http://www.networking.ibm.com/support/networkutility`

Para el Modelo 400: `http://www.networking.ibm.com/support/2216`

Parte 1. Cómo empezar

Capítulo 1. Puesta a punto del hardware

Este capítulo incluye los temas siguientes:
- Definición de los elementos necesarios para instalar y configurar el Network Utility
- Montaje del chasis del Network Utility en un bastidor o una superficie plana
- Inserción de tarjetas PCMCIA
- Primer encendido del Network Utility
- Verificación de que los LED indican que el sistema está en buen estado

Instalación del Network Utility

Antes de empezar: Las ilustraciones suponen que todas las ranuras del adaptador están llenas. Un Network Utility totalmente lleno pesa aproximadamente 15 kg (33 libras).

Requisitos previos a la instalación—Necesita disponer de:
- Un terminal ASCII o una estación de trabajo (PC)
- Para la estación de trabajo, software de emulación de terminal ASCII o cliente Telnet (por ejemplo, ProComm)
- Si va a emplear el módem PCMCIA del Network Utility, un módem para la estación de trabajo remota
- Si va a transferir archivos de configuración o código al Network Utility (de un modo que no sea a través de Xmodem), un adaptador LAN para la estación de trabajo
- Si va a utilizar la tarjeta EtherJet PCMCIA del Network Utility, un pequeño distribuidor Ethernet o un cable de cruce para conectar directamente una estación de trabajo con capacidad para Ethernet

Requisitos para el montaje en bastidor—Puede utilizar cualquier bastidor EIA estándar de 19 pulgadas. El bastidor puede estar abierto o cerrado. Sin embargo, si elige un bastidor cerrado, deberá asegurarse de que circula suficiente aire a través del Network Utility. Las cubiertas de la parte frontal del bastidor que obstruyan el paso del aire al Network Utility deberán quitarse o modificarse para permitir la circulación del aire. Del mismo modo, no deberán utilizarse cubiertas posteriores de bastidor sin orificios que no dejen salir el aire del Network Utility o que hagan que se forme una presión posterior procedente de varias máquinas.

1. Verificar el contenido

Verifique que se hayan incluido los elementos siguientes con el Network Utility.

Documentación

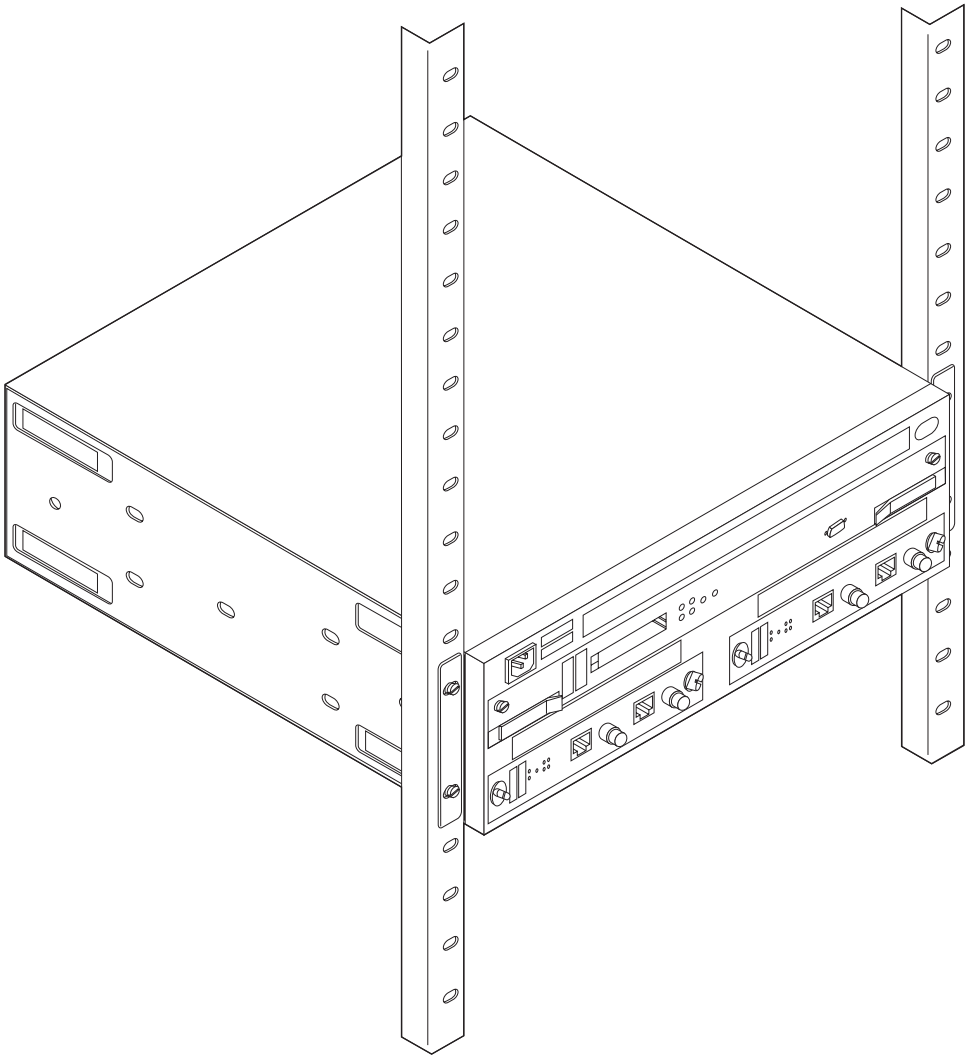
Además de este documento, el paquete debe incluir las publicaciones siguientes:
- *Atención: Información de Seguridad – Lea Esto Primero*, SD21-0030
- *2216 Nways Multiaccess Connector and Network Utility Introduction and Planning Guide*, GA27-4105
- *2216 Nways Multiaccess Connector and Network Utility Service and Maintenance Manual*, SY27-0350
- *Guía del usuario del Programa de Configuración*, GC10-3430
- *2216 Documentation CD-ROM*, SK2T-0405

Hardware
- Network Utility con los adaptadores ya instalados
- Los cables que se han pedido
- Ayuda de instalación para el montaje en bastidor
- Cable de alimentación
- Módem PCMCIA (excepto en países en los que no está disponible el módem PCMCIA)
- Tarjeta PC EtherJet de IBM
- Pieza de sujeción de cable de montaje en bastidor si el Network Utility contiene el FC 2299 (Adaptador de canal paralelo)
- Módem nulo y dos cables de comunicaciones serie de 9 a 25 patillas

Software
- CD-ROM del programa de configuración del IBM 2216 Modelo 400 y del Network Utility
- El código de operación está precargado en el Network Utility

Continúe con
Montaje en superficie - vaya al paso 7 en la página 9.
Montaje en bastidor - vaya al paso 2 en la página 5.

2. Montaje del Network Utility en bastidor



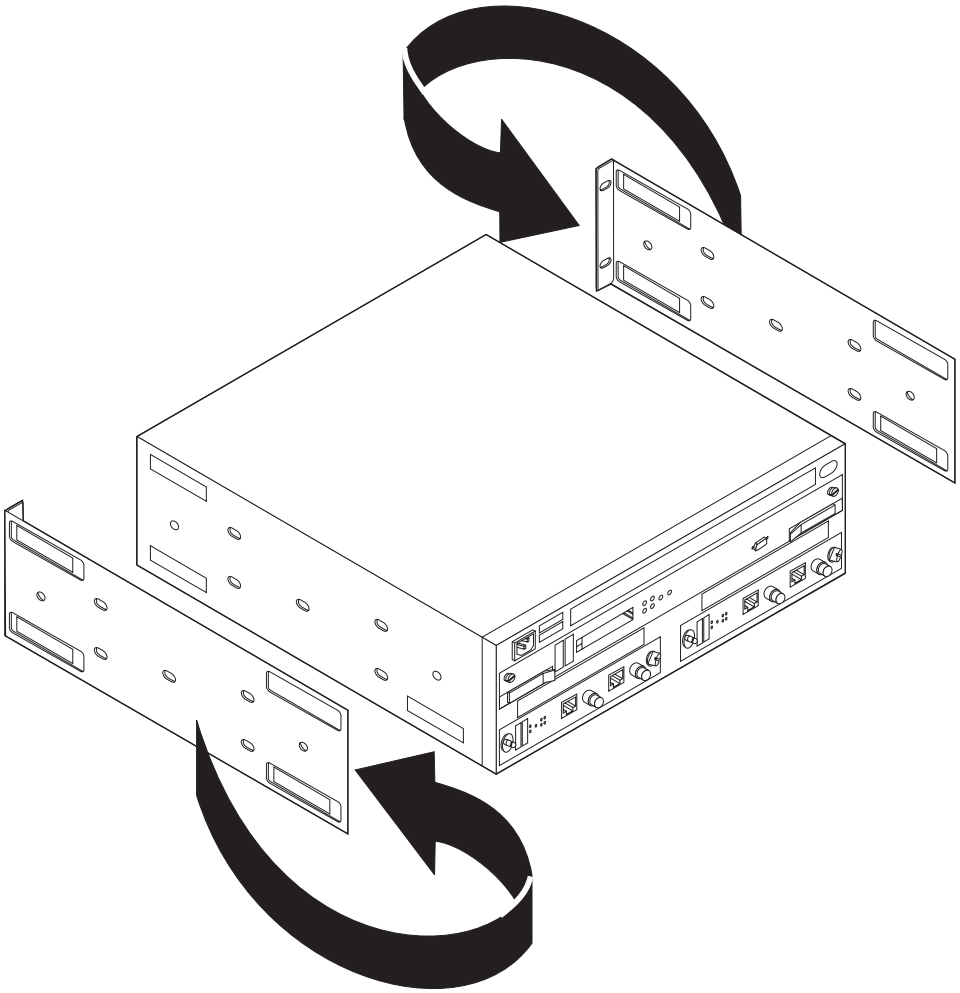
Necesita los elementos siguientes:
- Cables, según sean necesarios
- Cuatro tornillos de montaje en bastidor
- Destornillador

Notas:

1. Si tiene una estantería para el bastidor, instálela antes de continuar.
2. No utilice la ayuda de instalación si tiene instalada una estantería.

Continúe con el paso 3, en la página 6.

3. Montaje en bastidor (Opcional para montaje en superficie)

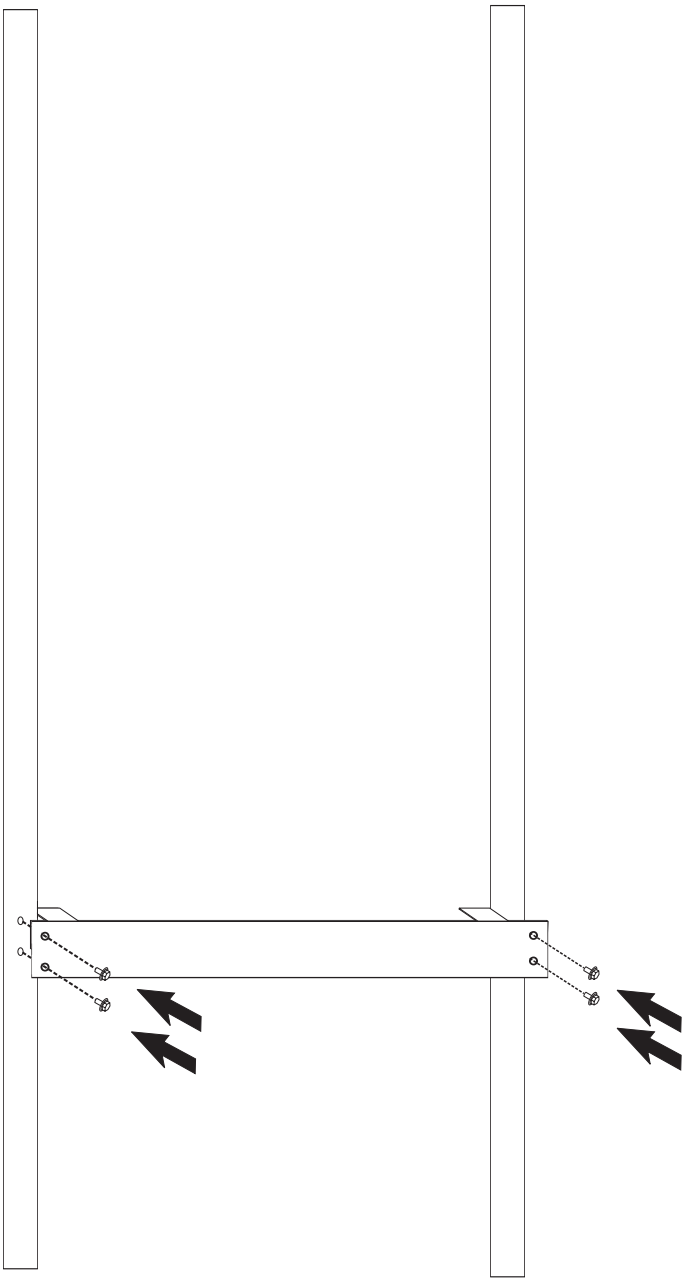


Las piezas de sujeción de montaje del Network Utility se envían con las pestañas orientadas hacia la parte posterior:

1. Quite los dos tornillos de cada pieza de sujeción (uno en la parte frontal y otro en la parte posterior).
2. Invierta cada pieza de sujeción para que el Network Utility pueda montarse en el bastidor.
3. Vuelva a instalar los cuatro tornillos.

Cuando las piezas de sujeción se encajen correctamente, la letra grabada en cada una de ellas quedará en el borde posterior; una A en el lado derecho y una B en el lado izquierdo.

4. Montaje en bastidor



La ayuda de instalación es una barra metálica que sostiene el Network Utility mientras lo instala en el bastidor. Esta barra asegura que el Network Utility y el bastidor queden alineados correctamente.

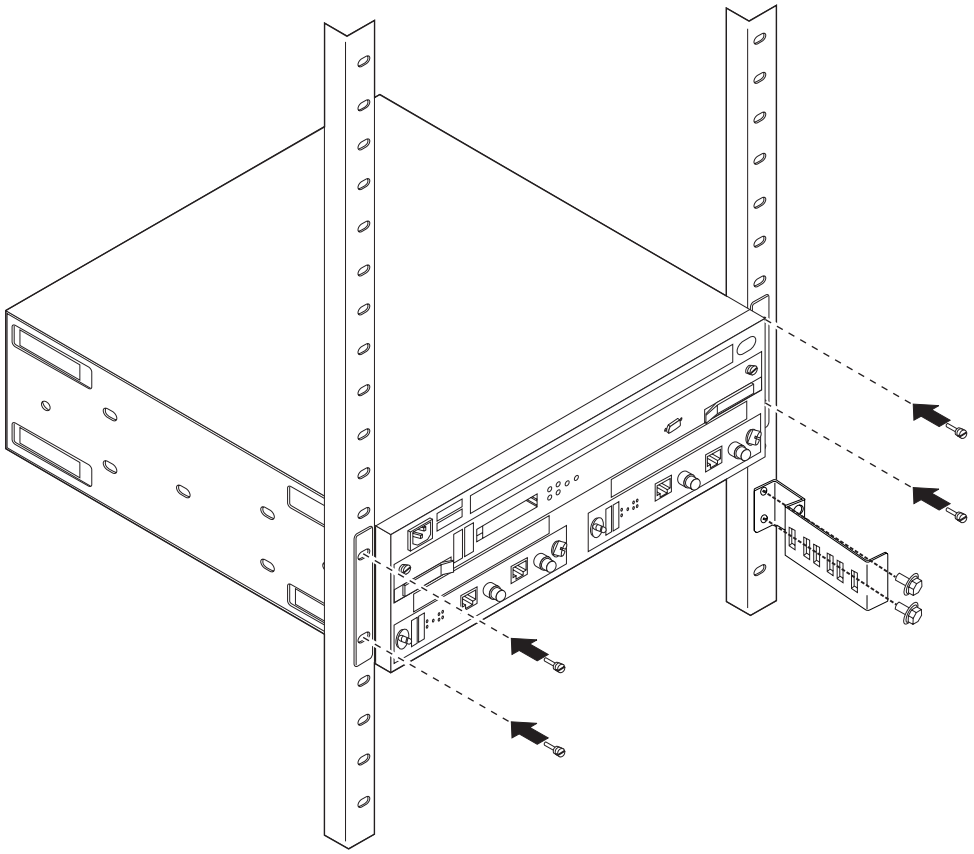
Alinee los orificios de la ayuda de instalación con el bastidor e instale todos los tornillos.

5. Montaje en bastidor

Coloque el Network Utility en la ayuda de instalación del IBM 2216 o en la estantería. Las piezas de sujeción de montaje impiden que el Network Utility caiga en el bastidor durante la instalación.

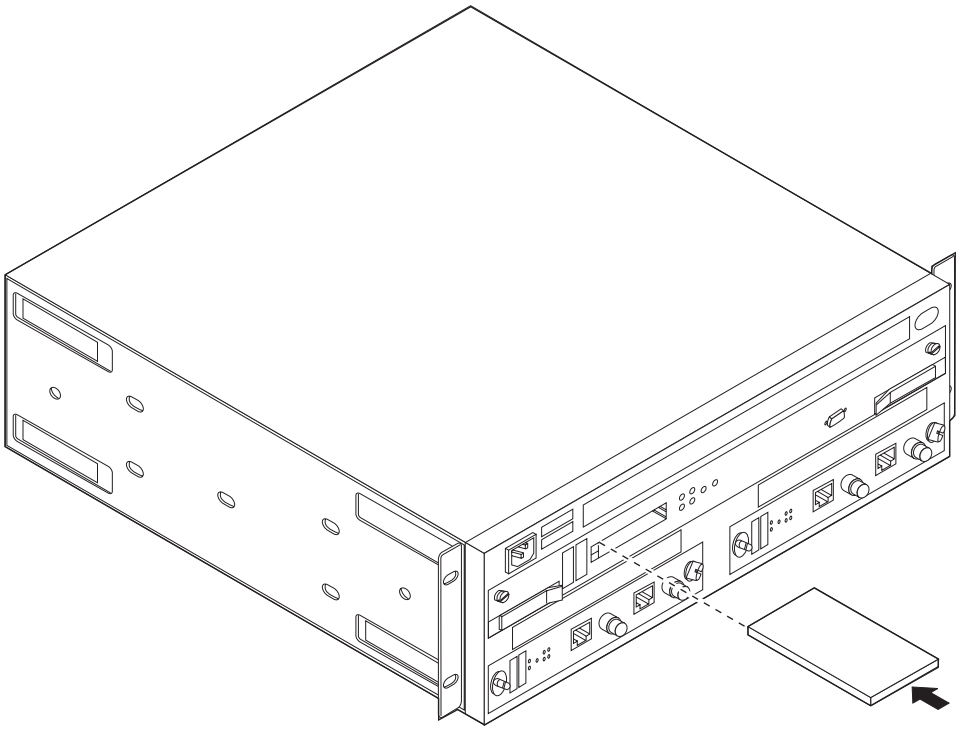
Con la ayuda de instalación instalada, fije el Network Utility mientras realiza el paso siguiente.

6. Montaje en bastidor



1. Instale los tornillos empezando con los tornillos inferiores.
2. Para el FC 2299: Utilizando 2 tornillos, instale la pieza de sujeción de cable de montaje en bastidor en la parte frontal del bastidor debajo del Network Utility.

7. Montaje en bastidor o en superficie

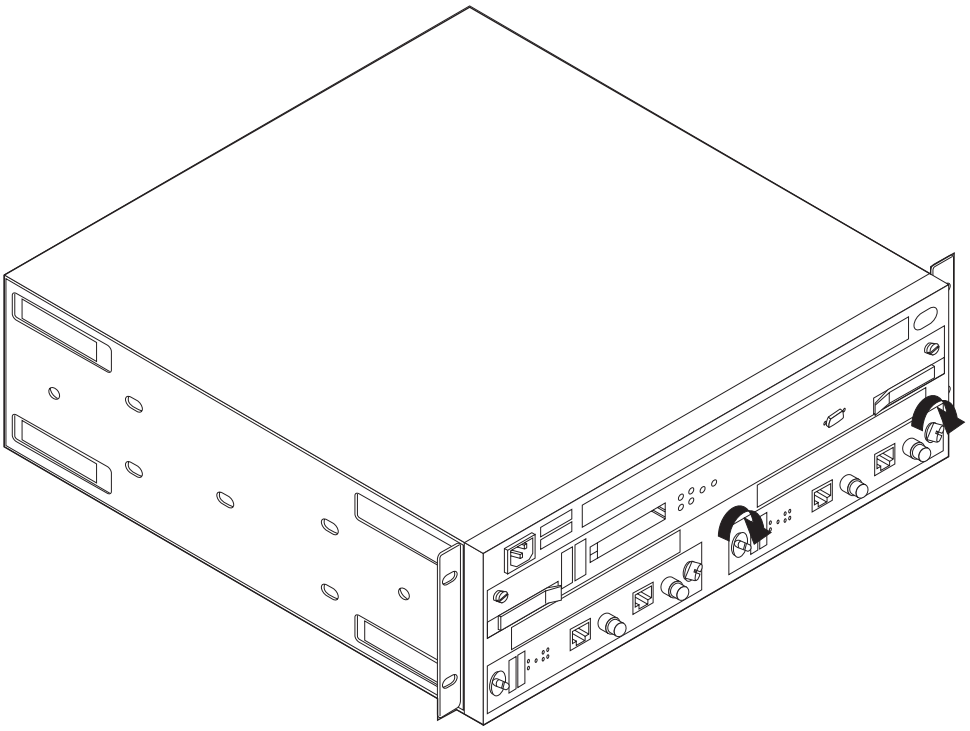


Si va a instalar un módem PCMCIA o un adaptador PCMCIA EtherJet LAN, insértelo en una de las ranuras PCMCIA de la tarjeta del sistema. Conecte el cable del teléfono al módem (un triángulo identifica el lado izquierdo del cable).

Notas:

1. No puede sustituir por una tarjeta PCMCIA Ethernet diferente el adaptador EtherJet LAN que se envía con el Network Utility.
2. El sistema no arrancará si instala dos módems PCMCIA o dos adaptadores PCMCIA Ethernet en un Network Utility.

8. Montaje en bastidor o en superficie



1. Verifique que ***todos*** los tornillos de mariposa estén bien apretados (incluso aunque no los haya aflojado durante la instalación).
2. Conecte el cable de alimentación al Network Utility y la toma de alimentación (para encender la unidad). Tras 4 ó 5 minutos, verifique que estén encendidos los LED correctos (consulte la Tabla 3 en la página 11). Supervise los estados de los LED que se muestran en la Figura 2 en la página 12.

   Mientras la unidad está arrancando y se están probando los adaptadores, es normal que:
   - Los LED verde y amarillo de la Tarjeta del sistema estén encendidos durante un breve periodo de tiempo.
   - Los LED verde y amarillo de la Tarjeta adaptadora estén encendidos durante un breve periodo de tiempo.
   - Los LED amarillos de Unidad de disco duro y de ranura incorrecta (Wrong Slot) de adaptador estén encendidos durante un breve periodo de tiempo.
3. Si detecta algún problema, utilice las tablas y los procedimientos del apartado “Resolución de problemas” en la página 13 para resolverlo o informar sobre él.

9. Complete la puesta a punto (Montaje en bastidor o en superficie)

1. Conecte los cables (excepto para el Adaptador de canal paralelo, FC 2299).
   Nota: Si tiene un FC 2299, para la instalación de los cables se necesitará una persona del servicio técnico de IBM o un empleado del cliente que tenga experiencia en canales.

   Llame al servicio técnico de IBM para instalar los cables del FC 2299. El Canal paralelo y los dispositivos conectados no funcionarán si los cables no se instalan correctamente.
2. Continúe con el “Capítulo 2. Arranque de una consola de usuario” en la página 15 para configurar una consola de terminal de usuario.

10. Tareas del servicio técnico de IBM para el FC 2299

1. Conecte los cables del adaptador al FC 2299 (utilizando los procedimientos del manual *Service and Maintenance Manual* bajo el apartado “Installing Channel Adapters”). No conecte aún los cables de canal del sistema principal.
2. Ejecute pruebas aisladas para verificar que todos los cables del adaptador estén correctamente instalados.
3. Conecte los cables de canal del sistema principal a los cables del adaptador.

Verificación de la puesta a punto del hardware

La Tabla 3 muestra el estado correcto de cada uno de los LED de la parte frontal de la unidad después de que ésta ha completado el arranque (**aproximadamente 4 ó 5 minutos después del encendido)**. Si todos los LED están en estado correcto, puede empezar a configurar la unidad. Consulte la Figura 2 en la página 12 para conocer las ubicaciones de los LED en el Network Utility.

Tabla 3. Estados de los LED de la máquina cuando está operativa

TARJETA	Nombre del LED	Color	Estado
Tarjeta del sistema	PCMCIA 1 (con dispositivo instalado)	Amarillo	APAGADO
	PCMCIA 2 (con dispositivo instalado)	Amarillo	APAGADO
	OK	Verde	ENCENDIDO
	incorrecto	Amarillo	APAGADO
Para todas las tarjetas adaptadoras	OK	Verde	ENCENDIDO
	incorrecto	Amarillo	APAGADO
	Ranura incorrecta (Wrong slot)	Amarillo	APAGADO
	Puerto de E/S (antes de que se cargue la configuración en la unidad)	Verde	APAGADO
	Puerto de E/S	Amarillo	APAGADO

Indicadores LED

El Network Utility tiene diversos diodos emisores de luz (LED) que indican cómo está funcionando la unidad.

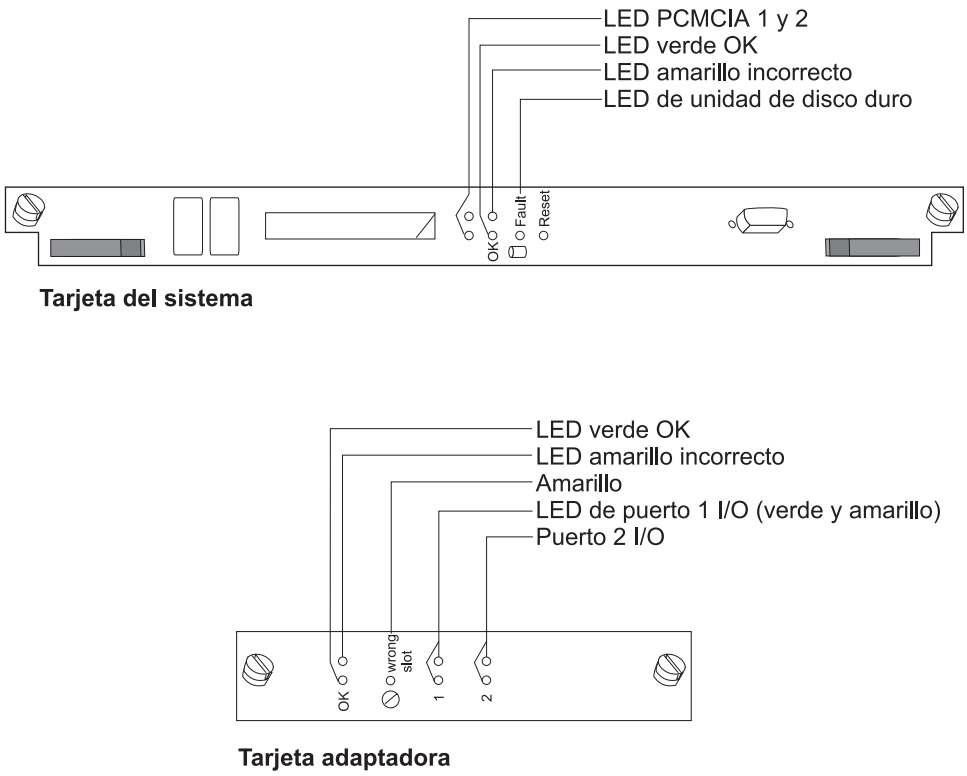


Figura 2. LED de tarjeta del sistema y de tarjeta adaptadora

Estado de la tarjeta del sistema

LED	Significado
PCMCIA 1 o PCMCIA 2 (Amarillo)	Encendido - El dispositivo PCMCIA tiene una anomalía, no está instalado o no está fijado correctamente. Apagado - El dispositivo ha pasado las autopruebas
OK (Verde)	Encendido - El hardware de la tarjeta está operando normalmente. Parpadeante - Cargando del disco fijo
(Amarillo)	Encendido - El hardware de la tarjeta tiene una anomalía.
Unidad de disco duro anómala (Amarillo)	Encendido - La unidad de disco duro ha fallado.

Estado de la tarjeta adaptadora

LED	Significado
OK (Verde)	Encendido - El adaptador está operativo.
(Amarillo)	Encendido - El adaptador tiene una anomalía.
Ranura incorrecta (Wrong Slot) (Amarillo)	Encendido - Póngase en contacto con el servicio técnico.

LED	Significado
Puerto[1] verde	Encendido - El puerto está operando normalmente (habilitado y configurado). Apagado - El puerto no está configurado o está inhabilitado. Parpadeante (sólo para el adaptador ESCON) - Se está ejecutando la prueba de medición de alimentación óptica.
Puerto[1] amarillo	Encendido - Uno o más puertos tienen una anomalía de hardware. Parpadeante - Uno o más puertos tienen una anomalía de red o de E/S de puerto. Utilice los Procedimientos de análisis de mantenimiento (MAP) de la publicación *2216 Nways Multiaccess Connector and Network Utility Service and Maintenance Manual* para aislar el problema. Apagado - No se ha detectado ningún problema.

Números de teléfono importantes

Nombre de contacto	Número de teléfono
Administrador del sistema:	
Servicio técnico:	

Resolución de problemas

Para identificar y corregir problemas que se producen durante la puesta a punto, responda a las preguntas y realice las acciones apropiadas que se indican:

En la tarjeta del sistema, ¿está encendido el LED amarillo de Incorrecto?

Sí: Hay una anomalía en la tarjeta.

1. Desconecte el sistema de la fuente de alimentación.
2. Apriete firmemente la tarjeta.
3. Vuelva a conectar el sistema a la fuente de alimentación.
4. Espere entre 4 y 5 minutos y verifique el estado de los LED.

Si el problema no se ha corregido, póngase en contacto con el servicio técnico.

No: Vaya a la pregunta siguiente.

En la tarjeta del sistema, ¿está apagado el LED verde de OK?

Sí: El LED verde lo enciende el código de operación.

Si el LED verde no se enciende, póngase en contacto con el servicio técnico.

No: Vaya a la pregunta siguiente.

En la tarjeta del sistema, ¿está encendido el LED de puerto PCMCIA?

Sí: La ranura de tarjeta PCMCIA está vacía o la tarjeta ha fallado la autoprueba de encendido. Apriete firmemente la tarjeta.

Si el problema no se ha corregido, póngase en contacto con el servicio técnico.

No: Vaya a la pregunta siguiente.

1. Los LED de puerto de los adaptadores WAN multipuerto (FC 2282, FC 2290 y FC 2291) reflejan el estado de uno o varios de los puertos.

En las tarjetas de E/S de las ranuras 1 y 2, ¿están encendidos los LED amarillos de Incorrecto?

Sí: Hay una anomalía en la tarjeta. Apriete firmemente el adaptador.
Si el problema no se ha corregido, póngase en contacto con el servicio técnico.
No: Vaya a la pregunta siguiente.

En las tarjetas de E/S de las ranuras 1 y 2, ¿están encendidos los LED verdes de OK?

Sí: Al parecer, el Network Utility está bien.
No: Apriete firmemente la tarjeta. Si el LED verde de OK aún no se enciende, la tarjeta es defectuosa. Póngase en contacto con el servicio técnico.

Capítulo 2. Arranque de una consola de usuario

Deberá definir un terminal para acceder al Network Utility para la configuración y operación. La información de este capítulo ayuda a:
- Conocer los modos en que puede definir un terminal
- Elegir el mejor método para el entorno
- Conectar y activar el terminal utilizando valores por omisión

Cuando haya finalizado este capítulo, deberá tener un terminal activo, que deberá estar en el indicador de mandatos inicial, preparado para la configuración.

Métodos de acceso

Puede acceder y conectarse al Network Utility de varios modos que se resumen en la Tabla 4.

Tabla 4. Opciones de conexión de consola de usuario

Conexión física	**Protocolo de línea**	**Protocolo de acceso**	**Direcciones IP por omisión**
Puerto serv + módem nulo Puerto serv + módem externo Módem PCMCIA	Caracteres asíncronos	Emulación de terminal ASCII	No aplicable
	SLIP	Telnet	Network Utility = 10.1.1.2 Estación de trabajo = 10.1.1.3
EtherJet PCMCIA	IP	Telnet	Network Utility = 10.1.0.2 Estación de trabajo = 10.1.0.3
Cualquier interfaz de red IP	IP	Telnet	Ningún valor por omisión

Realice las conexiones físicas de uno de los modos siguientes cuando desee utilizar:

1. Un **terminal ASCII** o una **estación de trabajo** que está ejecutando software de emulación de terminal:
   - Conexión local a través de un cable de módem nulo conectado al puerto de servicio EIA 232 (consulte la Figura 3 en la página 16). Este tipo de conexión utiliza el adaptador de módem nulo y los dos cables serie de 9 a 25 patillas que se proporcionan con este producto.
   - Marcación remota (utilizando líneas telefónicas) a través del módem PCMCIA (consulte la Figura 4 en la página 16).
   - Marcación remota (utilizando líneas telefónicas) con un módem externo (no aparece ilustrada) conectado al puerto de servicio EIA 232. Esta configuración se utilizará en países donde no hay ningún módem PCMCIA aprobado. Utilice un módem asíncrono que soporte el conjuntos de mandatos Hayes AT. Para determinar qué modems se soportan, consulte las páginas de ventas de literatura del producto en la dirección: `http://www.networking.ibm.com/networkutility`.
2. El **protocolo Telnet** en una estación de trabajo que está ejecutando software TCP/IP:
   - Cualquiera de las conexiones físicas que se describen en los métodos de la alternativa 1.

     Para estas conexiones físicas, la estación de trabajo Telnet ejecuta software TCP/IP que soporta el SLIP (Serial Line Internet Protocol). SLIP es un método para enviar paquetes IP a través de líneas asíncronas.

Telnet a través de SLIP sólo proporciona acceso a la interfaz de la línea de mandatos de código de operación y no a la interfaz de menús de firmware.

- Cable local de un adaptador PCMCIA de LAN de Network Utility (una tarjeta PC EtherJet de IBM) a una estación de trabajo utilizando un distribuidor Ethernet local. La Figura 5 en la página 17 muestra una versión de esta configuración.

  El adaptador Ethernet de la estación de trabajo también se podría conectar directamente a la tarjeta EtherJet a través de una cable cruzado o podría haber una red de área ancha entre la LAN Ethernet y la estación de trabajo Telnet.

  La tarjeta PC EtherJet de IBM del Network Utility es para realizar operaciones y tareas de mantenimiento, por ejemplo para proporcionar una consola de usuario y transferir archivos. No se puede utilizar como interfaz de direccionamiento de red normal.
- Una estación de trabajo conectada a red que esté conectada a cualquier interfaz de red capaz de manejar direcciones IP, de los adaptadores que están en las ranuras de adaptador.

  Esta configuración no aparece ilustrada. La interfaz de red podría estar en un adaptador de LAN, por ejemplo de una Red en anillo Ethernet de 10/100 Mbps o FDDI. También podría estar en cualquier otro adaptador, porque todos ellos soportan el direccionamiento IP. La estación de trabajo Telnet podría conectarse de forma local o remota.

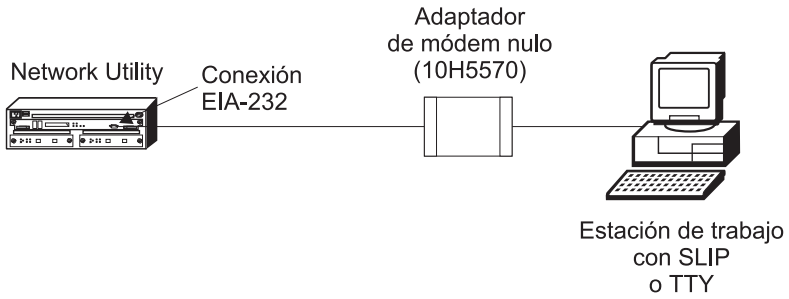


Figura 3. Conexión serie de estación de trabajo local al puerto EIA 232

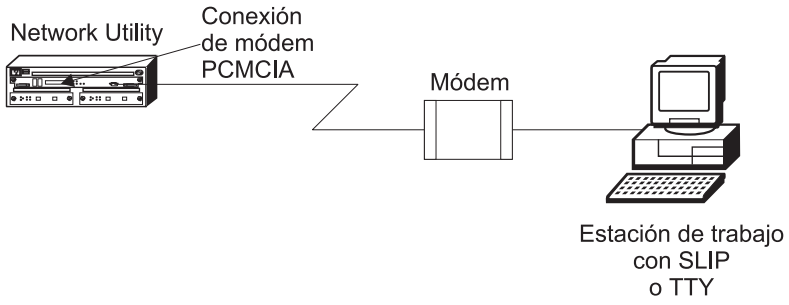


Figura 4. Conexión serie remota al módem PCMCIA

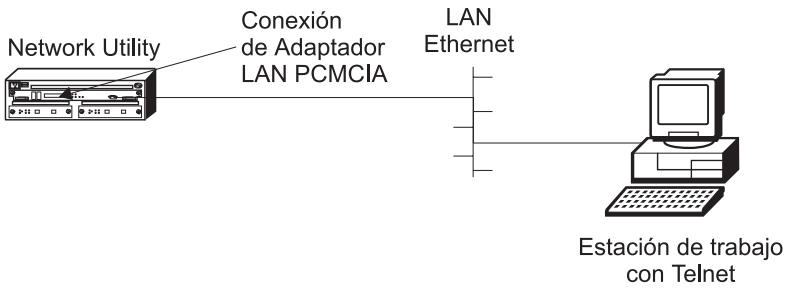


Figura 5. Conexión LAN a través del adaptador PCMCIA de LAN

¿Qué método de acceso debo utilizar?

- **Si es usted un usuario nuevo y está físicamente cerca del Network Utility**, conecte una estación de trabajo directamente a la unidad (consulte la Figura 3 en la página 16) utilizando la emulación de terminal ASCII para la consola de terminal (consulte el apartado “Definición y uso del terminal ASCII”). Las ventajas clave de este método son:
  - Proporciona una puesta a punto fácil.
  - Funciona bien con el software básico de emulación de terminal.
  - No necesita que se configure la unidad.
  - Proporciona una conexión estable si configura y rearranca repetidamente la unidad mientras aprende a utilizar el producto.
  - Proporciona acceso a la interfaz de usuario de firmware, ya que probablemente querrá utilizarla u obtener información acerca de ella.
- **Si es usted un usuario nuevo y está en una ubicación remota respecto al Network Utility**, es preferible la emulación de terminal de marcación a Telnet por algunas de las mismas razones que para un usuario nuevo que está físicamente cerca de la unidad.
- **Si va a colocar un Network Utility configurado en una red de producción**, elija el método de acceso de consola de terminal que mejor se adapte a su configuración de red y también a su estrategia de servicio y operaciones. Puede utilizar Telnet como el método de acceso de consola de terminal ″de cada día″ y la emulación de terminal de marcación como el método de servicio de reserva cuando la red no esté disponible o sea necesario el acceso a firmware. El personal de servicio de IBM utilizará cualquiera de los métodos cuando depure problemas de configuración y de red.

Definición y uso del terminal ASCII

Utilice esta sección si va a definir un terminal ASCII o una estación de trabajo con emulación de terminal. Puede utilizar la emulación de terminal ASCII para acceder al Network Utility, tanto si éste se ha configurado alguna vez como si no.

Una consola de terminal ASCII proporciona acceso al código de operación principal (la interfaz de la línea de mandatos) y a la interfaz de usuario de firmware (consulte el apartado “Firmware” en la página 71). Si se efectúa una marcación de forma remota en el PCMCIA o en un módem externo y rearranca la unidad, perderá la conexión de consola y necesitará volver a marcar[2]. Si está conectado localmente, la conexión de consola se mantendrá durante un rearranque.

2. Si está utilizando un módem externo y éste puede establecerse para que no tenga en cuenta las desconexiones en DTR desde el Network Utility, no perderá la conexión de consola cuando rearranque el Network Utility. Consulte la documentación de usuario para el módem.

Conexión de un terminal ASCII

Conecte un terminal ASCII o un emulador (con el software de emulación apropiado) para proporcionar acceso local o remoto como se muestra en la Figura 4 en la página 16 y la Figura 3 en la página 16. Se soportan los terminales ASCII DEC VT100 y DEC VT220, así como dispositivos que estén configurados para emularlos, por ejemplo sistemas personal computer.

Valores por omisión del puerto serie y del módem PCMCIA

Éstos son los valores por omisión para el puerto serie:

Velocidad 19,2 Kbps
Paridad Ninguna
Bits de datos 8
Bits de parada
1
Tipo de terminal
VT220, Monocromo

Para cambiar los valores del puerto serie, siga estos pasos:

1. Rearranque el Network Utility en el menú principal de firmware, utilizando una de las tareas del apartado “Opciones de arranque: Arranque rápido y obtención de firmware” en la página 46.
2. Seleccione la Opción 1, **Manage Configuration**
3. Mueva el cursor hasta la fila para el puerto serie COM1 y pulse **Intro**
4. Mueva el cursor hasta las características que desea cambiar (por ejemplo, velocidad en baudios) y pulse **Intro**
5. Seleccione el nuevo valor y pulse **Intro**
6. Pulse **Esc** para volver al menú principal de firmware
7. Si desea continuar la secuencia de arranque actual y hacer que el código de operación empiece a utilizar los nuevos valores, pulse **F9** (Iniciar el OS).

   Si desea rearrancar en el firmware y hacer que el firmware empiece a utilizar los nuevos valores, pulse **F3** (Rearrancar).
8. Cambie los valores del terminal o del software de emulación de terminal para que coincidan con los nuevos valores del puerto serie de Network Utility.

El módem PCMCIA es un elemento estándar que se envía con el Network Utility en la mayoría de países. Es un módem de datos V.34 a 33,6 Kbps y negocia la velocidad de datos a utilizar entre él mismo y el módem asociado que se encuentra al otro lado de la red telefónica. Utilizando la compresión de datos, este módem es capaz de proporcionar una velocida de transmisión superior a 33,6 Kbps.

La velocidad de datos entre el sistema Network Utility y el módem PCMCIA toma por omisión 19,2 Kbps, pero se puede aumentar esta cifra para adaptarse a la velocidad superior que los dos módems sean capaces de negociar. Por ejemplo, puede que desee establecer esta velocidad en 57,6 Kbps para que sea más alta que la velocidad de datos efectiva de dos módems a 33,6 Kbps con capacidad de compresión de datos. Si la velocidad de los dos módems es de más de 19,2 Kbps, el aumento de dicha velocidad reducirá el tiempo de transferencia de archivos de Xmodem.

Para cambiar la velocidad de datos y cualquiera de los demás valores del módem PCMCIA, siga el mismo procedimiento proporcionado anteriormente para los valores de puerto serie, pero seleccione COM2, el módem PCMCIA, en lugar del puerto serie.

Atributos de configuración de terminal ASCII

A continuación se proporciona una lista de todas las opciones necesarias para definir un terminal o emulador de terminal que está conectado al puerto de servicio del Network Utility. No todos los terminales (especialmente el 3151 y el 3161) disponen de todas estas opciones. Deberá utilizar la información para establecer las opciones aptas para el terminal.

Valores de terminal y teclas de función

Velocidad en baudios: 19200 bits por segundo

Nota: La velocidad en baudios debe coincidir con la velocidad del puerto serie de servicio del Network Utility.

Paridad: Ninguna
Bits de datos: 8
Bits de parada: 1

Dúplex: Dúplex
Control de flujo: XON/XOFF y RTS/CTS (vea la Nota 1)

Control de pantalla: Pantalla completa ANSI
Ancho de pantalla: 80 caracteres
Altura de pantalla: 24 líneas
Acomodación de línea: ACTIVADA
Desplazamiento de pantalla: ACTIVADO

Conversión de retorno de carro: CR (0Dx)
Conversión de retroceso: Destructivo

Notas:

1. Establezca los terminales y los programas de emulación de terminal que no tienen opciones de control de flujo en “Permanent Request to Send” (″Petición permanente de envío″).
2. Establezca los emuladores de terminal que necesitan una selección de tipo de terminal en VT-220.

Teclas de función

Para acceder al firmware, necesitará utilizar las teclas de función F1, F2, F3, F4, F6 y F9. No todos los terminales o emuladores de terminal proporcionan soporte estándar para estas teclas de función (por ejemplo, los tipos VT100).

El modo más simple de simular estas teclas de función consiste en escribir la secuencia siguiente, no dejando más de dos segundos entre cada paso:

1. **Control-a**
2. El número (no la tecla de función propiamente dicha) de la tecla de función que desea
3. **Intro**

Alternativamente, puede definir el emulador de terminal para que genere las secuencias de teclas de escape siguientes al pulsar una tecla de función:

```
Función 1 (F1):  <Esc> O P         Hex: 1B 4F 50
Función 2 (F2):  <Esc> O Q         Hex: 1B 4F 51
Función 3 (F3):  <Esc> O R         Hex: 1B 4F 52
Función 4 (F4):  <Esc> O S         Hex: 1B 4F 53
Función 6 (F6):  <Esc> [ 0 0 6 q   Hex: 1B 5B 30 30 36 71
Función 9 (F9):  <Esc> [ 0 0 9 q   Hex: 1B 5B 30 30 39 71
```

Nota: En las definiciones de teclas de función:
0 = O mayúscula
0 = el número cero
Todos los caracteres son sensibles a las mayúsculas y minúsculas

Varios usuarios de terminal

Solamente un usuario puede tener activa cada vez una consola de terminal a través del puerto serie de la tarjeta del sistema o de la interfaz del módem PCMCIA. Si una estación de trabajo se conecta localmente al puerto serie y entra una llamada a través del módem PCMCIA, se da prioridad a la llamada. Después de la llamada, el usuario de la estación de trabajo local tendrá que volverse a conectar.

Definición y uso de Telnet

Utilice esta sección si va a definir el acceso a consola de terminal Telnet.

Telnet sólo proporciona acceso al código de operación principal (la interfaz de la línea de mandatos) y no a la interfaz de usuario de firmware. Si rearranca la unidad desde la interfaz de la línea de mandatos, perderá la conexión Telnet y necesitará volver a establecerla después de que se haya rearrancado la unidad.

Si la unidad no se ha configurado nunca, el único modo de poder ejecutar Telnet en ella es utilizando las direcciones IP PCMCIA EtherJet o SLIP.

Direcciones SLIP

Las direcciones IP SLIP por omisión para utilizar con los módems externos o PCMCIA son:

Para la estación de trabajo:
10.1.1.3

Para el Network Utility:
10.1.1.2

Para obtener instrucciones sobre cómo instalar SLIP, consulte la documentación de la versión del software de TCP/IP de PC.

Direcciones IP de LAN PCMCIA

Las direcciones IP por omisión que se utilizan con la tarjeta PCMCIA EtherJet de PC son las siguientes:

Para la estación de trabajo:
10.1.0.3

Para el Network Utility:
10.1.0.2

Puede cambiar estas direcciones desde la interfaz de la línea de mandatos del código de operación o desde el firmware. (Utilice los procedimientos descritos en el apartado “Configuración y operación básicas de IP” en la página 43). Primero deberá arrancar la consola de usuario inicial utilizando la emulación de terminal ASCII o ejecutando Telnet en las direcciones IP por omisión.

Direcciones IP de interfaz de red

No existen direcciones IP por omisión para las interfaces de red (de los adaptadores de las ranuras de adaptador). Utilice la interfaz de la línea de mandatos o el Programa de configuración para definir direcciones IP para las interfaces de red. Todas las tablas de configuración de ejemplo de la “Parte 3. Datos específicos de configuración y gestión” en la página 123 muestran cómo definir direcciones IP en las interfaces.No puede ejecutar Telnet a través de una interfaz de red hasta que active el cambio de configuración de dirección IP.

Además de asignar direcciones IP a una interfaz, puede asignar una dirección a la unidad entera. Esta dirección IP se conoce como la dirección IP *interna* y permanece activa independientemente del estado de las interfaces de red individuales.

Si tiene un Modelo TN1 y está utilizando la función de servidor TN3270, deberá configurar la dirección IP y el número de puerto TCP que el TN3270 deberá utilizar. Si acepta el número de puerto Telnet por omisión 23 para TN3270, deberá conectar las sesiones Telnet de consola a una dirección IP diferente de la que ha configurado para el servidor TN3270. Esto permite a la unidad distinguir las sesiones Telnet de consola de las sesiones de cliente TN3270.

Varios usuarios de Telnet

Dos usuarios pueden arrancar al mismo tiempo consolas Telnet a través de interfaces de red. Se rechazará el intento de arranque de Telnet de un tercer usuario hasta que uno de los dos primeros usuarios se haya desconectado. Sólo un usuario puede tener cada vez una consola activa a través del puerto de servicio de tarjeta del sistema o de las interfaces PCMCIA, incluyendo Telnet a través de SLIP o de la tarjeta PCMCIA de LAN.

Cómo llegar al indicador de mandatos

Después de haber definido la consola de usuario, busque los mensajes y vaya a uno de los indicadores de mandatos descritos aquí.

Qué debe ver

Si tiene una consola de usuario activa desde el momento en que enciende el Network Utility hasta que ésta presenta el primer indicador de mandatos, verá una secuencia de mensajes de estado informativos acerca de:

- Cómo salir para cambiar el tipo de terminal
- La inicialización de memoria
- Los diagnósticos de la placa del sistema
- Otros diagnósticos
- El proceso de arranque (incluyendo cómo interrumpir el arranque para alcanzar los menús de firmware)

- Cómo cargar el código de operación desde disco, terminando con los mensajes siguientes:

```
Please press the space bar to obtain the console.

Loading /hd0/sys0/LMX.ld from disk ...
Loading /hd0/sys0/LML.ld from disk ...
Loading /hd0/sys0/sysext.ld from disk ...
Loading /hd0/sys0/diags.ld from disk ...
Loading /hd0/sys0/snmp.ld from disk ...
Loading /hd0/sys0/router.ld from disk ...
Loading /hd0/sys0/appn.ld from disk ...
Loading /hd0/sys0/tn3270e.ld from disk ...

<pulse la barra espaciadora>
Console granted to this interface
Config (only)>
```

En cualquier momento después de ver la solicitud `Please press the space bar to obtain the console`, pulse la barra espaciadora para conectar el proceso de consola del Network Utility a la sesión. El sistema reconoce esta acción con el mensaje `Console granted to this interface` y visualizando un indicador de mandatos después de que se haya completado la carga de código.

Si está en un Network Utility que no se ha configurado nunca, el sistema presenta el indicador de mandatos `Config (only)>`. Entonces puede continuar como se describe en el Capítulo 3. Realización de la configuración inicial, para configurar el Network Utility. Si el Network Utility se ha configurado lo suficiente para que quede totalmente operativo, el sistema presenta el indicador de mandatos de asterisco (*).

Sólo un dispositivo ASCII conectado directamente podrá mostrarle todos los mensajes de la secuencia de arranque entera. Si está marcando a través del módem PCMCIA o ejecutando Telnet para arrancar la consola de usuario, el Network Utility necesita estar como mínimo parcialmente arrancado antes de poder responder al intento de conexión. Cuando realice la conexión, es probable que el proceso de arranque esté en una de sus últimas fases. El sistema le otorga la consola inmediatamente y, a continuación, le proporciona un indicador de mandatos al terminar el proceso de arranque.

Resolución de problemas de terminal ASCII

Los residuos, los caracteres aleatorios o la imposibilidad de conectar el terminal al puerto de servicio del Network Utility pueden tener diversas causas. La causa más común de los residuos o de los caracteres aleatorios es que la velocidad en baudios del terminal no está sincronizada con la del Network Utility.

El Network Utility está siempre establecido en una velocidad en baudios específica, que es por omisión 19,2 Kbps. El único modo de cambiar esta velocidad es a través del firmware, de modo que deberá tener una consola en funcionamiento para cambiarla. Si la consola es ilegible, pruebe diferentes valores de velocidad en baudios en el lado del terminal hasta que encuentre el que proporcione indicadores de mandatos o mensajes de estado legibles.

Otras causas de problemas de conexión incluyen:
- No hay ningún módem nulo en el cable serie
- Tomas de tierra de CA de Network Utility o terminal defectuosas
- Cable defectuoso, incorrectamente blindado o con toma de tierra incorrecta entre el terminal y el Network Utility.
- Terminal o emulador de terminal defectuoso

- Placa del sistema Network Utility defectuosa

Consulte el apartado ″Service Terminal Display Unreadable″ de la publicación *2216 Nways Multiaccess Connector and Network Utility Service and Maintenance Manual* para obtener más información sobre cómo manejar estos problemas.

Resolución de problemas de Telnet

El problema más común de Telnet es no lograr comunicarse con el Network Utility a través de la red IP. Puede utilizar las herramientas estándares de depuración (ping y traceroute) para determinar qué está sucediendo. Si está intentando ejecutar ping en la dirección IP interna del Network Utility, necesita definir en la estación de trabajo una ruta de sistema principal para dicha dirección, en la que el salto siguiente sea la dirección IP de interfaz a través de la cual entrará al Network Utility.

También puede intentar ejecutar ping desde el Network Utility a la estación de trabajo. El firmware proporciona un modo de efectuar dicha acción desde un puerto EtherJet o SLIP y el proceso de Consola del código de operación proporciona un modo de efectuarla desde las interfaces de red. Consulte el apartado “Configuración y operación básicas de IP” en la página 43 para ver un resumen de estos procedimientos.

Capítulo 3. Realización de la configuración inicial

Este capítulo introduce los conceptos básicos de la configuración del Network Utility y proporciona procedimientos específicos para configurar un nuevo Network Utility. Estos procedimientos llevan al Network Utility del estado pasivo en que espera ser configurado a un estado en que tiene interfaces de red y protocolos activos.

Antes de utilizar estos procedimientos, deberá conectar una consola de usuario como se describe en el “Capítulo 2. Arranque de una consola de usuario” en la página 15.

Conceptos básicos de configuración

Una configuración de Network Utility es un conjunto de elementos de datos que controlan cómo funciona el software, incluyendo elementos tales como:

- Qué interfaces deben activarse
- Qué enlaces deben arrancarse
- Qué protocolos y características deben dejarse activos
- Qué funciones de una característica o un protocolo determinado deben dejarse activas
- Qué nombres o direcciones de red deben utilizarse

Al arrancar un Network Utility, el sistema lee la información de configuración en un archivo del disco duro y activa las interfaces y los protocolos de acuerdo con la información de dicho archivo. El archivo se crea de uno de estos dos modos:

- Utilizando la interfaz de la línea de mandatos desde una consola de terminal de usuario

  Escriba mandatos para crear elementos de datos de configuración en la memoria y, a continuación, grabe la configuración en el disco duro del Network Utility.
- Utilizando un programa de configuración gráfico que se ejecute en una estación de trabajo autónoma

  Cree la configuración en la estación de trabajo y, a continuación, transfiérala al disco duro del Network Utility.

  El Programa de configuración del Network Utility se envía en un CD-ROM junto con cada Network Utility nuevo y también se puede bajar de la Web. Hay disponibles versiones para Windows 95, Windows NT, AIX y OS/2. Los requisitos de estación de trabajo se documentan en el manual *Guía del usuario del Programa de Configuración*, del que también se adjunta una copia impresa con el Network Utility.

Elección del método de configuración

Algunos usuarios de productos de direccionamiento de IBM prefieren el Programa de configuración, otros prefieren la interfaz de la línea de mandatos y otros utilizan una combinación de ambos métodos. Cada usuario puede elegir la propuesta que desee.

A continuación se indican algunos de los factores citados por los usuarios que están a favor del Programa de configuración:

- Permite el mantenimiento centralizado de los archivos de configuración para múltiples Network Utilities y 2216.

- Proporciona una organización intuitiva y orientada a tablas de los elementos de datos.
- Efectúa más validación de entrada y comprobación cruzada de parámetros que el método de la línea de mandatos.
- Incluye ayudas en línea individualizadas para diversos elementos.

A continuación se indican algunos de los factores citados por los usuarios que están a favor de la interfaz de la línea de mandatos:
- Proporciona un solo método integrado para la configuración, la reconfiguración dinámica y la supervisión.
- Está bien documentado en las publicaciones del producto y en los ″redbooks″ de IBM.
- Es simple realizar e intentar cambios rápidos de configuración.
- La definición de una consola de usuario no necesita tantos recursos de estación de trabajo o tanto tiempo como la instalación del Programa de configuración.

Cómo empezar desde la modalidad de sólo configuración

Si al arrancar un Network Utility ve el indicador de mandatos `Config (only)>` desde la consola de usuario, está en modalidad de sólo configuración. Un Network Utility arranca en modalidad de sólo configuración cuando el archivo de configuración actual del disco duro no tiene elementos de datos que le permitan realizar funciones útiles, por ejemplo reenviar paquetes de datos[3]. Necesitará configurar como mínimo un puerto de adaptador y un protocolo (por ejemplo, IP, DLSw o APPN) y rearrancar para que el Network Utility arranque en modalidad de trabajo normal.

Si su Network Utility está en la modalidad de `Config (only)>`, efectúe las acciones siguientes:

1. Elija si desea utilizar la línea de mandatos o el Programa de configuración para la configuración inicial. Es fácil cambiar de método más adelante, si desea probarlos ambos.
2. Basándose en su elección, siga uno de estos procedimientos:
   - “Procedimiento A: Procedimiento de la línea de mandatos para la configuración inicial”
   - “Procedimiento B: Configuración inicial del Programa de configuración” en la página 29

Procedimiento A: Procedimiento de la línea de mandatos para la configuración inicial

Utilice este procedimiento para configurar un Network Utility por primera vez, empezando desde el indicador de línea de mandatos `Config (only)>`:

Parte 1: Crear una configuración básica mínima

1. Utilice el mandato **add device** para configurar como mínimo una interfaz de red del modo siguiente:
   a. Escriba **add dev ?** para ver una lista de tipos de adaptador soportados.
   b. Escriba **add dev** *tipo*, donde *tipo* consta de las primeras letras de una fila de la lista de adaptadores. Por ejemplo, **add dev tok** selecciona el

3. Esto también sucede si la configuración está corrupta.

adaptador de Red en Anillo. Escriba suficientes letras para identificar de forma exclusiva el adaptador que desea.

c. Cuando se le solicite un número de ranura, entre **1** para la ranura de adaptador de la izquierda del Network Utility o **2** para la ranura de la derecha.

d. Si va a añadir un adaptador multipuerto, el sistema le solicitará el número de puerto de la interfaz que desea configurar. Los números de puerto de los adaptadores están fijados del modo siguiente:
   - Los puertos de los adaptadores multipuerto de LAN están numerados 1 y 2 y etiquetados en la cara del adaptador.
   - Los puertos de los adaptadores multipuerto de WAN están numerados a partir de 0 y están etiquetados en los conectores del cable de adaptador.

e. Entonces el sistema asigna un *número de interfaz* lógica, conocido también como *número de red*. Éste es el número clave que deberá utilizar para hacer referencia a esta interfaz en todos los demás mandatos del sistema. Por ejemplo, si desea suprimir la configuración de esta interfaz, escriba **delete interface** y, a continuación, el número de interfaz lógica.

f. Si es necesario, realice los ajustes siguientes en la configuración de dispositivo por omisión:

   Si ha añadido un puerto de Red en Anillo y desea que éste se ejecute a 16 Mbps en lugar del valor por omisión de 4 Mbps, escriba estos mandatos:

   net *número interfaz*
   speed 16
   exit

   Si ha añadido un puerto Ethernet de 10 Mbps (no 10/100) y desea utilizar el conector BNC (10BASE2) en lugar del conector por omisión RJ45 (10BASET), escriba estos mandatos:

   net *número interfaz*
   conn bnc
   exit

Repita el paso 1 para cada interfaz que desee configurar.

2. Si desea poder añadir interfaces de forma dinámica en el futuro sin necesidad de rearrancar el Network Utility, escriba **set spare** *número* desde el indicador `Config (only)>`, donde *número* es el número máximo de interfaces que necesita añadir sin rearrancar.

3. Utilice el mandato **qconfig** para iniciar el programa ″Quick Config″. Utilice este programa para configurar acceso IP y SNMP al Network Utility como se muestra más abajo.

   Quick Config es una característica del proceso de configuración de la línea de mandatos. En lugar de esperar a que escriba los mandatos, le hace preguntas y crea datos de configuración basándose en las respuestas. He aquí un ejemplo de pregunta de Quick Config:

   ```
   Configure Bridging? (Yes, No, Quit): [Yes]
   ```

   Los valores entre paréntesis son las respuestas posibles. El valor entre corchetes es la respuesta por omisión. Para aceptar el valor por omisión, pulse **Intro**.

   Responda del modo siguiente a las preguntas de Quick Config (algunas de ellas son respuestas por omisión):

   a. Configure puentes respondiendo **no** a `Configure Bridging?`

b. Configure protocolos respondiendo **yes** a `Configure Protocols?`

c. Configure IP del modo siguiente:

   1) Entre **yes** para `Configure IP?`

   2) Para las interfaces a las que desea asignar una dirección IP, responda **yes** a `Configure IP on this interface?` Si tiene la intención de utilizar la tarjeta PCMCIA EtherJet como interfaz IP única, responda **no** para cada interfaz de red configurada.

   3) Entre la dirección IP en el indicador `IP Address`.

   4) Entre la máscara IP en el indicador `Address Mask`.

   5) Si desea habilitar RIP o OSPF, responda **yes** a `Enable Dynamic Routing?` y responda las preguntas relacionadas subsiguientes.

   6) Si en algún momento desea enviar una configuración directamente desde el Programa de configuración a este Network Utility, responda **yes** a `Define Community with Read_Write_Trap Access?` y entre cualquier nombre de una sola palabra que desee como nombre de comunidad.

      Si no piensa utilizar el Programa de configuración nunca, responda **no**.

   7) Responda **yes** a `Save this configuration?` Esto guarda la parte IP de la configuración en la memoria.

d. Guarde el archivo de configuración respondiendo **yes** a `Do you want to write this configuration?`

Parte 2: Activar la nueva configuración

Ahora ya ha configurado al menos una interfaz y un protocolo (IP, con SNMP). Esta pequeña configuración es suficiente para salir de la modalidad de sólo configuración.

1. Desde el indicador de mandatos `Config (only)>`, escriba **reload** y responda **yes** a la solicitud de confirmación. El Network Utility rearranca y activa la nueva configuración.

   Si ve una solicitud que indica algo relativo a guardar los cambios de configuración, significa que ha efectuado cambios de configuración después de guardar el archivo de configuración cuando ha completado la Parte 1 de este procedimiento. Escriba **yes** para guardar dichos cambios como parte de la nueva configuración antes de que continúe el rearranque.

2. Verifique el rearranque del Network Utility.

   Si la consola de usuario está utilizando una conexión Telnet o de marcación, el rearranque le hará perder la conexión. Vuelva a conectarse al cabo de unos minutos. De lo contrario, simplemente observe los mensajes de arranque desde la consola.

   Cuando el rearranque se haya completado, la consola deberá visualizar el indicador de mandatos *, que indica que está en modalidad de operación normal y ya no está en modalidad de sólo configuración. Ahora, la configuración que ha creado en la Parte 1 de este procedimiento está activa.

Parte 3 - Añadir información de protocolo adicional

Ahora está en modalidad de operación normal con las interfaces que ha configurado, ejecutando IP solamente.

Si es usted un usuario nuevo y desea familiarizarse con el producto antes de configurar el resto de las funciones (por ejemplo TN3270 o DLSw), sáltese el resto de este procedimiento y consulte las directrices del apartado “Qué hacer a continuación” en la página 33.

Si desea configurar todas las funciones ahora inmediatamente, continúe aquí.

1. Seleccione en la “Parte 3. Datos específicos de configuración y gestión” en la página 123, el escenario de configuración más próximo al que desea para este Network Utility.
   - Usuarios del Modelo TN1 - Consulte el “Capítulo 12. Servidor TN3270E” en la página 133.
   - Usuarios del Modelo TX1 - Consulte el “Capítulo 14. Pasarela de canal” en la página 203, el “Capítulo 16. Conmutación de enlace de datos” en la página 237 o el “Capítulo 19. Redes privadas virtuales” en la página 275.

   Si ninguno de estos escenarios es adecuado, utilice las publicaciones *MAS Consulta de configuración y supervisión de protocolos*, *MAS Utilización y configuración de las características* y *MAS Guía del usuario de software* para determinar qué necesita configurar.
2. En el capítulo ″Detalles de configuración de ejemplo″ que sigue al escenario seleccionado, busque la tabla de parámetros de configuración que corresponde a dicho escenario[4]. Utilice la columna ″Mandatos de línea de mandatos″ para guiarse en la configuración de dicho escenario, cambiando los valores para los adaptadores y la red particulares.

   Si encuentra que tiene problemas al navegar por la línea de mandatos y al entrar los mandatos, es aconsejable que se familiarice más con la configuración general de la línea de mandatos antes de continuar. Consulte el apartado “Qué hacer a continuación” en la página 33 para obtener sugerencias respecto al modo de continuar.
3. Cuando haya terminado de entrar mandatos de configuración, repita los pasos de la “Parte 2: Activar la nueva configuración” en la página 28, pero emita el mandato **reload** desde el indicador * en lugar del indicador `Config (only)>`.

Procedimiento B: Configuración inicial del Programa de configuración

Utilice este procedimiento para configurar un Network Utility por primera vez utilizando el Programa de configuración del Network Utility.

Parte 1: Crear la configuración en el Programa de configuración

1. Desde el CD-ROM del Programa de configuración, instale la versión apropiada del Programa de configuración en la estación de trabajo.

   Para obtener instrucciones de instalación, consulte:
   - El archivo README del Network Utility en el CD-ROM.
   - La publicación *Guía del usuario del Programa de Configuración*, que se envía junto con el CD-ROM.

   Inicie el Programa de configuración. Si desea probar el programa realizando una nueva configuración a partir de cero, seleccione **New configuration** y **Network Utility** en la opción **Configure** de la barra de menús de la ventana de navegación (Navigation Window).

4. Si no existe ninguna tabla correspondiente, utilice para empezar la sección ″Claves para la configuración″ para dicho escenario.

2. Seleccione en la “Parte 3. Datos específicos de configuración y gestión” en la página 123 , el escenario de configuración que se parezca más al uso que le está dando a este Network Utility.
   - Usuarios del Modelo TN1 - Consulte el “Capítulo 12. Servidor TN3270E” en la página 133.
   - Usuarios del Modelo TX1 - Consulte el “Capítulo 14. Pasarela de canal” en la página 203, el “Capítulo 16. Conmutación de enlace de datos” en la página 237 o el “Capítulo 19. Redes privadas virtuales” en la página 275.

   Si ninguno de estos escenarios es adecuado, utilice los manuales *MAS Consulta de configuración y supervisión de protocolos*, *MAS Utilización y configuración de las características* y *MAS Guía del usuario de software* para determinar qué necesita configurar. Utilice cualquiera de las tablas de parámetros de configuración de la “Parte 3. Datos específicos de configuración y gestión” en la página 123 como ejemplo de correlación de mandatos de la línea de mandatos con los paneles del Programa de configuración. Cuando haya completado la configuración, salte al paso 7.
3. En el capítulo ″Detalles de configuración de ejemplo″ que sigue al escenario seleccionado, busque la tabla de parámetros de configuración que corresponde a dicho escenario.[4]
4. Desde el navegador Web, siga los enlaces `Support and Downloads` de la página web principal del Network Utility

   `http://www.networking.ibm.com/networkutility`,

   y busque el archivo de configuración de ejemplo que coincide con el escenario seleccionado. Baje este archivo en binario y transfiéralo a la estación de trabajo que ejecuta el Programa de configuración.
5. Seleccione **Open Configuration ...** en Navigation Window y seleccione la vía de acceso y el nombre del archivo de configuración de ejemplo que ha bajado.
6. Utilice las columnas ″Navegación de Programa de configuración″ y ″Valores de Programa de configuración″ de la tabla del paso 3 para guiarse al moverse por la configuración y al cambiar los valores para los adaptadores y la red particulares.
7. Cuando tenga una configuración lista para enviar al Network Utility, seleccione **Save configuration as ...** para guardar la configuración en la estación de trabajo. Es aconsejable elegir un nombre nuevo para poder dejar el archivo de configuración de ejemplo original sin modificarlo.

Parte 2: Transferir la configuración al Network Utility y activarla

Ahora ya ha creado la configuración inicial. Lo único que queda por hacer es transferir la configuración al disco duro del Network Utility y rearrancar el Network Utility para activarla. El modo de realizar dicha transferencia dependerá de la definición de conexión, como se indica a continuación:

- Si la estación de trabajo del Programa de configuración soporta TCP/IP y tiene conectividad física a la tarjeta PCMCIA EtherJet del Network Utility o a un adaptador de red de la ranura 1 o 2, utilice el Procedimiento A.
- Si la consola de usuario es a través de la emulación de terminal ASCII y prefiere utilizar el Xmodem para definir la conectividad IP anterior, utilice el Procedimiento B.

También puede consultar el apartado “Carga de archivos de configuración nuevos” en la página 84 para obtener una lista completa de los modos de transferir una configuración al Network Utility. Necesitará software de servidor TFTP en una

estación de trabajo TCP/IP si elige no seguir el Procedimiento A o B.

Procedimiento A: Transferencia directa mediante una tarjeta PCMCIA EtherJet de Network Utility o un adaptador de red

Utilice este procedimiento si la estación de trabajo del Programa de configuración soporta TCP/IP y tiene conectividad física a la tarjeta PCMCIA EtherJet del Network Utility o a un adaptador de red en la ranura 1 ó 2.

1. Configure el Network Utility rápidamente desde la línea de mandatos, para que tenga una dirección IP en una interfaz como mínimo e IP y SNMP habilitados.
   a. Desde la consola de usuario, realice los pasos de la “Parte 1: Crear una configuración básica mínima” en la página 26. Asegúrese de:
      1) Utilizar **add device** para definir como mínimo una interfaz en la ranura 1 ó 2
      2) En Quick Config, responda **yes** a `Define Community with Read_Write_Trap Access?`
   b. En el Programa de configuración, verifique si la configuración que está a punto de enviar tiene habilitado SNMP y tiene el mismo nombre de comunidad definido con acceso ″read-write trap″. Esto es necesario para que después de activar la configuración, pueda repetir el paso 3 de este procedimiento para enviar otra configuración.
   c. Realice los pasos de la “Parte 2: Activar la nueva configuración” en la página 28 para rearrancar el Network Utility y activar esta configuración de línea de mandatos temporal.
2. Si piensa utilizar la tarjeta PCMCIA, defina sus direcciones IP del modo siguiente después de que se haya completado el rearranque del Network Utility:

   Desde el indicador *, escriba **talk 6**. Desde el indicador `Config>`, escriba **system set ip** y entre los valores siguientes cuando se le soliciten:
   - Dirección IP: dirección IP que desea utilizar para la tarjeta EtherJet
   - Máscara de red: máscara para la subred conectada a la tarjeta EtherJet
   - Dirección de pasarela: dirección IP para la estación de trabajo del Programa de configuración o dirección IP de un direccionador a través del cual se puede alcanzar el Network Utility

   Junto a cada indicador, el sistema muestra el valor actual como valor por omisión. Para aceptar el valor por omisión, pulse **Intro**. Después de entrar todos los valores, cualquier cambio de dirección especificado entrará en vigor inmediatamente. Los valores se almacenan en la NVRAM del Network Utility y no como parte de un archivo de configuración.
3. Envíe la configuración desde el Programa de configuración (utilizando SNMP):
   a. En el menú desplegable **Configure**, seleccione **Communications** y **Single router**.
   b. En el panel Communicate, entre:
      - Dirección IP o nombre: Dirección IP de la interfaz del Network Utility a través de la cual desea enviar la configuración. Se trata de la dirección IP PCMCIA EtherJet o la dirección IP de interfaz de red que ha asignado en Quick Config.
      - Comunidad: Nombre de comunidad asignado en Quick Config.
   c. Seleccione **Send configuration** y **Restart router**. Acepte o entre la fecha y hora actual, para que el Network Utility rearranque con la nueva configuración inmediatamente después de recibirla.
   d. Pulse en **OK**. El Programa de configuración empieza inmediatamente a enviar elementos de datos de configuración a los direccionadores especificados utilizando SNMP.

El Programa de configuración proporciona mensajes de estado y resultado acerca de la transferencia. Si falla la operación de envío, el Programa de configuración lista las posibles razones que, a continuación, se deberán verificar y corregir.

Después de que el Programa de configuración haya completado la transferencia de configuración, el Network Utility almacena la configuración en disco y se rearranca a sí mismo como se ha indicado.

4. Verifique el rearranque del Network Utility

   Si la consola es a través de una conexión Telnet o de marcación, el rearranque hará que se pierda la conexión. Vuelva a conectarse al cabo de unos minutos. De lo contrario, simplemente observe los mensajes de arranque desde la consola de usuario.

   Cuando el rearranque se haya completado, la consola deberá visualizar el indicador de mandatos *, que indica que está en modalidad de operación normal y ya no está en modalidad de sólo configuración. Ahora, la configuración que ha creado en la Parte 1 de este procedimiento está activa.

Procedimiento B: Transferencia de Xmodem indirecta a través de sesión de consola de usuario

Utilice este procedimiento si la consola es a través de la emulación de terminal ASCII y prefiere utilizar el Xmodem para definir la conectividad IP desde la estación de trabajo del Programa de configuración.

1. Desde el Programa de configuración, exporte la configuración en el formato de archivo que el Network Utility comprenda

   En el menú desplegable **Configure**, seleccione **Create router configuration** y especifique la vía de acceso y el nombre para un archivo .CFG. Pulse en **OK** para grabar el archivo.

2. Si es necesario, transfiera el archivo .CFG de la estación de trabajo del Programa de configuración a la estación de trabajo de emulación de terminal.
3. Desde la consola en el indicador `Config (only)>`, siga esta secuencia:

```
Config (only)>boot
Boot configuration
Boot config>dis auto
Select the duration to disable autoboot: (once, always): [always] once
AutoBoot mode is now disabled once.

Operation completed successfully.
Boot config>exit
Config (only)>rel y
```

   Si se le solicita si desea guardar los cambios de configuración, responda **no**. El Network Utility rearranca y se detiene en el menú de firmware.

   Si la consola es a través de una conexión de marcación, el rearranque le hará perder la conexión. Vuelva a conectarse al cabo de unos minutos y verá el menú de firmware.

4. Efectúe la secuencia siguiente de selecciones de menú de firmware:
   a. System Management Services (menú principal): Opción 4, **Utilities**
   b. System Management Utilities: Opción 12, **Change Management**
   c. Change Management Software Control: Opción 12, **Xmodem software**
   d. Select Type: **Config**
   e. Select Bank: elija **Bank A** (banco activo)

f. Select Config: elija la posición **1**[5]

El firmware le indica cuándo debe iniciar la transferencia de archivos.

5. Vaya al paquete de emulación de terminal e inicie la transferencia del archivo desde el servidor de estación de trabajo, utilizando el nombre que desee. Cuando el Network Utility haya recibido el archivo de configuración, el estado de la posición de archivo cambiará de CORRUPT a AVAIL. Puede verificar que ha sucedido lo indicado utilizando la opción 7, **List Software**, en el menú Change Management de firmware.
6. Arranque el Network Utility utilizando la configuración que acaba de cargar.
   a. Utilice la Opción 9 **Set Boot Information** para seleccionar el banco de código de operación actual y la nueva configuración.
   b. Pulse **Esc** para alcanzar el menú principal y, a continuación, **F9** (Iniciar el OS) para arrancar el Network Utility con la nueva configuración.
7. Verifique el arranque del Network Utility

   Si la consola es a través de una conexión de marcación, no perderá la conexión al utilizar la opción Iniciar el OS. Observe los mensajes de arranque desde la consola.

   Cuando el arranque se haya completado, la consola deberá visualizar el indicador de mandatos *, que indica que está en modalidad de operación normal y ya no está en modalidad de sólo configuración. Ahora, la configuración que ha creado en la Parte 1 de este procedimiento está activa.

Qué hacer a continuación

Si ha seguido los procedimientos de este capítulo, ahora el Network Utility está en plena modalidad de operación con una configuración que ha creado. Con la consola de usuario en el indicador *, se encuentra ahora en posición de utilizar la interfaz de la línea de mandatos para:

- Consultar el estado de las interfaces y los protocolos
- Activar sucesos y supervisar la anotación cronológica de sucesos
- Emitir mandatos de operador para efectuar cambios de estado
- Realizar cambios de configuración dinámicos sin rearrancar

Éstas son las herramientas básicas para ver si la nueva configuración funciona correctamente y para efectuar pequeños ajustes en dicha configuración.

Si la interfaz de la línea de mandatos es nueva para usted, puede utilizar el “Capítulo 5. Recorrido por la interfaz de la línea de mandatos” en la página 53 para familiarizarse con sus conceptos y con el modo de utilizarla.

Si tiene experiencia previa con productos de direccionamiento de IBM o prefiere probar tareas sin seguir una guía, puede utilizar el “Capítulo 4. Consulta rápida a la interfaz de usuario” en la página 35 como información de resumen acerca de la navegación en la línea de mandatos y algunas tareas comunes.

Puede utilizar los Capítulos 6 a 10 para obtener más información básica sobre:

- La gestión de archivos de configuración
- La reconfiguración dinámica

5. Esta selección de posición de banco y archivo de configuración supone que ésta es la primera vez que ha arrancado este Network Utility. Para obtener más información básica sobre este tema, consulte el apartado “Archivos de configuración en disco” en la página 74.

- Cómo gestionar lo que está haciendo el Network Utility, localmente y utilizando productos de gestión de red remota
- La actualización de software y firmware
- La solicitud de servicio y soporte

Puede que ya haya utilizado la información de configuración de ejemplo de la “Parte 3. Datos específicos de configuración y gestión” en la página 123. Los capítulos de dicha parte también contienen información de introducción sobre la configuración y supervisión de las funciones:
- Servidor TN3270E
- Pasarela de canal
- Conmutación de enlace de datos
- Red privada virtual

Si ya ha configurado una de estas funciones en la configuración inicial, utilice la sección de ″Gestión″ del capítulo correspondiente para empezar a supervisar y depurar dicha configuración.

Capítulo 4. Consulta rápida a la interfaz de usuario

Este capítulo contiene información de resumen acerca de la navegación por la interfaz de la línea de mandatos, la entrada de mandatos y la realización de tareas comunes. Para obtener una explicación completa de este material con ejemplos, consulte el “Capítulo 5. Recorrido por la interfaz de la línea de mandatos” en la página 53.

Navegación

La interfaz de la línea de mandatos consta de un árbol de menús cuya raíz es el indicador asterisco (*). El usuario escribe mandatos y utiliza teclas de control para moverse a diversos lugares del árbol y luego escribe mandatos para efectuar realmente las tareas.

Procesos e indicadores

Desde el indicador *, utilice el mandato **talk** (**t** abreviado) para conectarse a uno de diversos procesos o modos de ver el sistema. Cada proceso desde el que entra mandatos se identifica por un indicador de mandatos diferente.

Tabla 5. Procesos clave

Nombre	Mandato para acceder	Finalidad	Indicador de nivel superior
Config	**t 6** o **config**	Ver y modificar la configuración	`Config>`
Console	**t 5** o **console**	Ver y controlar el estado en ejecución, efectuar cambios dinámicos de configuración	+ (signo más)
Monitor	**t 2** o **event**	Ver la anotación cronológica de mensajes de sucesos en tiempo real	(ninguno)

Escriba **t *n*** y, a continuación pulse **Intro** dos veces para obtener el indicador de mandatos. Escriba **Control-p** para volver al indicador * desde dentro de cualquier proceso.

El proceso de supervisión (Monitor) no tiene ningún indicador de mandatos porque en lugar de emitir mandatos en dicho proceso, se observa una anotación cronológica de mensajes de sucesos en ejecución. Puede escribir **Control-s** para hacer una pausa en el desplazamiento y **Control-q** para reanudarlo.

Subprocesos

Cuando se está trabajando dentro de los procesos talk 6 o talk 5, algunos mandatos cambian el indicador de entrada y proporcionan un nuevo menú de mandatos que es específico de un área funcional. Por ejemplo,

- Si escribe **protocol dlsw** bajo talk 6 irá al subproceso Config para configurar la Conmutación de enlace de datos. El indicador de mandatos se convierte en `DLSw config>`.
- Si escribe **perf** bajo talk 5, irá al subproceso Console para ver estadísticas de utilización de CPU. El indicador de mandatos se convierte en `PERF Console>`.

También se puede mover de un subproceso a otro subproceso. Por ejemplo, si escribe **ban** desde el subproceso DLSw Config, irá al subproceso Boundary Access Node Config. Ha ido a un nivel más profundo de anidamiento en el sistema de menús; deberá volver a través del subproceso DLSw.

Se aplican las normas de navegación siguientes:

- Para entrar en un subproceso, escriba el mandato específico que le lleva allí. Escriba **?** en cualquier menú para ver los mandatos disponibles. Sabrá que ha entrado en un subproceso cuando cambie el indicador de mandatos.
- Para salir de cualquier subproceso y volver al menú del siguiente nivel superior, escriba **exit**.
- Para salir de cualquier subproceso e ir inmediatamente al indicador *, escriba **Control-p**. Esto también le hace salir del proceso actual.
- Para reanudar un subproceso después de haber escrito **Control-p**, escriba **t** *n* (donde *n* es el número de proceso del que ha salido), y a continuación pulse **Intro** dos veces. Reanudará dicho proceso en el subproceso donde ha escrito **Control-p**.

Entrada de mandatos

Para entrar en los procesos, entrar y salir de los subprocesos y realizar tareas se escriben mandatos. Algunos mandatos de tarea le solicitan valores de parámetro, mientras que otros no necesitan ninguna entrada distinta del nombre de mandato.

Formación de mandatos

Un mandato es una secuencia de una o más palabras clave, opcionalmente seguidas de valores de parámetros que se han escrito en la línea de mandatos original. Para formar un mandato se aplican las directrices siguientes:

- Debe escribir un mandato completo antes de que el sistema realice la acción o le solicite parámetros de entrada. Si sólo escribe parte de un mandato válido (no suficientes palabras clave), el sistema responde con `Command not fully specified`.
- Puede escribir **?** en cualquier indicador de proceso o subproceso o después de cualquier mandato incompleto, para ver un menú de palabras clave de mandato disponibles desde dicho punto. Puede utilizar este signo para buscar o completar un mandato, como se muestra en este ejemplo abreviado:

```
Config>?
ADD (device, user)
BOOT and load file functions
CHANGE (device, password, user)
  ...             < otros mandatos no mostrados>
Config>add
Command not fully specified
Config>add ?
DEVICE
NAMED-PROFILE
PPP-USER
TUNNEL-PROFILE
USER
Config>add user
Enter user name:  []?  <intro>
No user was added
Config>
```

En el ejemplo, **add** no era un mandato completo, pero **add user** sí lo es. Después de que el usuario ha escrito el mandato completo, el sistema le solicita un valor de parámetro de entrada.

- Puede abreviar la mayoría de las palabras clave de mandato al número mínimo de caracteres que las seleccionen de forma exclusiva en el menú en el que aparecen. Por ejemplo, puede escribir **t 6** en lugar de **talk 6** y **p appn** en lugar de **protocol appn**. En el ejemplo anterior, el usuario podría haber escrito **a u** en lugar de **add user**.
- Puede trabajar con mandatos entrados previamente en talk 6 y talk 5 utilizando las claves siguientes:

  Control-B
  para desplazarse atrás por mandatos entrados anteriormente

  Control-F
  para desplazarse adelante por la lista de mandatos entrados anteriormente

  Control-U
  para borrar un mandato recuperado de la línea de mandatos

  Retroceso
  para editar un mandato recuperado empezando desde el final

  talk 6 y talk 5 comparten el almacenamiento intermedio del histórico de mandatos.

Terminación automática de mandatos

A partir de MAS V3.3, el Network Utility puede ayudarle a formar mandatos completando automáticamente palabras clave que usted escribe y mostrándole opciones de menú disponibles. Configure esta función de terminación de mandatos para que esté inhabilitada o habilitada, en la línea de mandatos o desde el Programa de configuración. La terminación de mandatos está habilitada por omisión al iniciar una configuración nueva de MAS V3.3, pero si actualiza una configuración existente, esta función está inhabilitada por omisión. Se recomienda a los usuarios nuevos que ejecuten con la terminación de mandatos habilitada (escriba **enable command** desde el indicador **Config (only)>** o **Config>**).

Para ilustrar el comportamiento de la terminación de mandatos, suponga que se permiten los mandatos siguientes en un contexto de menú determinado. (Esto sólo es un menú de ejemplo).

enable	auto-refresh
	caching
set	cache-size
	cache-timeout
	priority

- Si escribe **ena** y pulsa la barra espaciadora, el mandato completo se muestra como **ENABLE**. Si ahora escribe **?**, se muestra una lista de elementos posibles (**auto-refresh** y **caching**) y el mandato **ENABLE** permanece en la línea de mandatos.

- Si escribe **ena** y pulsa **Intro**, se imprime un mensaje indicando que el mandato no se ha especificado completamente, se muestra una lista de posibles elementos a habilitar (**auto-refresh** y **caching**) y el mandato **ENABLE** permanece en la línea de mandatos.
- Dado que el mandato **ENABLE** necesita que se habilite un elemento, aparecerá en una lista de posibles terminaciones de mandato con "..." en el margen izquierdo para indicar que se necesita más entrada para el mandato.
- Si la entrada coincide con varios mandatos, se visualiza una lista de posibles terminaciones. La entrada en la nueva línea de mandatos se expande al prefijo común más largo. Por ejemplo, si entra **set ca** y luego pulsa la barra espaciadora, se listarán **CACHE-SIZE** y **CACHE-TIMEOUT** y la nueva línea de mandatos se expandirá a **SET cache-**, dado que "cache-" es común a las dos terminaciones posibles. Ahora debe escribir la letra "s" o la letra "t" para distinguir entre las posibles terminaciones ″size″ o ″timeout″.
- Los mandatos comunes aparecen a veces en una forma alternativa (**SHOW**, **DISPLAY**, **LIST**). Si la terminación de mandatos no produce una coincidencia en un mandato común, por ejemplo **SHOW**, se visualizarán las alternativas **DISPLAY** o **LIST**, si se encuentran.
- Si la búsqueda de un mandato (y alternativas) no produce una coincidencia exacta, aparecerá una lista de terminaciones posibles, que utilizan una parte de la entrada. Por ejemplo, **enable** seguido de la barra espaciadora se sustituiría por **ena** y se listaría **ENABLE** como la posible terminación.
- Cuando se muestra una lista de mandatos posibles, puede utilizar la tecla de tabulador para pasar los mandatos de uno en uno en la línea de mandatos actual. Puede utilizar la barra espaciadora o la tecla Intro para seleccionar el mandato mostrado.

Para obtener ayuda en línea completa para la función de Terminación de mandatos, escriba **<esc> ?** desde cualquier indicador de mandatos.

Entrada de valores de parámetros de mandatos

Algunos de los mandatos que efectúan una tarea necesitan que se proporcionen valores para los parámetros de entrada. Puede dejar que el sistema le solicite estos valores de entrada o (en la mayoría de los casos) escribirlo anticipadamente en la línea de mandatos a continuación del nombre de mandato.

Si no escribe valores de parámetros anticipadamente:

- Escriba sólo el nombre de mandatos y pulse **Intro**.
- El sistema le solicita cada parámetro uno tras otro, proporcionando el valor por omisión para dicho parámetro entre corchetes. Algunos valores por omisión son fijos, pero la mayoría son el último valor que se ha asignado a dicho parámetro en particular.
  - Para aceptar el valor por omisión, pulse **Intro**
  - Para proporcionar un valor nuevo, escriba el valor y pulse **Intro**
  - Si los corchetes son adyacentes, como en [], no existe ningún valor por omisión y será necesario que proporcione un valor

  El sistema efectúa una comprobación de validez en la respuesta antes de solicitarle el siguiente valor.
- Cuando haya respondido a la última solicitud de parámetro, el sistema realizará la acción especificada por el mandato.

Si desea escribir los valores de los parámetros anticipadamente:

- Escriba el nombre de mandato seguido de uno o más valores de parámetros separados por espacios en blanco y, a continuación, pulse **Intro**.
- El sistema analiza la línea de mandatos y proporciona el primer valor al primer parámetro, el segundo valor al segundo parámetros, y así sucesivamente. Deberá proporcionar los valores en el orden esperado.

  El sistema efectúa una comprobación de validez a medida que asigna cada valor al parámetro correspondiente.
- Si el mandato necesita más parámetros que aquéllos para los que ha proporcionado valores, el sistema le solicitará los valores adicionales como se ha indicado más arriba.
- Cuando el sistema ha proporcionado un valor válido a cada parámetro, realiza la acción especificada por el mandato.

La acción de escribir los valores anticipadamente puede ser un método abreviado cómodo para los usuarios con experiencia. Deberá tener cuidado de proporcionar parámetros válidos en el orden correcto.

Tendrá que estar alerta en los casos en que escribe **?** a continuación de un mandato completo y el mandato trata el ″?″ como un valor escrito anticipadamente para su primer parámetro de entrada. Si sucede esto, termine anormalmente o deshaga el mandato e inténtelo de nuevo.

Mensajes de error comunes

La Tabla 6 explica varios mensajes de error estándares de la interfaz de la línea de mandatos:

Tabla 6. Mensajes de error y acciones correctivas

Mensaje de error	Explicación y acción correctiva
`Command error (Error de mandato)`	El mandato que ha escrito no existe en el menú actual. Puede que se trate de un error tipográfico, que esté en el lugar incorrecto para emitir este mandato o que no haya escrito suficientes caracteres para identificar el mandato del menú. Observe el indicador para verificar dónde está y escriba **?** para ver los mandatos disponibles. Corrija el mandato o vaya al lugar correcto.
`Command not fully specified (Mandato no especificado totalmente)`	Las palabras clave de mandato que ha escrito no forman un mandato completo. Pulse **Control-b** para recuperar el mandato y, a continuación, añada ″ **?**″ al final del mismo para ver las opciones para la siguiente palabra clave. Seleccione la siguiente palabra clave a añadir y vuelva a emitir el mandato sustituyendo **?** por dicha palabra clave. Es aconsejable también que consulte el manual de consulta de la línea de mandatos MAS apropiado para ver el mandato que está intentando entrar.
`Command syntax error (Error de sintaxis de mandato)`	Ha escrito un formato incorrecto de un mandato válido. Puede que haya proporcionado un parámetro no válido o inesperado. Pruebe el mandato otra vez sin ningún valor de parámetro o consulte la entrada del manual de consulta de la línea de mandatos MAS apropiado.

Tabla 6. Mensajes de error y acciones correctivas (continuación)

Mensaje de error	Explicación y acción correctiva
`Feature <name> available but not enabled (Característica <nombre> disponible pero no habilitada)`	Bajo talk 5, ha intentado entrar en el subproceso Console para una característica que se soporta en la carga de software pero que no está ejecutándose de forma activa. La configuración actual no ha habilitado la característica o en dicha configuración faltan valores clave necesarios para activar la característica. Si está utilizando el Programa de configuración, busque en el panel de navegación los **?**, que indican que no se han establecido los parámetros necesarios. Haga un seguimiento de los **?** en el panel o paneles con nombres de campos en rojo que no se han establecido. Si está efectuando la configuración desde la línea de mandatos, consulte las configuraciones de ejemplo en este manual y en el capítulo para esta característica del manual de consulta de MAS. Busque los parámetros clave que se muestran como parámetros básicos para habilitar la función.
`Protocol <name> available but not configured (Protocolo <nombre> disponible pero no configurado)`	Lo mismo que se ha descrito más arriba para `Feature available but not enabled`, pero aplicado a un protocolo.

Tareas clave de usuario

Esta sección organiza las tareas de usuario comunes en grupos y proporciona tablas con una consulta rápida a los mandatos para efectuar cada tarea.

Configuración de interfaces y adaptadores físicos

La Tabla 7 describe cómo efectuar tareas relacionadas con la configuración de interfaces y adaptadores físicos.

Tabla 7. Cómo configurar interfaces y adaptadores físicos

Tarea	Cómo llevarla a cabo
Añadir una interfaz en la configuración inicial	1. Desde el indicador *, escriba **talk 6** y pulse **Intro** dos veces para obtener el indicador `Config>`. 2. Escriba **add dev ?** para ver una lista de tipos de adaptador soportados. 3. Escriba **add dev** *tipo*, donde *tipo* es la palabra clave de la lista para el tipo de adaptador que desea. 4. Entre la ranura física y el número de puerto (si se le solicita) de la interfaz que está configurando. Las ranuras son 1 y 2 de izquierda a derecha. Los puertos LAN están numerados en la cara de adaptador y los puertos WAN están numerados en los conectores de cable. 5. Anote el nuevo número de interfaz lógica (red) que el Network Utility asigna a esta interfaz. 6. Escriba **net** *número interfaz lógica* para entrar en el subproceso Config para el tipo de interfaz en particular. Utilice los mandatos en dicho subproceso para verificar o cambiar los valores por omisión para la interfaz. 7. Escriba **exit** para volver al indicador `Config>`. 8. Escriba **write** para guardar esta configuración y luego **reload** seguido de **yes** para rearrancar con ella.

Tabla 7. Cómo configurar interfaces y adaptadores físicos (continuación)

Tarea	Cómo llevarla a cabo
Habilitar la adición dinámica de interfaces después de la configuración inicial	Antes de poder añadir una interfaz dinámicamente, la configuración de Network Utility activa debe tener definidas ″interfaces de repuesto″. 1. Desde el indicador *, escriba **talk 6** y pulse **Intro** dos veces para obtener el indicador `Config>`. 2. Escriba **set spare** y entre el número de interfaces de repuesto que desea. 3. Escriba **write** para guardar esta configuración y luego **reload** seguido de **yes** para rearrancar con ella.
Añadir una interfaz dinámicamente después de la configuración inicial	1. Verifique si tiene interfaces de repuesto activas: a. Desde el indicador *, escriba **talk 5** y pulse **Intro** dos veces para obtener el indicador +. b. Escriba **int** y verifique si tiene interfaces NULL. c. Escriba **Control-p** para volver al indicador *. Si no tiene ninguna interfaz de repuesto, deberá seguir el procedimiento anterior para añadir alguna a la configuración y rearrancar. 2. Desde el indicador *, escriba **talk 6** y pulse **Intro** dos veces para obtener el indicador `Config>`. 3. Utilice los mandatos **add dev** y **net** para configurar una nueva interfaz, como se describe en los procedimientos de configuración inicial. Anote el nuevo número de interfaz lógica asignado por el mandato **add dev**. 4. Utilice los mandatos **protocol** y **feature** para ir a los subprocesos Config y configurar información de protocolo relacionada con la nueva interfaz. 5. Escriba **Control-p**, **talk 5** y pulse **Intro** dos veces para obtener el indicador +. 6. Escriba **activate int** y proporcione el nuevo número de interfaz lógica. El sistema activa la nueva interfaz dinámicamente. 7. Si desea guardar la nueva configuración de interfaz para que sobreviva un rearranque, vuelva a talk 6 y escriba **write** para grabar la configuración modificada en disco. O efectúe los cambios correspondientes en el Programa de configuración y baje la configuración revisada al Network Utility.

Tabla 7. Cómo configurar interfaces y adaptadores físicos (continuación)

Tarea	Cómo llevarla a cabo
Cambiar dinámicamente la configuración de interfaz	1. Desde el indicador *, escriba **talk 6** y pulse **Intro** dos veces para obtener el indicador `Config>`. 2. Escriba **list dev** para ver el número de interfaz lógica para la interfaz que desea cambiar. 3. Escriba **net** *número interfaz lógica* para entrar en el subproceso Config para el tipo de interfaz específico. Entre mandatos para cambiar la configuración de la interfaz. Escriba **exit** para volver al indicador Config>. 4. Utilice los mandatos **protocol** y **feature** para obtener los subprocesos Config de protocolo y característica. Entre mandatos para cambiar parámetros relacionados con la interfaz. 5. Escriba **Control-p**, a continuación **talk 5** y pulse **Intro** dos veces para obtener el indicador +. 6. Escriba **reset** y entre el número lógico de la interfaz que acaba de reconfigurar. El Network Utility detiene la interfaz y la vuelve a arrancar utilizando la configuración modificada. 7. Si desea guardar estos cambios de configuración para que sobrevivan a un rearranque, vuelva a talk 6 y escriba **write** para grabar la configuración modificada en disco. O efectúe los cambios correspondientes en el Programa de configuración y baje la configuración revisada al Network Utility.

Gestión de interfaces y adaptadores físicos

La Tabla 8 describe cómo efectuar tareas relacionadas con la gestión de interfaces y adaptadores físicos.

Tabla 8. Cómo gestionar interfaces y adaptadores físicos

Tarea	Cómo llevarla a cabo
Consultar el estado de una interfaz	1. Desde el indicador *, escriba **talk 5** y pulse **Intro** dos veces para obtener el indicador +. 2. Escriba **config** para ver información acerca del software y, al final, el estado actual de todas las interfaces. Si la salida de pantalla se detiene visualizando `--More--`, pulse la barra espaciadora para ver la siguiente pantalla de salida. 3. Escriba **int** para ver los números de ranura y puerto y las cuentas de activación para las interfaces. 4. Escriba **stat** para ver estadísticas de paquete y bytes para interfaces. 5. Escriba **err** para ver cuentas de errores para las interfaces. 6. Escriba **queue** y **buff** para ver las cuentas de almacenamiento intermedio para las interfaces. 7. Escriba **net** *número interfaz lógica* para entrar en el subproceso Console para el tipo de interfaz específico. Utilice los mandatos de dicho subproceso para visualizar información de estado de interfaz específica del tipo.

Tabla 8. Cómo gestionar interfaces y adaptadores físicos (continuación)

Tarea	Cómo llevarla a cabo
Reciclar (inhabilitar/habilitar) una interfaz	1. Desde el indicador *, escriba **talk 5** y pulse **Intro** dos veces para obtener el indicador +. 2. Escriba **int** para ver el número lógico de ″red″ para la interfaz que desea reciclar. 3. Escriba **disable int** *número interfaz lógica* para dejar a la interfaz fuera de línea de forma dinámica. 4. Escriba **test** *número interfaz lógica* para volver a arrancar la interfaz.
Reciclar (inhabilitar/habilitar) un adaptador	**Nota**: Si tiene la intención de quitar el adaptador mientras está inhabilitado (el procedimiento ″enchufe en caliente″ estándar), también deberá consultar el capítulo ″Removal and Replacement Procedures″ de la publicación *2216 Nways Multiaccess Connector and Network Utility Service and Maintenance Manual*. 1. Desde el indicador *, escriba **talk 5** y pulse **Intro** dos veces para obtener el indicador +. 2. Escriba **disable slot** *número ranura*, donde 1 es la ranura de la izquierda y 2 es la ranura de la derecha. Esto inhabilita todas las interfaces en el adaptador de dicha ranura. 3. Escriba **enable slot** *número ranura* para activar todas las interfaces en el adaptador de dicha ranura.

Configuración y operación básicas de IP

La Tabla 9 describe tareas básicas de configuración y operación para interfaces y adaptadores IP.

Tabla 9. Configuración y operación básicas de IP

Tarea	Cómo llevarla a cabo
Añadir una dirección IP a un adaptador de red	1. Desde el indicador *, escriba **talk 6** y pulse **Intro** dos veces para obtener el indicador `Config>`. 2. Escriba **prot ip** para obtener el subproceso Config de IP. 3. Escriba **li addr** para ver direcciones IP configuradas actualmente. 4. Escriba **add addr** para añadir una dirección IP. Proporcione el número de interfaz lógica (red) de la interfaz, la dirección IP y la máscara de dirección. 5. Si desea activar éste y otros cambios de configuración de IP en el Network Utility en ejecución: a. Escriba **Control-p**, a continuación **talk 5** y pulse **Intro** dos veces para obtener el indicador +. b. Escriba **prot ip** para obtener el subproceso Console de IP. c. Escriba **int** para ver direcciones IP de interfaz actualmente activas. d. Escriba **reset ip** para activar la nueva dirección. e. Escriba **int** para verificar la nueva dirección.

Tabla 9. Configuración y operación básicas de IP (continuación)

Tarea	Cómo llevarla a cabo
Establecer la dirección IP del adaptador PCMCIA EtherJet	1. Desde el indicador *, escriba **talk 6** y pulse **Intro** dos veces para obtener el indicador `Config>`. 2. Escriba **system set ip** y proporcione la información siguiente (los valores por omisión son los valores actuales de estos parámetros): • Dirección IP - dirección a utilizar para el adaptador EtherJet • Máscara de red IP - máscara de red para dicha dirección • Dirección de pasarela IP - dirección de la estación de trabajo IP con la que probablemente se comunicará o el direccionador que utiliza para comunicarse con dicha estación de trabajo. Los cambios efectuados entran en vigor inmediatamente y se almacenan la memoria no volátil del Network Utility. Estas direcciones no forman parte de la configuración del Network Utility. También puede establecer la dirección IP EtherJet del firmware. Siga el procedimiento más abajo para EtherJet Ping, pero seleccione la opción 1 **IP Parameters**, en lugar de la opción 3 **Ping**.
Añadir una ruta estática	1. Desde el indicador *, escriba **talk 6** y pulse **Intro** dos veces para obtener el indicador `Config>`. 2. Escriba **prot ip** para obtener el subproceso Config de IP. 3. Escriba **li route** para ver las rutas configuradas actualmente. 4. Escriba **add route** para añadir una ruta estática. Proporcione la información solicitada.
Ping y traceroute desde un adaptador de red	1. Desde el indicador *, escriba **talk 5** y pulse **Intro** dos veces para obtener el indicador +. 2. Escriba **prot ip** para obtener el subproceso Console de IP. 3. Para hacer ping en una dirección con parámetros por omisión, escriba **ping** *dirección ip*. Para modificar parámetros, escriba sólo **ping** y responda a las solicitudes. Escriba **Control-c** para finalizar el ping. 4. Para rastrear la ruta a una dirección con parámetros por omisión, escriba **trace** *dirección ip*. Para modificar parámetros, escriba sólo **trace** y responda a las solicitudes. Escriba **Control-c** par< finalizar el traceroute.
Ping desde el adaptador PCMCIA EtherJet	1. Utilice uno de los procedimientos del apartado “Opciones de arranque: Arranque rápido y obtención de firmware” en la página 46 para obtener el menú principal de firmware. 2. Arranque el panel desde el que hará un Ping a. Seleccione la opción 4, **Utilities**. b. Seleccione la opción 11, **Remote Initial Program Load Setup**. c. Seleccione la opción 3, **Ping**. d. Seleccione la interfaz PCMCIA Ethernet. 3. Entre las direcciones IP que desea utilizar para el ping (éstas prevalecerán temporalmente sobre las direcciones configuradas) y pulse **Intro**.

Gestión de la configuración de la línea de mandatos

La Tabla 10 en la página 45 describe cómo gestionar la configuración de la línea de mandatos.

Tabla 10. Cómo gestionar la configuración de la línea de mandatos

Tarea	Cómo llevarla a cabo
Borrar la configuración para un protocolo o para todos los protocolos	1. Desde el indicador *, escriba **talk 6** y pulse **Intro** dos veces para obtener el indicador `Config>`. 2. Escriba **clear ?** para ver una lista de conjuntos de información de configuración que puede borrar con un solo mandato. 3. Escriba **clear** *nombre protocolo* para borrar información para un protocolo determinado o **clear all** para borrar información para todos los protocolos (pero no información de dispositivos). Estos mandatos cambian la configuración actual en memoria pero no afectan al estado de operación del Network Utility.
Borrar la configuración para una interfaz o para todas las interfaces	1. Desde el indicador *, escriba **talk 6** y pulse **Intro** dos veces para obtener el indicador `Config>`. 2. Escriba **del int** si desea suprimir la configuración para una interfaz determinada, incluyendo toda la configuración de protocolo relacionada con dicha interfaz. 3. Escriba **clear dev** si desea suprimir la configuración para todas las interfaces. Este mandato no borra información de protocolo asociada, de modo que normalmente lo utilizará con **clear all** para borrar una configuración completamente. Estos mandatos cambian la configuración actual en memoria pero no afectan al estado de operación del Network Utility.
Activar la configuración actual entera de talk 6	1. Desde el indicador *, escriba **talk 6** y pulse **Intro** dos veces para obtener el indicador `Config>`. 2. Escriba **write** para grabar la configuración actual en memoria en disco en la siguiente posición de archivo de configuración disponible del banco activo. 3. Escriba **reload** y, a continuación, **yes** para rearrancar el Network Utility y activar dicha configuración. Si activa una configuración sin información de protocolo o dispositivo, el Network Utility entrará en modalidad de sólo configuración. Tendrá que definir un protocolo y una interfaz y rearrancar antes de que el Network Utility pueda estar totalmente operativo.

Supervisión de estado general

La Tabla 11 en la página 46 describe cómo efectuar tareas de supervisión de estado general.

Tabla 11. Cómo efectuar la supervisión de estado general

Tarea	Cómo llevarla a cabo
Examinar la utilización de CPU	1. Desde el indicador *, escriba **talk 5** y pulse **Intro** dos veces para obtener el indicador +. 2. Escriba **perf** para obtener el subproceso Console de supervisión de rendimiento. 3. Escriba **list** y verifique que el estado del monitor de CPU es ENABLED (Habilitado). Éste es el valor por omisión para el Network Utility. Si el estado no es ENABLED, escriba **enable cpu**. 4. Escriba **report** para ver estadísticas de utilización de CPU recientes. La instantánea más actual es el valor ″Most recent short window.″ 5. Si desea que se informe de la utilización de CPU con la misma frecuencia que un mensaje de sucesos que puede supervisar con talk 2, escriba **enable t2**. Escriba **Control-p** y **talk 2** para examinar los mensajes de utilización de CPU que se están generando. Escriba **Control-p** para salir talk 2. 6. Si desea que la información de CPU de talk 2 continúe después del siguiente rearranque, vaya a talk 6 y repita los mandatos anteriores. O configure los mismos valores en el panel de utilización de CPU del Programa de configuración y transfiera la configuración actualizada al Network Utility.
Examinar la utilización de memoria	1. Desde el indicador *, escriba **talk 5** y pulse **Intro** dos veces para obtener el indicador +. 2. Escriba **mem** para ver estadísticas de memoria global actuales. Este mensaje indica la memoria física total instalada y detalles acerca de la parte de memoria utilizada por la función de direccionamiento. La función de direccionamiento incluye todos los protocolos de red y características excepto APPN y el servidor TN3270. 3. Si está ejecutando APPN o el servidor TN3270, escriba **p appn** para obtener el subproceso Console de APPN. Escriba **mem** para ver estadísticas de memoria APPN actual y estados de umbral. El uso del servidor TN3270 se incluye en estas estadísticas, aunque sólo se esté ejecutando la conexión de sistema principal TN3270 de subárea.
Activar los mensajes ELS por omisión	1. Desde el indicador *, escriba **talk 5** y pulse **Intro** dos veces para obtener el indicador +. 2. Escriba **event** para obtener el subproceso Console de anotación cronológica de sucesos. 3. Escriba **disp sub all** para activar el nivel STANDARD (estándar) de anotación cronológica para todos los subsistemas definidos. Esto incluye mensajes de error y mensajes informativos poco comunes. 4. Escriba **Control-p** y luego **talk 2** para observar cualquier mensaje que se esté generando y **Control-p** para salir de talk 2. 5. Si desea que se mantengan estos valores después del siguiente rearranque, vaya a talk 6 y repita los mandatos anteriores. Esto hará que los valores formen parte de la configuración.

Opciones de arranque: Arranque rápido y obtención de firmware

La Tabla 12 en la página 47 describe cómo efectuar las tareas de opciones de arranque para el arranque rápido y la obtención de firmware.

Tabla 12. Opciones de arranque: Arranque rápido y obtención de firmware

Tarea	Cómo llevarla a cabo
Minimizar el tiempo de arranque en un entorno de prueba	1. Escriba **talk 6** y luego **boot** para obtener el subproceso Config de arranque. 2. Escriba **en fast** para habilitar la opción de arranque rápido. La siguiente vez que rearranque el Network Utility, éste arrancará más rápidamente saltándose algunos de los diagnósticos de encendido. Esta opción no se recomienda para entornos de producción. Puede utilizar **dis fast** para volver a la modalidad de diagnóstico completo normal.
Obtener el firmware si tiene una consola de terminal conectada directamente	1. Asegúrese de que el tamaño de pantalla de emulación de terminal está establecido en 24 filas por 80 columnas o desactive la acomodación automática en el emulador de terminal. 2. Desde el indicador *, escriba **reload** y luego **yes** al mensaje de confirmación. Empiece a observar detenidamente los mensajes de estado de arranque. 3. Cuando vea el mensaje `Starting Boot Sequence` seguido de `Strike F1 key now to prematurely terminate Boot`, escriba **Control-c** o **F1** inmediatamente. Para asegurarse de que no pierde este mensaje, puede empezar a mantener pulsadas las teclas **Control-c** en cualquier momento después del inicio de los diagnósticos de la placa del sistema. Continúe manteniendo pulsadas **Control-c** hasta que vea el menú principal de firmware o la solicitud de una contraseña de supervisión. 4. Al cabo de unos segundos de que haya aparecido el mensaje `Strike F1 key now to prematurely terminate Boot`, deberá estar en el menú principal de firmware o en una solicitud de contraseña de supervisión. Si no aparece ni uno ni otro y aparecen mensajes de carga de disco, ha esperado demasiado tiempo y ha perdido la ventana de tiempo para escribir **Control-c** o **F1**. Espere a que se complete la secuencia de arranque y, a continuación, repita los pasos 2 y 3 de este procedimiento. O bien, utilice el procedimiento de marcación para asegurarse de que se detendrá en el firmware sin tener que pulsar una tecla en el momento adecuado. 5. Si el sistema le solicita una contraseña de supervisión, entre la contraseña actual, establecida originalmente en ″2216″ en la fábrica. Entonces el sistema presenta el menú principal de firmware.

Tabla 12. Opciones de arranque: Arranque rápido y obtención de firmware (continuación)

Tarea	Cómo llevarla a cabo
Obtener el firmware si tiene una consola de terminal de marcación	1. Asegúrese de que el tamaño de pantalla de emulación de terminal está establecido en 24 filas por 80 columnas o desactive la acomodación automática en el emulador de terminal. 2. Desde el indicador *, escriba **talk 6** y pulse **Intro** dos veces para obtener el indicador `Config>`. 3. Escriba **boot** para obtener el subproceso Config de arranque. 4. Escriba **disable auto-boot** para seleccionar la modalidad en la que una secuencia de arranque se detendrá siempre en el firmware. Si se le solicita la duración (una vez/siempre), seleccione si desea detenerse en el firmware con el siguiente rearranque solamente o con cada rearranque subsiguiente. 5. Escriba **Control-p** para obtener el indicador * y luego **reload yes** para rearrancar el Network Utility. El rearranque le hará perder la conexión de marcación. 6. Después de unos minutos, vuelva a marcar y deberá estar en el menú principal de firmware o en una solicitud de contraseña de supervisión. 7. Si el sistema le solicita una contraseña de supervisión, entre la contraseña actual, establecida originalmente en ″2216″ en la fábrica. Entonces el sistema presenta el menú principal de firmware. Si se le ha solicitado la duración (una vez/siempre) y ha seleccionado siempre o si no ha aparecido dicha solicitud, efectúe un **enable auto-boot** la siguiente vez que obtenga el código de operación.
Arrancar desde el firmware en el código de operación	1. Desde dentro de la estructura de menús de firmware, pulse **Esc** según sea necesario para obtener el menú principal de firmware. 2. Si desea continuar la secuencia de arranque actual hasta llegar al código de operación, pulse **F9** (Iniciar el OS). Si desea rearrancar completamente empezando desde los diagnósticos de encendido, pulse **F3** (Rearrancar). Esto le hará perder la conexión si ha marcado en el módem PCMCIA del Network Utility o el puerto de servicio de tarjeta del sistema. 3. Vuelva a marcar si es necesario o simplemente supervise los mensajes de carga de disco. Pulse la barra espaciadora para obtener el indicador de mandatos si el sistema le solicita dicha acción.

Parte 2. Introducción al Network Utility

Capítulo 5. Recorrido por la interfaz de la línea de mandatos

Este capítulo es una guía que conduce a los usuarios sin experiencia en productos de direccionamiento de IBM a través de los conceptos y la navegación básica de la interfaz de la línea de mandatos del Network Utility. Incluye:

- Conceptos básicos de numeración de puertos y adaptadores
- Cómo trasladarse a diferentes partes del sistema y para qué sirve cada una
- Ejemplos de tareas y mandatos de diferentes procesos
- Cómo navegar por los menús y emitir mandatos
- Cómo configurar y examinar la anotación cronológica del sistema y consultar su estado
- Conceptos básicos para guardar y activar cambios de configuración
- Qué es el firmware, cómo se llega al mismo y unas cuantas cosas que se pueden hacer con él
- Modos en que la función de terminación automática de mandatos le ayuda con la sintaxis para los mandatos entrados en la línea de mandatos

El texto de guía tiene mucho más sentido si se sigue desde el principio al final con el mismo Network Utility.

Si ya tiene experiencia con el IBM 2216, descubrirá que la interfaz del Network Utility es casi idéntica. Esto también es válido para los usuarios del IBM 2212, a excepción de la interfaz de firmware. Los usuarios del IBM 2210 encontrarán indicadores y navegación por menús que les resultarán familiares, pero también encontrarán diferencias en áreas que incluyen la configuración de adaptadores, la salvaguarda de configuraciones y el rearranque del producto.

Indicadores y procesos

Si ha seguido uno de los procedimientos de configuración inicial del “Capítulo 3. Realización de la configuración inicial” en la página 25, ha configurado el Network Utility y lo ha arrancado en modalidad de operación normal. La consola de usuario debe mostrar el indicador de mandatos de asterisco (*).

En modalidad de operación normal, la función de direccionamiento del Network Utility está en ejecución. Como operador, puede utilizar la interfaz de la línea de mandatos para examinar y modificar la configuración, ver el estado del sistema activo, examinar la anotación cronológica de mensajes, etc. Para efectuar estas distintas tareas, navegue por las diferentes partes de la interfaz de la línea de mandatos y el indicador * será la raíz del árbol de navegación.

Escriba **?** desde el indicador * para ver los mandatos disponibles desde este punto:

```
  *?
CONFIGURATION        (Talk 6)
CONSOLE              (Talk 5)
EVENT Logging System (Talk 2)
ELS Console          (Talk 7)
LOGOUT
PING   <Dirección IP>
RELOAD
TELNET to IP-Address <este tipo de terminal>
-------------------------------------------------
DIAGS hardware diagnostics
DIVERT output from process
FLUSH output from process
HALT output from process
```

```
INTERCEPT character is
MEMORY statistics
STATUS of process(es)
SUSPEND command completion
TALK to process
*
```

Aunque cada uno de estos mandatos tiene su finalidad, utilizará dos de ellos mucho más que cualquiera de los demás:

talk Conecta la consola a uno de diversos procesos o modos de ver el sistema.

reload Rearranca el Network Utility.

Para utilizar el mandato **talk**, escriba **t** *n*, donde *n* (un *id de proceso*) toma generalmente uno de los valores siguientes:

6 Examinar y modificar la configuración (el proceso *Config*)

5 Examinar el estado del sistema actual, controlar activamente el estado del sistema en ejecución y activar los cambios de configuración dinámicos (el proceso *Console*)

2 Examinar una anotación cronológica continua de mensajes informativos y de estado (el proceso *Monitor*)

Para deshacer el mandato **talk** y volver desde dentro de cualquier proceso directamente al indicador *, escriba **Control-p**.

MAS V3.3 introdujo mandatos más naturales que efectúan la misma función del mandato **talk**. En lugar de **talk 6**, puede escribir simplemente **config**. Del mismo modo, **console** puede sustituir a **talk 5** y **event** a **talk 2**.

Las tres secciones siguientes describen cada uno de los procesos principales y explican algunas de las tareas que se pueden efectuar dentro de cada proceso. A medida que vaya avanzando, aprenderá a moverse entre procesos y menús y a entrar mandatos.

Configuración (utilizando talk 6, el proceso Config)

Desde el indicador *, escriba **t 6** o **config** para entrar en el proceso de la línea de mandatos para configurar el Network Utility:

```
*         <Intro>
*t 6
Gateway user configuration
Config>   <Intro>
Config>
```

Ahora que está dentro del proceso Config, el indicador de mandatos ha cambiado de * a `Config>`. Los procesos Config y Console tienen indicadores exclusivos de modo que puede saber de un vistazo en qué proceso se encuentra. El mensaje de estado `Gateway user configuration` sólo aparece la primera vez que entra en el proceso Config a continuación de un rearranque (″gateway″ se utiliza como sinónimo de ″router″ en diversos lugares del sistema).

Cuando haya estado en un proceso anteriormente y vuelva a entrar en el mismo utilizando el mandato **talk**, el sistema le dará una línea en blanco en lugar de un indicador de mandatos inmediato. Pulse **Intro** y volverá al lugar en que se encontraba la última vez que estuvo dentro de dicho proceso:

```
Config>   <Control-p>     <---- dejar Config y volver a *
*         <Intro>
*t 6                      <---- volver a Config
          <Intro>
Config>                   <---- hemos vuelto al indicador principal de Config
```

Cuando se trabaja dentro del proceso Config, se cambia el modo en que el Network Utility se ha configurado para operar. Con unas pocas excepciones, estos cambios no tienen ningún efecto en el estado en ejecución del direccionador. Para activar los cambios de talk 6 deberá:

- Emitir uno de varios mandatos para activar un conjunto de cambios o
- Guardar los cambios en el disco duro y rearrancar el sistema

A medida que avance por esta guía verá ejemplos de ambos métodos.

Visión general de mandatos

En el indicador principal `Config>`, escriba **?** para ver una lista alfabética de los mandatos disponibles:

```
Config>?
  ADD (device, user)
  BOOT and load file functions
  CHANGE (device, password, user)
  CLEAR configuration information
  DELETE (interface, user)
  DISABLE (interface, console-login, etc)
  ENABLE (interface, console-login, etc)
  EVENT logging system and messages
  FEATURE (non-protocol and network features)
  LIST (devices, configuration, patches, users)
  LOAD (add, delete, list)
  NETWORK interface configuration
  PATCH global configuration parameters
  PERFORMANCE monitor
  PROTOCOL configuration
  QCONFIG (quick configuration)
  SET system-wide parameters
  SYSTEM
  TIME of day parameters
  UNPATCH global configuration parameters
  UPDATE
  WRITE
  Config>
```

Algunos de estos mandatos son para configurar realmente las funciones del sistema y otros son para la gestión de la configuración y la administración del sistema. Para que tenga una idea de los tipos de acciones que se hacen bajo talk 6, la lista siguiente agrupa mandatos clave por tarea de usuario:

- Configuración de adaptadores y puertos

  add device
  : Configura una sola ranura de adaptador y un puerto

  change device
  : Mueve una configuración de ranura a otra ranura o la copia en otra ranura

  delete interface
  : Suprime una interfaz individual (puerto de adaptador) y la información de protocolo asociada

  disable/enable interface
  : Controla si se activará una interfaz específica

list device
Muestra todas las interfaces configuradas
net*número interfaz*
Va al subproceso para configurar la interfaz específica, debajo del nivel de protocolo
set data-link
Cambia un puerto de adaptador de WAN recién añadido del valor por omisión de PPP a Frame Relay, SDLC, SDLC Relay o X.25
system set/display ip
Establece/Muestra los parámetros IP para el adaptador PCMCIA de LAN

- Configuración de protocolos y características
  protocol *nombre*
  Va al subproceso para configurar el protocolo especificado
  feature *nombre*
  Va al subproceso para configurar la característica especificada
- Gestión de configuraciones y cargas de software
  boot Va al subproceso para gestionar la transferencia y la utilización de archivos de configuración y cargas de software en disco
  clear Puede borrar toda la configuración actual de dispositivos o de protocolos en la RAM o bien partes específicas de dicha configuración.
  write Guarda en el disco duro la configuración actual que se encuentra en la RAM
- Configuración para supervisar el sistema
  event Va al subproceso para configurar los mensajes del sistema de anotación cronológica de sucesos (ELS) que están activos
  performance
  Va al subproceso para configurar la supervisión de utilización de CPU
- Administración del sistema
  add/change/delete/list user, change password
  Administra los ID de usuario para el acceso a consola controlado
  disable/enable console-login
  Controla el acceso remoto a consola
  set host/prompt/contact/location
  Define un nombre de sistema principal, un prefijo de indicador, una persona de contacto o una ubicación
  time Establece la hora y el formato de hora o indica si se debe obtener la hora de un sistema principal remoto
- Servicio al software
  disable/enable/set dump, reboot
  Controla los vuelcos y los rearranques si el sistema Network Utility termina anormalmente la operación
  patch, unpatch
  Controla funciones de software especializadas para evitar problemas en entornos de usuario específicos
  system retrieve
  Envía un vuelco de sistema compactado del direccionador a un servidor
  system view
  Muestra información acerca de los archivos de vuelco actuales

Los ejemplos siguientes muestran cómo utilizar algunos de estos mandatos de talk 6 para realizar tareas de configuración básicas. A medida que avance por los ejemplos, ganará experiencia no sólo con las tareas mostradas sino también en el modo general de moverse por los menús y de emitir mandatos. Los ejemplos empiezan con una tarea que ya puede serle familiar si ha utilizado el procedimiento de la línea de mandatos para la configuración inicial.

Ejemplo: Configuración de un puerto en un adaptador

En el ejemplo en ejecución utilizado en toda esta guía, el usuario ha arrancado primero un Network Utility con la configuración siguiente:

- Adaptador ESCON en la ranura 1, IP no configurado
- Adaptador de Red en Anillo en la ranura 2, puerto 2 configurado con la dirección IP 192.1.1.8

Si desea seguir este ejemplo, utilice **clear dev** para borrar su propia configuración de dispositivo[6] y, a continuación, utilice **add dev** y **del int** para entrar en la configuración de dispositivo ESCON/TR como se muestra a continuación.

Desde el indicador `Config>`, escriba **list device** (o **li dev**, abreviado) para ver los adaptadores y puertos que están definidos en la configuración actual. Si no tiene ninguna configuración o ningún puerto de adaptador definido, **li dev** no le proporciona ninguna salida sino que simplemente vuelve a emitir el indicador de usuario. Dado que ha borrado todos los dispositivos, puede añadir uno. Escriba **add dev ?** para ver una lista de todos los tipos de adaptador que puede añadir:

```
Config>clear dev
You are about to clear all Device configuration information.
Are you sure you want to do this? ? [No]: yes
Device configuration cleared
Config>li dev
Config>add dev ?
ATM             1-port 155 Mbps ATM adapter
EIA-232E        8-port EIA-232E/V.24 adapter
ESCON Channel   1-port ESCON Channel adapter
ETHERNET        2-port Ethernet adapter
ETH100          1-port 10/100 Mb Ethernet adapter
FDDI            1-port FDDI adapter
HSSI            1-port HSSI adapter
PCA             1-port Parallel Channel adapter
TOKEN-RING      2-port Token-Ring adapter
V35/V36         6-port V.35/V.36 adapter
X21             8-port X.21 adapter
Config>
```

Utilice el mandato **add dev** para configurar un solo puerto en un solo adaptador. Para un adaptador multipuerto, deberá especificar qué puerto está añadiendo a la configuración y volver a emitir el mandato para cada puerto que desee tener activo. Aquí añadimos un adaptador ESCON de un solo puerto y ambos puertos de un adaptador de Red en Anillo de 2 puertos:

```
Config>add dev esc
Device Slot #(1-2) [1]? 1
Adding ESCON Channel device in slot 1  port 1 as interface #0
Use "net 0" to configure ESCON Channel parameters
Config>add dev tok
Device Slot #(1-2) [1]? 2
Device Port #(1-2) [1]? 1
Adding Token-Ring device in slot 2  port 1 as interface #1
Use "net 1" to configure Token-Ring parameters
Config>add dev tok
Device Slot #(1-2) [1]? 2
Device Port #(1-2) [2]? 2
Adding Token-Ring device in slot 2  port 2 as interface #2
Use "net 2" to configure Token-Ring parameters
Config>li dev
```

6. Normalmente, sólo utilizará **clear dev** junto con **clear all**, que borra la información de protocolo.

```
Ifc 0     ESCON Channel                    Slot: 1   Port: 1
Ifc 1     Token-Ring                       Slot: 2   Port: 1
Ifc 2     Token-Ring                       Slot: 2   Port: 2
Config>
```

Para especificar el tipo de adaptador, escriba en la misma línea que **add dev** los primeros caracteres de las palabras de la columna izquierda de la lista de salida de **add dev ?** (los caracteres suficientes para distinguir el tipo de adaptador que desea). Cuando se le solicite, deberá proporcionar la ranura y (para adaptadores multipuerto solamente) el número de puerto. La numeración de ranuras y puertos se fija del modo siguiente:

- Las dos ranuras de adaptador de un Network Utility se numeran 1 y 2, de izquierda a derecha mirando el sistema de frente.
- Los puertos de los adaptadores multipuerto de LAN se numeran 1 y 2 y están etiquetados en la cara del adaptador.
- Los puertos de los adaptadores multipuerto de WAN se numeran a partir de 0 y están etiquetados en los conectores al final del cable de adaptador.

El mandato **add dev** se asegura de que no se intenta añadir dos adaptadores diferentes en la misma ranura, añadir un adaptador en una ranura que no existe o especificar un número de puerto que no existe en un adaptador determinado. ***No*** valida el tipo de dispositivo seleccionado con los adaptadores que están físicamente instalados en el Network Utility. Esto le permite configurar adaptadores que aún no ha instalado o producir una configuración para un Network Utility diferente. El sistema sólo valida la configuración de dispositivo cuando se arranca con una configuración determinada o se intenta activar una interfaz dinámicamente. El sistema indica las discrepancias mediante los LED de la parte frontal del adaptador, así como desde una anotación cronológica de sucesos que se puede ver localmente. También puede escribir mandatos para ver el estado del adaptador, como verá más adelante en esta guía.

Números de interfaz lógica

En respuesta al mandato **add dev**, el Network Utility asigna un *número de interfaz* lógica o *número de red* al puerto que acaba de añadir. Éste es el número clave mediante el cual hará referencia a esta interfaz en todos los demás mandatos del sistema. Únicamente el mandato **add dev** utiliza los números de puerto y ranura física; todos los demás mandatos utilizan el número de interfaz lógica. Cuando se subdivide un puerto físico (″base″), por ejemplo ESCON, en múltiples interfaces virtuales, cada interfaz virtual tiene también un número de interfaz. Como se muestra más arriba, puede utilizar el mandato **li dev** para ver el número de interfaz para cada interfaz física y virtual.

Ejemplo: Supresión de una interfaz

Si comete un error y desea deshacer el mandato **add dev** o desea suprimir la configuración de adaptador/puerto por cualquier razón, utilice el mandato **delete interface**. (No se denomina ″delete device″, porque trata con los números de interfaz lógica y no con los números de ranura/puerto del adaptador). Para continuar el ejemplo, suponga que desea utilizar solamente el puerto 2 del adaptador de Red en Anillo. Suprima el puerto 1 (que resulta ser la interfaz 1) como se indica a continuación:

```
Config>li dev
Ifc 0     ESCON Channel                    Slot: 1   Port: 1
Ifc 1     Token-Ring                       Slot: 2   Port: 1
Ifc 2     Token-Ring                       Slot: 2   Port: 2
```

```
Config>del int
Interface number? 1
Interface being deleted... please be patient.
The router must be restarted
Interface 1 deleted successfully
Config>li dev
Ifc 0     ESCON Channel                    Slot: 1   Port: 1
Ifc 1     Token-Ring                       Slot: 2   Port: 2
Config>
```

Observe que el puerto 2 de Red en Anillo se ha convertido ahora la interfaz lógica 1. Si hubieran existido otras interfaces con números superiores a 1, estos números también se habrían disminuido en 1. Si desea suprimir cada interfaz de una configuración, suprima sólo la interfaz 0 repetidamente hasta que no haya más interfaces.

Además de la configuración de dispositivo propiamente dicha, es normal tener la configuración de protocolo asociada con una interfaz determinada. Cuando se suprime una interfaz utilizando el mandato **del int**, el sistema también suprime toda la configuración de protocolo asociada con dicha interfaz y vuelve a numerar toda la configuración de protocolo asociada con las interfaces renumeradas[7]. Necesita rearrancar el Network Utility para que una operación **del int** entre en vigor en el sistema en ejecución.

Ejemplo: Establecimiento del nombre de sistema principal utilizando menús

Para examinar más detenidamente cómo emitir mandatos en general, pruebe algo sencillo, como utilizar el mandato **set** para configurar un nombre (″nombre de sistema principal″) para este Network Utility.

Nota: Este ejemplo supone que está ejecutando con la terminación de mandatos inhabilitada. Consulte el apartado “Terminación automática de mandatos” en la página 37 para comprender cómo puede el Network Utility proporcionar la terminación automática de mandatos.

En primer lugar, pruebe el mandato solo:

```
Config>set
Command not fully specified
```

Este mensaje de error informa que el mandato **set** está respaldado por un menú de palabras clave adicionales y que es necesario que escriba más palabras clave hasta formar un mandato completo que efectúe una acción. En cualquier momento que se encuentre en un menú (como ya ha visto), puede escribir **?** para ver los mandatos disponibles o las palabras clave a escribir. Si sólo está intentando recordar palabras clave de mandatos, generalmente es más rápido moverse escribiendo **?** que consultar el mandato en un manual. En este caso, las opciones son:

```
Config>set ?
CONTACT-PERSON
DATA-LINK
DOWN-NOTIFY
GLOBAL-BUFFERS
HOSTNAME
INACTIVITY-TIMER
```

7. El mandato **clear dev** no realiza esta función, de modo que sólo lo deberá utilizar cuando esté también borrando información de protocolo a mano.

```
INPUT-LOW-WATER
LOCATION
PACKET-SIZE
PROMPT
RECEIVE-BUFFERS
SPARE-INTERFACES
```

Como puede ver, el menú **set** incluye una mezcla de elementos de datos: algunos para la administración del sistema, otros para el ajuste de nodos, etc. En Network Utility, las opciones de ajuste de nodos toman valores por omisión y no tendrá que cambiarlas.

Volviendo a la tarea, la palabra clave que desea es claramente ″hostname″. Puede abreviar cualquier elemento de menú (nombre de mandato o palabra clave) al número de caracteres necesarios para hacerlo exclusivo, de modo que acorte ″hostname″ un poco:

```
Config>set host
Host name for this node []? rtp01
Host name updated successfully
rtp01 Config>
```

Por omisión, el sistema inserta el nuevo nombre de sistema principal delante de todos los indicadores de mandatos. A muchos usuarios les gusta esto porque les permite ejecutar Telnet en diversos direccionadores desde una sola estación de trabajo y distinguir fácilmente una consola de direccionador de otra. Si desea elegir un prefijo de indicador diferente, puede utilizar para ello el mandato **set prompt**. Para restablecer el sistema principal o el indicador a un valor nulo, utilice el mandato **clear host** o **clear prompt** y rearranque el Network Utility. Para consultar los valores actuales, utilice **list config**.

Tenga en cuenta que **set host** es una excepción de la regla normal de talk 6 porque ha entrado en vigor inmediatamente y no ha sido necesario que emitiera algún tipo de mandato de ″activación″ ni que rearrancara el Network Utility. Hay muy pocos mandatos de talk 6 que se comporten de este modo, pero éste es útil porque puede ver inmediatamente su efecto en el indicador de usuario.

Ejemplo: Tecleo anticipado

Suponga que no le gusta el nuevo indicador y desea cambiar el nombre de sistema principal de ″rtp01″ a ″RTP01″. Puede efectuar esta acción en un solo mandato, como se indica a continuación:

```
rtp01 Config>set host RTP01
Host name updated successfully
RTP01 Config>
```

El sistema no le ha solicitado el nombre de sistema principal porque lo ha escrito en la línea de mandatos original. Esto ilustra otra norma general: cuando un mandato completo le solicita parámetros de entrada, tiene la opción de escribirlo en la línea de mandatos original y de saltarse las solicitudes. Si elige saltarse las solicitudes, deberá tener cuidado de escribir los parámetros en el orden correcto.

Ejemplo: Establecimiento de un parámetro de puerto utilizando ″net″

Ahora que ya ha configurado el nombre de sistema principal, pruebe algo un poco más complejo. Suponga que al rearrancar de la modalidad de sólo configuración (Config-only) ha notado que el puerto 2 de adaptador de Red en Anillo recién configurado no se ha activado. Puede consultar la velocidad de anillo para la que

se ha configurado y cambiar dicho valor. Como se muestra a continuación, el mandato **net** se utiliza para esta clase de parámetro de configuración de bajo nivel específico de dispositivo:

```
RTP01 Config>li dev           <------ ¿cuáles eran esos números de i/f?
Ifc 0     ESCON Channel                Slot: 1   Port: 1
Ifc 1     Token-Ring                   Slot: 2   Port: 2
RTP01 Config>       <Intro>
RTP01 Config>net 1            <------ Configuro la interfaz 1
Token-Ring interface configuration
RTP01 TKR config>   <Intro>   <------ observe el nuevo indicador de subproceso
RTP01 TKR config>?            <------ ¿cuáles son los mandatos aquí?
EXIT
FRAME
LIST
LLC
MEDIA
SET
PACKET-SIZE bytes
SOURCE-ROUTING
SPEED Mb/sec
RTP01 TKR config>li           <------ mostrarme qué tengo ahora
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                    4 Mb/sec       <----- Debería ser 16 Mb/seg
Media:                    Shielded

RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              000000000000
RTP01 TKR config>speed
Speed (4 or 16) [4]? 16       <------ cambiar la velocidad aquí
RTP01 TKR config>li           <------ verificar el nuevo valor
Token-Ring configuration:

Packet size (INFO field): 2052
Speed:                    16 Mb/sec       <----- ahora parece correcto
Media:                    Shielded

RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              000000000000
RTP01 TKR config>ex           <------ salir del subproceso
RTP01 Config>                 <------ vuelve a estar en el menú principal T 6
```

Este cambio en la velocidad del anillo no entra en vigor inmediatamente, sino que necesita un mandato talk 5 o un rearranque para activarlo. El apartado “Reconfiguración dinámica” en la página 77 incluye los conceptos básicos para activar cambios de configuración sin un rearranque. Normalmente se utiliza el mandato **net** inmediatamente después de **add dev** para ver los valores por omisión para la nueva interfaz y efectuar los cambios necesarios antes de activar el puerto por primera vez.

En este ejemplo, al escribir **net 1**, se ha trasladado a un subproceso para configurar interfaces de Red en Anillo. El menú base ha cambiado y el indicador también ha cambiado para indicarle que ya no estaba en el menú principal de `Config>`, sino en un nivel más profundo. Para salir de cualquier menú de subproceso y volver al menú superior siguiente, escriba **exit**. Recuerde también que **Control-p** le hace salir inmediatamente al indicador * y que cuando vuelve a dicho proceso, vuelve a entrar en el punto en el que estuvo por última vez:

```
RTP01 Config>       <Intro>       <------ empezar aquí
  RTP01 Config>net 1              <------ entrar en un subproceso Config
```

```
  Token-Ring interface configuration
  RTP01 TKR config>   <Control-p> <------ saltar hacia fuera
  RTP01 *             <Intro>
  RTP01 *t 6                      <------ volver a Config
                      <Intro>
  RTP01 TKR config>   <Intro>     <------ vuelve a estar en el subproceso
  RTP01 TKR config>ex             <------ salir del subproceso
  RTP01 Config>                   <------ vuelve a estar donde empezó
```

Ahora intente dos ejemplos más en el proceso Config y, a continuación, trasládese al proceso Console. El primer ejemplo muestra cómo reducir el tiempo para recargar el sistema y el segundo muestra cómo cambiar parámetros asociados con un protocolo de sistema.

Ejemplo: Habilitación del ″fast-boot″

Desde el indicador `Config>`, escriba **boot** para obtener el subsistema para gestionar configuraciones, cargas de código y opciones de arranque. El “Capítulo 7. Manejo de archivos de configuración” en la página 81 le proporciona la información básica completa acerca de este subsistema, de modo que aquí no necesita consultar todos los mandatos. Mire bajo el mandato **enable** e intente la opción de ″fast-boot″ (″arranque rápido″):

```
RTP01 Config>boot                       <----- entrar en subproceso
  Boot configuration
  RTP01 Boot config>   <Intro>          <----- observe el nuevo indicador
  RTP01 Boot config>en ?                <----- listar opciones de "enable"
  AUTO-BOOT-- set Unattended mode
  FAST-BOOT-- bypass diags
  RTP01 Boot config>en fast             <----- intentar "fast-boot"
  FastBoot mode is now enabled.

  Operation completed successfully.
  RTP01 Boot config>ex                  <----- salir del subproceso boot
  RTP01 Config>
```

Si ha observado los mensajes de arranque de consola al encender el Network Utility o ha escrito el mandato **reload**, puede que se haya dado cuenta de que el sistema ejecuta diversos diagnósticos de encendido cuando está arrancando. Aunque es deseable para un direccionador de producción que se rearranca con poca frecuencia y cuyo hardware debe validarse, esta acción alarga el tiempo de arranque. Si está configurando activamente y rearrancando repetidamente un direccionador determinado, puede que desee reducir el tiempo de arranque saltándose estos diagnósticos. Con el mandato **enable fast-boot** acaba de reducir dicho tiempo. La siguiente vez que realice un **reload**, dicha acción se efectuará más rápidamente. Antes de poner el Network Utility en producción deberá deshacer este cambio utilizando **disable fast-boot**.

Tenga en cuenta que la modalidad de arranque rápido sólo se puede controlar a través de la línea de mandatos y no desde el Programa de configuración. La modalidad de arranque del sistema se almacena en memoria no volátil del sistema y no forma parte del archivo de configuración.

Ejemplo: Modificación de la dirección IP de una interfaz

El último ejemplo del proceso Config utiliza los menús y mandatos del subproceso de protocolo IP para modificar la dirección IP de una interfaz. Como se ha indicado

en la página 57, este ejemplo ha empezado con un Network Utility que tenía una dirección IP configurada en la Interfaz 1 (puerto 2 del adaptador de Red en Anillo de la ranura 2).

```
RTP01 Config>li dev            <----- ¿cuáles son las interfaces de nuevo?
Ifc 0     ESCON Channel                Slot: 1   Port: 1
Ifc 1     Token-Ring                   Slot: 2   Port: 2
RTP01 Config>p ip              <----- abreviatura para "protocol ip"
Internet protocol user configuration
RTP01 IP config>   <Intro>     <----- ahora en subproceso IP Config
RTP01 IP config>li addr        <----- listar direcciones IP configuradas
IP addresses for each interface:
   intf     0                                    IP inhabilitado en esta interfaz

   intf     1   192.1.1.8        255.255.255.0    Difusión hilo local, rellenar 1
RTP01 IP config>change addr
Enter the address to be changed []? 192.1.1.8
New address [192.1.1.8]? 192.7.7.7
Address mask [255.255.255.0]?   <Intro>
RTP01 IP config>li addr         <----- verificar la modificación
IP addresses for each interface:
   intf     0                                    IP inhabilitado en esta interfaz

   intf     1   192.7.7.7        255.255.255.0    Difusión hilo local, rellenar 1
RTP01 IP config>ex              <----- salir de IP config
RTP01 Config>
```

Éste es el primer ejemplo de utilización del mandato **protocol** para entrar en el subproceso para un protocolo individual. IP es sólo uno de los diversos protocolos que podría haber seleccionado y existe una lista similar de características a las que puede acceder utilizando el mandato **feature**. Escriba **list config** desde `Config>` para obtener una lista completa de los protocolos y características que puede configurar o sólo **p ?** o **f ?** para obtener un recordatorio rápido. Todos los protocolos y las características funcionan del mismo modo: entre en el subproceso para un protocolo o característica, configúrelo utilizando mandatos específicos de dicho protocolo o característica y luego ejecute **exit** para salir al indicador principal `Config>`.

Para obtener material detallado de consulta de mandatos sobre un protocolo determinado, consulte el capítulo relacionado con dicho protocolo en uno de los dos volúmenes de la publicación *MAS Consulta de configuración y supervisión de protocolos*. Cada uno de estos capítulos proporciona material de introducción acerca del protocolo así como una descripción de cada mandato de consola de supervisión y configuración para dicho protocolo. Para obtener la misma información acerca de las características MAS, consulte la publicación *MAS Utilización y configuración de las características*.

Ahora ya ha completado la visión general del proceso Config y de sus mandatos. Ahora puede ir a talk 5, el proceso Console. Recuerde, para salir de cualquier proceso escriba **Control-p** para obtener el indicador * y entonces estará listo para utilizar el mandato **talk** para entrar en otro proceso:

```
RTP01 Config>   <Control-p>
RTP01 *
```

Operación (Utilizando talk 5, el proceso Console)

Desde el indicador *, escriba **t 5** o **console** para entrar en el proceso de la línea de mandatos a fin de supervisar y controlar el estado activo del Network Utility:

```
RTP01 *   <Intro>
RTP01 *t 5


CGW Operator Console

RTP01 +   <Intro>
RTP01 +
```

Ahora que está dentro del proceso Console, el indicador de mandatos ha cambiado de * a +. Los procesos Config y Console y sus subprocesos tienen indicadores exclusivos que indican la posición de un vistazo. El mensaje de estado `CGW Operator Console` sólo aparece la primera vez que se entra en el proceso Console tras un rearranque. Como se ha explicado con talk 6, si el sistema le muestra una línea en blanco al escribir **t 5**, ello significa que ha estado antes en talk 5 y necesita pulsar **Intro** para reanudar en el lugar en el que se encontraba por última vez.

Cuando se trabaja en el proceso Console, se escriben mandatos para ver y modificar el estado activo en ejecución del Network Utility. Desde este proceso no se pueden modificar los archivos de configuración del Network Utility. Algunos mandatos de talk 5 permiten modificar de forma dinámica parámetros de configuración, pero estas modificaciones se pierden al rearrancar el Network Utility. Sin embargo, si ha efectuado cambios de configuración bajo talk 6, puede activar de forma dinámica algunos de ellos desde talk 5 sin rearrancar el Network Utility.

Visión general de mandatos

En el indicador principal +, escriba **?** para ver una lista alfabética de los mandatos disponibles:

```
RTP01 +?
ACTIVATE interface
BUFFER statistics
CLEAR statistics
CONFIGURATION of router
DISABLE interface or slot
ENABLE slot
ERROR counts
EVENT logging
FEATURE commands
INTERFACE statistics
MEMORY statistics
NETWORK commands
PERFORMANCE monitor
PROTOCOL commands
QUEUE lengths
RESET interface
STATISTICS of network
TEST network
UPTIME
RTP01 +
```

Algunos de estos mandatos son para ver el estado del sistema y algunos son mandatos del operador para cambiar el estado de forma activa. Además, bajo cada protocolo y característica hay un subproceso Console que contiene una combinación de estos dos tipos de mandatos. La lista siguiente agrupa los mandatos clave de talk 5 por tarea de usuario:

- Visualización del estado del sistema
  buffer Muestra la asignación de almacenamiento intermedio de interfaz y las cuentas en uso

configuration
Muestra la identidad del software, protocolos/características y el estado de interfaz

error Muestra cuentas de error de trama para una o más interfaces

interface
Muestra el número de interfaz para la correlación de ranura/puerto (el equivalente de talk 5 de **list dev** de talk 6), más el número de veces que han pasado/fallado las autopruebas

memory
Muestra la memoria instalada y las estadísticas en uso para la memoria y los almacenamientos intermedios generales (no de interfaz)

queue Muestra cuentas de colas de almacenamiento intermedio de entrada y salida para una o más interfaces

statistics
Muestra cuentas de paquetes y bytes para una o más interfaces

uptime
Muestra el tiempo transcurrido desde el último rearranque

- Control del estado del sistema

  activate
  Habilita una interfaz de repuesto que acaba de configurar bajo talk 6

  clear Restablece los contadores para una o más interfaces

  disable
  Deja fuera de línea una interfaz individual o todas las interfaces de una ranura

  enable
  Pone en línea todas las interfaces de una ranura especificada

  reset Inhabilita una interfaz y vuelve a habilitarla utilizando parámetros de configuración nuevos que se han cambiado bajo talk 6

  test Verifica y pone en línea una interfaz individual

- Acceso a otros proceso de consola

  event Ir a ver cuentas y cambiar temporalmente los mensajes de ELS que se están anotando

  feature *nombre*
  Ir a ver y cambiar el estado para la característica especificada

  network *número interfaz*
  Ir a ver y cambiar el estado para la interfaz especificada

  performance
  Ir a ver estadísticas de CPU y cambiar temporalmente el modo en que éstas se reúnen y se visualizan

  protocol *nombre*
  Ir a ver y cambiar el estado para el protocolo especificado

Ejemplo: Visualización del estado del sistema

Igual que ha hecho desde talk 6, pruebe algunos de estos mandatos de talk 5. Los mandatos para ver el estado del sistema son muy sencillos; simplemente escriba el mandato de una palabra y observe la salida:

```
RTP01 +mem
Physical installed memory:       256 MB
Total routing (heap) memory:     228 MB
Routing memory in use:             3 %

                  Total  Reserve    Never     Perm     Temp     Prev
                                    Alloc    Alloc    Alloc    Alloc
Heap memory    239390720    26616 232309212  7029792    49828     1888
```

```
Number of global buffers: Total = 1000, Free = 1000, Fair = 194, Low = 200
Global buff size: Data = 4478, Hdr = 82, Wrap = 72, Trail = 7, Total = 4644
RTP01 +   <Intro>
RTP01 +buff
                    Input Buffers        Buffer sizes                    Bytes
Net   Interface     Req Alloc Low Curr   Hdr  Wrap  Data Trail Total    Alloc
0     ESCON/0       255   255  20    0    86    72  4478     0  4636  1182180
1     TKR/0         250   250   7    0    85    72  2052     7  2216   554000
```

Como puede ver, **mem** muestra el estado a nivel del sistema, mientras que **buff** proporciona información a nivel de interfaz. Para todos los mandatos que proporcionan información por interfaz (**buff**, **config**, **error**, **int**, **queue**, **stat**), puede especificar una lista o un rango de números de interfaz en los que está interesado:

```
RTP01 +int 0-1
                                                Self-Test  Self-Test Maintenance
  Net   Net'   Interface   Slot-Port              Passed     Failed      Failed
  0     0      ESCON/0     Slot: 1   Port: 1           0          0           0
  1     1      TKR/0       Slot: 2   Port: 2           0          0           0
  RTP01 +stat 1
  Net   Interface      Unicast  Multicast      Bytes    Packets      Bytes
                      Pkts Rcv   Pkts Rcv   Received      Trans      Trans
  1     TKR/0                0          0          0          0          0
```

Consulte el capítulo ″The Operating/Monitoring Process″ de la publicación *MAS Guía del usuario de software* para obtener una descripción de los campos de la salida de cada mandato.

Ejemplo: Visualización del estado de interfaz

El mandato **config** es especialmente importante porque, al final de la salida, se encuentra el estado de todas las interfaces especificadas (esta salida de ejemplo se ha editado eliminando las líneas en blanco):

```
RTP01 +c
Multiprotocol Access Services
NetU-TX1 Feature 1001 V3.1 Mod 0 PTF 1 RPQ 0 MAS.DE1 netu_38PB

Num Name  Protocol
0   IP     DOD-IP
3   ARP    Address Resolution
11  SNMP   Simple Network Management Protocol
29  NHRP   Next Hop Resolution Protocol

Num Name  Feature
2   MCF    MAC Filtering
7   CMPRS  Data Compression Subsystem
8   NDR    Network Dispatching Router
10  AUTH   Authentication

2 Total Networks:
Net  Interface   MAC/Data-Link        Hardware                    State
0    ESCON/0     ESCON               ESCON Channel               Not present

1    TKR/0       Token-Ring/802.5    Token-Ring                  HW Mismatch
RTP01 +
```

El Network Utility del que se ha capturado esta salida de ejemplo tiene de hecho una ranura 1 vacía y un adaptador Ethernet en la ranura 2. En talk 6, no importa si lo que se configura no coincide con los adaptadores instalados, pero al rearrancar con dicha configuración, talk 5 le mostrará que las interfaces configuradas no se han activado.

Si hubiera realizado una configuración correcta, el estado de interfaz empezaría con ″Testing″, luego se movería a ″Up″ y podrá utilizar el mandato **net** para entrar en un subproceso Console específico de adaptador para obtener información de estado más detallada. Tal como está ahora, obtendrá lo siguiente:

```
RTP01 +net 0
 Network interface is not available.
RTP01 +
```

Ejemplo: Acceso a un protocolo no configurado

Para ver y controlar lo que está sucediendo actualmente con un protocolo determinado, utilice el mandato **protocol** para entrar en el subproceso Console para dicho protocolo. Tal como se ha explicado anteriormente, **p ?** generará una lista rápida de los protocolos soportados en una carga de software determinada. Por ejemplo, seleccione DLSw (Data Link Switching) (Conmutación de enlace de datos):

```
RTP01 +p dls                    <----- abreviatura para "protocol dlsw"
   Protocol DLSW is available but not configured
  RTP01 +
```

DLSw está disponible ***(available)*** porque esta carga de software lo soporta[8], pero no está configurado ***(not configured)*** porque no ha entrado en talk 6 ni ha entrado los mandatos para habilitar DLSw. Ahora que ha arrancado el sistema sin DLSw en la configuración, éste no está en ejecución y no hay ningún estado de DLSw para ver o modificar desde talk 5.

Ejemplo: Acceso a un protocolo configurado

Como se ha indicado en la página 57, este ejemplo empieza en un Network Utility ya arrancado con una configuración IP. Dado que IP se está ejecutando activamente, puede entrar en el subproceso Console y ver qué mandatos están disponibles:

```
RTP01 +p ip                     <----- abreviatura para "protocol ip"
RTP01 IP>?
ACCESS controls
CACHE
COUNTERS
DUMP routing tables
INTERFACE addresses
PACKET-FILTER summary
PARAMETERS
PING dest_addr [src_addr size ttl rate]
REDUNDANT Default Gateways
RESET
RIP
ROUTE given address
ROUTE-TABLE-FILTERING
SIZES
STATIC routes
TRACEROUTE dest_addr [src_addr size probes wait ttl]
UDP-FORWARDING
VRID
VRRP
EXIT
RTP01 IP>
```

8. Si no se soportara, no habría aparecido bajo **p ?** y el sistema no habría reconocido el valor ″dls″.

Si compara esta lista de mandatos con la que se ha generado en talk 6 al escribir **?** en el indicador **IP config>**, verá que los mandatos de talk 5 y talk 6 son bastante diferentes. En talk 5, por ejemplo, puede iniciar un **ping** para ver si puede obtener una dirección IP determinada desde el Network Utility. Dado que se trata de un mandato activo que opera inmediatamente en una interfaz de red activa, no pertenece a talk 6. Otros mandatos para ver el estado activo son también mandatos de talk 5 y no mandatos de talk 6.

Ejemplo: Reconfiguración dinámica

En talk 6 ha cambiado la dirección IP del puerto 2 de Red en Anillo 2 de 192.1.1.8 a 192.7.7.7. Ahora vea qué valor aparece bajo talk 5:

```
RTP01 IP>int                          <----- abreviatura para "interface"
  Interface  IP Address(es)   Mask(s)
    TKR/0    192.1.1.8        255.255.255.0
```

El cambio de talk 6 no ha tenido ningún efecto en el estado de operación del Network Utility, porque aún no lo ha activado mediante un mandato explícito o rearrancando. Utilice el mandato **reset ip** para volver a leer la configuración IP actual de talk 6 y activarla en el sistema en ejecución:

```
RTP01 IP>reset ip
RTP01 IP>int
Interface  IP Address(es)   Mask(s)
  TKR/0    192.7.7.7        255.255.255.0
RTP01 IP>ex
RTP01 +
```

Como puede ver, el cambio de dirección IP (y cualquier otro cambio de IP efectuado bajo talk 6) están ahora activos. La mayoría de los protocolos tienen algún mecanismo para la reconfiguración dinámica, pero no todos los protocolos tienen un mandato **reset** bajo talk 5. Consulte el apartado “Reconfiguración dinámica” en la página 77 para obtener más información básica sobre los procedimientos para realizar la reconfiguración dinámica.

Ahora ya ha visto cómo emitir mandatos de talk 5 para consultar activamente el estado del sistema. Hay disponible otro mecanismo más pasivo: ver los mensajes de sucesos que genera el Network Utility. Para ello utilice **talk 2**. Como siempre, escriba **Control-p** para salir del proceso actual:

```
RTP01 +   <control-p>
RTP01 *
```

Anotación cronológica de sucesos (Utilizando talk 2, el proceso Monitor)

Desde el indicador *, escriba **t 2** o **event** a fin de conectar la consola al proceso para ver la anotación cronológica local de mensajes del Network Utility:

```
RTP01 *   <Intro>
RTP01 *t 2
00:00:50   GW.001:

Copyright 1984 Massachusetts Institute of Technology,
Copyright 1989 The Regents of the University of California


00:00:50   GW.002: Portable CGW RTP01 Rel NetU-TX1 Feature 1001 V3.1 Mod 0 PTF 1
 RPQ 0 MAS.DE1 netu_38PB
```

```
 strtd
00:00:50   GW.005: Bffrs: 1000 avail 1000 idle   fair 194 low 200
00:00:50  DOLOG: .....Remote Logging Facility is now available.....
```

En este ejemplo, sólo se han anotado cuatro mensajes desde que se arrancó el Network Utility por última vez. Cada mensaje tiene el formato:

- Indicación de la hora en el formato *HH:MM:SS*

  Los 4 mensajes anteriores se han anotado en el mismo segundo, 50 segundos después de que se iniciara el reloj.
- ID de mensaje en el formato *ID.SUBSISTEMA*

  GW.001, GW.002 y GW.005 son mensajes ELS del subsistema GW (GateWay). DOLOG es un tipo de mensaje no estándar incondicional que verá de vez en cuando.
- Cuerpo del mensaje

  El cuerpo de GW.001 son las dos frases de copyright. El cuerpo de GW.002 es la frase de versión de software. Para consultar el significado de un mensaje ELS determinado, consulte la publicación *Guía de mensajes del sistema para el registro cronológico de sucesos* en la Web o en formato de CD-ROM.

A diferencia de los procesos talk 6 y talk 5, el proceso talk 2 no tiene ningún indicador de mandatos de usuario. Ello se debe a que no se escriben mandatos cuando se está en talk 2; simplemente se observa cómo pasan uno tras otro los mensajes a medida que el Network Utility los genera. Puede controlar los mensajes que aparecen habilitando o inhabilitando mensajes individuales o grupos de mensajes bajo el subproceso **event** de talk 6 o talk 5. Consulte el apartado “Supervisión de mensajes de sucesos” en la página 92 para obtener una introducción a los conceptos de ELS y al control de mensajes ELS.

Por lo tanto, bajo talk 2, lo único que escribirá normalmente es **Control-p**, para volver al indicador * y trasladarse a talk 5 o talk 6. Si los mensajes se desplazan demasiado deprisa para poder leerlos, puede utilizar **Control-s** para hacer una pausa en el desplazamiento y **Control-q** para reanudarlo. Para capturar mensajes de sucesos que se mueven rápidamente existen otras opciones que incluyen:

- Activar un archivo de anotaciones cronológicas desde dentro de un programa de emulación de terminal de PC que esté utilizando para la consola
- Desde una estación de trabajo UNIX o AIX, ejecutar Telnet en el Network Utility para obtener la conexión de consola y ejecutar *tee* para la sesión Telnet en un archivo de estación de trabajo local
- Utilizar la posibilidad del Network Utility para anotar mensajes ELS a través de la red en un sistema principal remoto, en lugar de hacerlo en el proceso talk 2 local

Estas opciones se describen detalladamente en el capítulo ″Using the Event Logging System (ELS)″ de la publicación *MAS Guía del usuario de software*.

Al entrar en talk 2, el sistema visualiza todos los mensajes que se han colocado en el almacenamiento intermedio desde la última vez que salió de talk 2. Si el almacenamiento intermedio de mensajes se ha desbordado o el sistema está generando actualmente mensajes más rápidamente de lo que puede visualizarlos, verá líneas intercaladas acerca de ″mensajes desechados″ en la salida de desplazamiento de talk 2.

Si está a punto de entrar en talk 2 y sabe que existe una acumulación de mensajes viejos que deben visualizarse antes de poder ver los mensajes actuales en los que está interesado, utilice el mandato **flush 2** desde el indicador * antes de escribir

talk 2. El sistema elimina la acumulación entera y talk 2 sólo visualiza los mensajes generados después de haber entrado el mandato **flush**.

Escriba **Control-p** para salir de talk 2 y volver al indicador *.

Cómo guardar la configuración y rearrancar

Si ha seguido desde el principio al final los ejemplos de esta guía, ha efectuado los cambios de configuración de talk 6 siguientes desde que empezó:

- Ha añadido dos interfaces
- Ha establecido el nombre de sistema principal
- Ha cambiado la velocidad de Red en Anillo de una interfaz
- Ha cambiado la dirección IP de una interfaz

Nota: También ha habilitado la opción ″fast-boot″, pero este cambio se almacena en la NVRAM y no es pertinente aquí.

En un Network Utility, los cambios de talk 6 se efectúan en realidad en una copia RAM de la configuración. Si desea que dichos cambios sean permanentes y se utilicen con el siguiente rearranque del Network Utility, deberá grabarlos en el disco duro. Existen dos secuencias de mandatos diferentes que pueden llevar a cabo esta tarea:

```
RTP01 *t 6
                <Intro>
RTP01 Config>write
Config Save: Using bank A and config number 3

<empiezan a aparecer mensajes de arranque>

RTP01 Config>   <Control-p>
RTP01 *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes

<empiezan a aparecer mensajes de arranque>
```

..... o .....

```
RTP01 *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 3

<empiezan a aparecer mensajes de arranque>
```

En la primera secuencia, el usuario utiliza el mandato **write** para confirmar cambios en el disco antes del **reload**. En la segunda secuencia, el usuario no utiliza el mandato **write** y el sistema solicita si debe guardar los cambios en el disco antes de continuar con el **reload**.

Puede elegir el método que desee. Muchos usuarios prefieren el segundo método porque hay que pensar y escribir menos, pero también puede ser más fácil olvidar qué cambios se han efectuado en talk 6 si no se emite un **write** inmediatamente después de efectuarlos.

Firmware

Hasta este momento, los ejemplos han arrancado siempre el Network Utility totalmente hasta el software de operación, en el indicador `Config (only)>` o *. Existe otra importante interfaz de usuario de consola que aún no ha visitado, la del *firmware*. Puede que no necesite interactuar demasiado con el firmware, pero deberá estar al corriente del mismo porque proporciona un modo alternativo para cargar código y archivos de configuración en el disco duro y puede proporcionarle una salida de un problema difícil.

El firmware del Network Utility es software de bajo nivel que controla la lógica de encendido y arranque del sistema. Reside en la memoria instantánea en lugar de hacerlo en el disco duro, de modo que en el caso de producirse una anomalía, por ejemplo la corrupción de la carga de software de operación en el disco, puede recuperar software o archivos de configuración nuevos y volver a estar activo y en ejecución.

Para obtener la interfaz de usuario de firmware, la consola de usuario debe realizarse a través de la emulación de terminal ASCII de marcación o local. No puede ejecutar Telnet en la interfaz de usuario de firmware. Para obtener el menú principal de firmware, efectúe un **reload** desde el indicador * y examine los mensajes:

```
  Starting Boot Sequence...
  Strike F1 key now to prematurely terminate Boot
```

Observe con atención porque cada uno de estos mensajes sólo aparece durante unos segundos. Pulse **F1** cuando se le solicite o mantenga pulsadas las teclas **Control-c** antes y durante los mensajes para interrumpir la secuencia de arranque normal y entrar en el firmware.

Después de interrumpir la secuencia de arranque, puede que el sistema le solicite una contraseña de supervisión antes de poder ver el menú principal de firmware. Esta contraseña controla el acceso a funciones de firmware delicadas de bajo nivel. Su valor inicial proporcionado en la fábrica es ″2216″. Sólo puede cambiarlo desde el propio firmware, bajo el menú Utilities.

Si efectúa la marcación en el Network Utility a través de módem para obtener la consola y pierde la conexión durante el **reload**, es posible que no pueda volverse a conectar a tiempo para pulsar **F1**. En este caso, vaya al subsistema **boot** del proceso Config y emita el mandato **disable auto-boot**:

```
*t 6
  Gateway user configuration
  Config>boot
  Boot configuration
  Boot config>dis auto             <----- abreviatura para "disable auto-boot"
  Select the duration to disable autoboot: (once, always) [always] once
  AutoBoot mode is now disabled once.

  Operation completed successfully.
  Boot config>   <Control-p>
  *rel y                           <----- abreviatura para "reload, yes"

  <aparecen mensajes de arranque>
```

Con la modalidad AutoBoot inhabilitada, el sistema detendrá el proceso **reload** en el firmware, sin que tenga que pulsar **F1**. Luego, cuando vuelva a conectarse, estará en el menú principal o en la petición de contraseña de supervisión.

Si siempre inhabilita el arranque automático en talk 6 para obtener el firmware o si no apareciese el indicador de duración (once/always), recuerde que debe volver a habilitarlo al obtener el código de operación o se detendrá en el firmware para cada **reload**.

Al obtener el firmware, verá en la consola de usuario un menú de texto como el que se muestra a continuación:

```
Nways System Firmware
Version 3.00 built on 04/21/98 at 22:18:42 in cc3:paws_netu6e:cc3_6e
(C)Copyright IBM Corporation, 1996, 1998.  All rights reserved.
                            System Management Services

 Select one:
  1. Manage Configuration
  2. Boot Sequence Selection
  3. Select Device to Test
  4. Utilities



     Enter    -    Esc=Quit   -     F1=Help   -    F3=Reboot  -   F9=Start OS
  -------------   -------------   -------------   -------------   ------------
```

La estructura del menú de firmware y sus opciones se describen en la publicación *2216 and Network Utility Service and Maintenance Manual* en el capítulo ″Using 2216 Firmware″. No tendrá que escribir ningún mandato, sino que se moverá por una secuencia de menús seleccionando opciones. Las tareas clave que puede que necesite efectuar desde el firmware son las siguientes:

- Transferir archivos de configuración y software de operación a disco

  Estas funciones son equivalentes a las funciones del subsistema **boot** bajo talk 6. Las encontrará en los menús de firmware bajo ″Utilities″ y luego bajo ″Change Management″.
- Actualizar el firmware propiamente dicho

  Para ello, empiece con ″Utilities″ en el menú principal y, a continuación, ″Update System Firmware″.

Es aconsejable que se desplace un poco por los menús para familiarizarse con ellos. Cuando haya completado cualquier tarea de firmware, pulse **Esc** para volver al menú principal. Utilice una de las opciones siguientes para continuar:

F3=Rearrancar - inicia el proceso de arranque desde el principio. Si tiene inhabilitado el arranque automático, simplemente se detendrá en el firmware otra vez. Si ha marcado, perderá la conexión de nuevo.

F9=Iniciar el OS - continúa el proceso de arranque más allá del firmware hasta entrar en el código de operación.

Ya ha llegado al final de esta guía de la interfaz de usuario del Network Utility. Los capítulos siguientes incluyen otros diversos conceptos y métodos importantes del Network Utility y suponen que el usuario ya ha adquirido los conocimientos proporcionados en este capítulo.

Capítulo 6. Conceptos y métodos de configuración

Este capítulo proporciona información básica sobre la configuración del Network Utility, incluyendo:

- Qué significa configurar el Network Utility
- Los diferentes modos en que se almacena y se transfiere la información de configuración
- Los diferentes métodos disponibles para crear y cambiar configuraciones

El “Capítulo 3. Realización de la configuración inicial” en la página 25 introduce los métodos básicos de configuración del Network Utility y proporciona una guía para elegirlos (consulte el apartado “Elección del método de configuración” en la página 25). Este capítulo proporciona detalles adicionales acerca de cada método y describe la utilización de ambos métodos juntos.

Para conocer procedimientos y mandatos específicos que tratan sobre los archivos de configuración, consulte el “Capítulo 7. Manejo de archivos de configuración” en la página 81. En el “Capítulo 4. Consulta rápida a la interfaz de usuario” en la página 35 se describen algunas tareas de configuración comunes.

Conceptos básicos de configuración

Una configuración de Network Utility es un conjunto de elementos de datos que controlan cómo funciona el software, incluyendo elementos tales como:

- Qué interfaces deben activarse
- Qué enlaces deben arrancarse
- Qué protocolos y características deben dejarse activos
- Qué funciones de una característica o un protocolo determinado deben dejarse activas
- Qué nombres o direcciones de red deben utilizarse

Al arrancar un Network Utility, el sistema lee su configuración en un archivo del disco y activa las interfaces y los protocolos de acuerdo con la información contenida en dicho archivo. El archivo se crea de uno de estos dos modos:

- Utilizando la interfaz de la línea de mandatos desde una consola de terminal de usuario

  Escriba mandatos para crear elementos de datos de configuración en la memoria y, a continuación, grabe la configuración en el disco duro del Network Utility.
- Utilizando un programa de configuración gráfico que se ejecute en un PC o una estación de trabajo

  Cree la configuración en la estación de trabajo y, a continuación, transfiérala al disco duro del Network Utility.

Una vez que el sistema esté activo y en ejecución, puede utilizar la interfaz de la línea de mandatos para efectuar los siguientes tipos de cambios de configuración:

- Cambios que entran en vigor en el sistema en ejecución, pero que no se guardan en un archivo y, por consiguiente, se pierden al rearrancar
- Cambios que entran en vigor en el sistema en ejecución, que también se guardan en un archivo y que, por consiguiente, se mantienen al rearrancar
- Cambios que no entran en vigor en el sistema en ejecución, pero que se guardan en un archivo y sólo se activan al rearrancar

Archivos de configuración en disco

El disco duro del Network Utility está organizado para contener dos *bancos* lógicos, uno para cada una de las dos cargas de código de operación (software). Esto le permite tener la carga de código activa en un banco, transferir una nueva carga al otro banco, probarla y poder retroceder a la carga original si es necesario. Los dos bancos se denominan Banco A y Banco B.

Cada uno de los dos bancos tiene espacio para cuatro archivos de configuración. Puede seleccionar arrancar la carga de código en el Banco A con cualquiera de los 4 archivos de configuración del Banco A. Lo mismo es válido para el Banco B. Para utilizar un archivo de configuración del Banco A con la carga de código del Banco B, primero deberá copiar el archivo de configuración del Banco A en una de las cuatro posiciones de archivo del Banco B.

Existen cuatro modos de transferir un archivo de configuración a un banco del disco duro:

1. Utilizar el mandato de talk 6 **write** para almacenar la configuración actual en la RAM como un archivo de disco.

   Utilice este mandato si está configurando la Network Utility con el proceso de talk 6 de la línea de mandatos, en lugar de hacerlo con el Programa de configuración.

   Nota: Si el término ″talk 6″ no le resulta familiar, utilice el “Capítulo 5. Recorrido por la interfaz de la línea de mandatos” en la página 53 como guía en la interfaz de la línea de mandatos.
2. Utilizar TFTP o Xmodem para transferir el archivo de configuración de un servidor local (PC o estación de trabajo) directamente al disco duro.

   Puede transferir un archivo de configuración, tanto si el archivo se ha creado desde el Programa de configuración como si se ha transferido anteriormente desde este u otro Network Utility.
3. Utilizar SNMP para transferir datos de configuración del Programa de configuración a la RAM y luego al disco duro.

   Inicie la transferencia de archivos desde el Programa de configuración. Este método sólo está disponible desde el Programa de configuración.
4. Copiar un archivo de configuración de un banco al otro.

   Inicie las copias y otras operaciones de gestión de archivos de configuración desde la consola del Network Utility bajo talk 6 en el subproceso **boot**.

Consulte la sección “Carga de archivos de configuración nuevos” en la página 84 en el “Capítulo 7. Manejo de archivos de configuración” en la página 81 para encontrar datos específicos sobre estas operaciones.

Métodos de configuración

Interfaz de la línea de mandatos

Para utilizar la interfaz de la línea de mandatos, arranque primero una consola local o remota en un Network Utility. Para obtener detalles sobre cómo efectuar dicha acción y obtener el indicador * o `Config (only)>`, consulte el “Capítulo 2. Arranque de una consola de usuario” en la página 15.

Si tiene una consola activa en el indicador *, utilice **talk 6** para acceder al proceso Config. Si se encuentra en el `Config (only)>`, el proceso Config es el único proceso que tiene disponible. Desde el proceso Config, navegue por los menús y emita mandatos para configurar interfaces y protocolos y grabe dichos cambios en archivos de configuración en el disco duro del Network Utility.

En la mayoría de los casos, la interfaz de la línea de mandatos se utiliza para configurar solamente el Network Utility al que se está conectado. Pero puede utilizar fácilmente un solo Network Utility para producir archivos de configuración que se deben transferir a otros Network Utilities. Simplemente utilice el mandato **write** bajo talk 6 para almacenar una configuración en un archivo de disco y, a continuación, utilice **tftp put** bajo el subproceso de arranque para transferir el archivo fuera del Network Utility. Desde ese momento, tendrá un archivo que se podrá cargar en el Network Utility de destino igual que si procediera del Programa de configuración.

Quick Config es una opción disponible sólo desde la línea de mandatos. Como se describe en el paso 3 en la página 27, Quick Config le guía en una configuración inicial de un subconjunto de los protocolos del Network Utility. El sistema le hace preguntas en lugar de esperar a que escriba mandatos como sucede en la modalidad normal.

La posibilidad de activar dinámicamente cambios de configuración sin rearrancar el Network Utility es también exclusiva de la interfaz de la línea de mandatos. El apartado “Ejemplo: Reconfiguración dinámica” en la página 68 describía la utilización de talk 5 para activar un cambio de dirección IP efectuado bajo talk 6. El apartado “Reconfiguración dinámica” en la página 77 proporciona más información básica sobre las posibilidades de reconfiguración dinámica del Network Utility.

Programa de configuración

El Network Utility está soportado por el mismo programa de configuración gráfico que se puede utilizar para configurar el 2216-400. Ejecute este programa en un PC o una estación de trabajo y envíe las configuraciones que produzca a uno o más 2216 o Network Utilities. Está disponible una versión del Programa de configuración del 2216/Network Utility para cada uno de los sistemas operativos siguientes:

- Microsoft™ Windows 95 o Windows NT
- IBM AIX
- IBM OS/2

IBM distribuye los principales releases del Programa de configuración en CD-ROM y en la Web. Los PTF de mantenimiento regular sólo están disponibles en la Web. La publicación *Guía del usuario del Programa de Configuración* describe los requisitos del sistema y contiene instrucciones para instalar y utilizar el programa.

Soporte para el Network Utility y el 2216-400

Al iniciar una configuración nueva con el Programa de configuración, éste presenta una lista desplegable para que seleccione si la nueva configuración es para un 2216-400 o para un Network Utility. La elección afecta a lo siguiente:

- El número de ranuras de adaptador que se pueden configurar
- Los tipos de adaptadores que se pueden configurar (el Network Utility soporta un subconjunto de la lista completa de adaptadores 2216)
- Los protocolos y las características que se pueden configurar (el Network Utility soporta un subconjunto de la función MAS completa)

- El valor por omisión para diversos parámetros de ajuste (el Network Utility está preestablecido para las aplicaciones a las que está destinado)

Las configuraciones para el 2216-400 y el Network Utility no son intercambiables.

Formatos de archivo de configuración

El Programa de configuración maneja tres formatos diferentes de archivos de configuración:

- Archivos .CSF: contienen datos en un formato que es nativo del Programa de configuración.

  Utilice este formato con los mandatos del desplegable *Configuration* **Open**, **Save**, **Save as** y **Delete**. El contenido depende del release de software; el Programa de configuración migra automáticamente los elementos de datos al efectuar un **Open**.
- Archivos .CFG: contienen datos en un formato que es nativo del direccionador.

  Utilice este formato cuando desee crear un archivo para transferirlo al direccionador o cuando desee leer un archivo que ha transferido desde un direccionador.
- Archivos .ACF: contienen datos en formato de archivo ASCII plano

  Puede grabar la configuración fuera en un archivo ASCII plano, efectuar cambios en él con un editor de texto y volverlo a leer dentro.

Transferencia y activación de configuraciones

Existen dos modos de transferir una configuración desde el Programa de configuración a un Network Utility:

1. Crear un archivo de formato de direccionador (.CFG), transferirlo (posiblemente utilizando FTP) a un servidor cercano al Network Utility y, a continuación, recuperarlo con Xmodem o TFTP en el disco duro del Network Utility. La configuración se activa al seleccionarla y rearrancar el Network Utility.
2. Inicie una operación ″send″ del Programa de configuración. El Programa de configuración utiliza SNMP para enviar elementos de datos individuales (no un verdadero archivo) al Network Utility. El Network Utility borra la copia de memoria activa de su configuración actual, recibe estos elementos de datos y luego los graba en disco en un archivo nuevo. Antes de efectuar el ″send,″ seleccione en el Programa de configuración si el Network Utility deberá arrancar con la nueva configuración y, si debe arrancar, cuándo debe hacerlo. La configuración enviada sólo se activa al realizar el rearranque.

Tenga en cuenta que con cada método, se transfiere y activa una configuración de Network Utility entera. No existe ningún mecanismo para que el Programa de configuración envíe dinámicamente un pequeño cambio de configuración y lo active en el Network Utility sin necesitar un rearranque del Network Utility. Sólo se puede efectuar este tipo de reconfiguración dinámica utilizando la interfaz de la línea de mandatos.

Otras características del Programa de configuración

Las características del Programa de configuración incluyen:

- Reinicio temporizado

  Cuando utilice el recurso del Programa de configuración para enviar una configuración a un direccionador, puede especificar la fecha y hora en la que desea que el direccionador se reinicie y utilice la configuración.

- Envío a múltiples direccionadores

  Puede crear una lista de direccionadores de destino que recibirán los archivos de configuración, con archivos de configuración iguales o diferentes, horas de reinicio iguales o diferentes, etc. para cada direccionador.
- Recurso de la línea de mandatos

  Puede utilizar la línea de mandatos del sistema operativo de la estación de trabajo, desde la que inicia el Programa de configuración, para automatizar las operaciones de configuración que están disponibles en el programa. Coloque los argumentos en la línea de mandatos original o en un archivo de argumentos y el Programa de configuración los utilizará para dirigir la operación.

  Desde AIX, no es necesario tener instalado el entorno gráfico de sistema operativo (por ejemplo, Xwindows) para utilizar este recurso. Inicie el Programa de configuración utilizando el mandato **headless**.
- Soporte de archivo ASCII

  Puede utilizar el Programa de configuración para crear y leer archivos de configuración en formato ASCII. También puede convertir archivos de configuración de un formato a otro. Un archivo de configuración ASCII puede ser útil si desea modificar muchas configuraciones al mismo tiempo sin tener que cargar las configuraciones en el Programa de configuración. Esta característica no está destinada a ser utilizada para crear nuevas configuraciones o para realizar modificaciones importantes en configuraciones existentes.
- Ayuda en línea

  El Programa de configuración soporta un amplio conjunto de archivos de ayuda. Pulse **F1** cuando esté colocado en cualquier elemento de datos y verá una ventana emergente que describe el elemento y proporciona su valor por omisión así como el rango permitido.

Reconfiguración dinámica

La posibilidad de modificar dinámicamente parámetros de configuración sin rearrancar el Network Utility sólo está disponible desde la interfaz de la línea de mandatos. La Tabla 13 resume los diferentes modos en que se pueden cambiar los parámetros de configuración desde la línea de mandatos e indica si un cambio afecta al sistema en ejecución antes de un rearranque y si el cambio está activo a continuación de un rearranque. La columna ″Elegir grabar en disco″ indica si se ha emitido el mandato **write** desde el menú principal de talk 6 para guardar la configuración en disco o se ha solicitado que se guardara el disco después de emitir el mandato **reload**.

Tabla 13. Opciones de reconfiguración dinámica

Método	Elegir grabar en disco	Afecta al sistema en ejecución	Activo después de rearranque
Cambiar en talk 6	Sí	No (Nota 1)	Sí
	No	No (Nota 1)	No
Cambiar en talk 5	No aplicable	Sí	No
Cambiar en talk 6, luego activar en talk 5 (Nota 3)	Sí	Sí (Nota 2)	Sí
	No	Sí (Nota 2)	No

Tabla 13. Opciones de reconfiguración dinámica (continuación)

Método	Elegir grabar en disco	Afecta al sistema en ejecución	Activo después de rearranque
Nota: 1. La característica Asignador de tareas de red es una excepción a esta regla; los cambios en talk 6 entran en vigor inmediatamente. 2. El cambio entra en vigor al emitir el mandato de activación, no al cambiar el parámetro (a diferencia de un cambio directo en talk 5). 3. El protocolo APPN es una excepción a esta regla; se activan los cambios en talk 6 desde talk 6 en lugar de talk 5.			

Como puede ver, la regla general es que los cambios en talk 6 quedan activos a continuación de un arranque o de un mandato de talk 5 para activarlos. Los mandatos de talk 5 quedan activos inmediatamente pero se pierden al rearrancar.

No todos los elementos de datos de configuración pueden cambiarse de todos los modos descritos más arriba. Ello depende de la parte del sistema (protocolo, interfaz, etc.) a la que pertenece un elemento de datos determinado. Por ejemplo, las configuraciones de DLSw, de SNMP y de ELS soportan todas ellas la mayoría de los mismos mandatos en talk 6 y talk 5. Puede efectuar un cambio en cualquier lugar en función de la permanencia que desee para el cambio. No existe ningún mandato de talk 5 para activar cambios en talk 6, porque ya existe un mandato de talk 5 para efectuar el mismo cambio.

Sin embargo, en IP no existen mandatos de talk 5 correspondientes a los mandatos de talk 6. Utilice **reset ip** en talk 5 para activar la configuración actual de talk 6. La reconfiguración de interfaz también se activa utilizando un solo mandato de talk 5, porque ello implica desactivar y activar la interfaz.

Consulte el apartado “Configuración de interfaces y adaptadores físicos” en la página 40 para obtener unos ejemplos de tareas de reconfiguración dinámicas comunes que incluyen adaptadores e interfaces.

Combinación de métodos de configuración

Si decide utilizar solamente la interfaz de línea de mandatos para la configuración, no necesitará nunca utilizar el Programa de configuración. Si utiliza el Programa de configuración, seguirá necesitando utilizar el proceso Config de la línea de mandatos por varias razones:

- Para algunos protocolos, talk 6 constituye el único modo de ver la configuración del Programa de configuración en un Network Utility activo.
- Existen unos pocos elementos de configuración, por ejemplo mensajes ELS y las direcciones PCMCIA EtherJet, a los que sólo puede acceder talk 6 y a los que no se puede acceder desde el Programa de configuración.
- La línea de mandatos constituye el único modo de efectuar cambios de configuración dinámicos.

Para utilizar una combinación del Programa de configuración y talk 6, deberá mantener el archivo .CSF contenido en el Programa de configuración sincronizado con la información de configuración contenida en el Network Utility. Lo siguiente podría ser un escenario típico:

1. Efectúe la configuración inicial en el Programa de configuración.

2. Transfiera esta configuración al Network Utility, utilizando SNMP o creando un archivo .CFG y transfiriéndolo manualmente.
3. Active, depure y ajuste la configuración en el Network Utility utilizando la interfaz de la línea de mandatos.
4. Vuelva a recuperar la configuración en el Programa de configuración utilizando SNMP o leyéndola en un archivo .CFG.
5. Recupere normalmente la configuración del Network Utility, dado que necesita efectuar cambios de configuración dinámicos.
6. Realice los cambios de red planificados desde el Programa de configuración y envíe las nuevas configuraciones al Network Utility.

Consulte el “Capítulo 7. Manejo de archivos de configuración” en la página 81 para obtener procedimientos específicos para transferir archivos de configuración.

Migración de una configuración a un nuevo release de MAS

De vez en cuando necesitará migrar el Network Utility a un nuevo release de MAS, ya sea para realizar tareas de mantenimiento ya sea para obtener nuevas funciones[9]. Dado que una configuración de Network Utility contiene información específica de release, también deberá actualizar la configuración al nivel del release de MAS que está instalando.

Si utiliza ***sólo*** la interfaz de la línea de mandatos para configurar el Network Utility, simplemente cargue y arranque el nuevo release de MAS utilizando uno de los procedimientos del “Capítulo 10. Mantenimiento de software” en la página 109. Cuando el nuevo release de MAS arranque, ajustará automáticamente la configuración al nivel de release nuevo. Estos ajustes se efectúan en la memoria y no afectan a la copia en disco de la configuración. Puede emitir el mandato **write** en el indicador `Config>` para guardar en disco la configuración actualizada. Puede dejar una copia de la configuración del release anterior en el banco de disco con el nivel anterior de código, por si necesita arrancar desde el release anterior.

Aunque no utilice el Programa de configuración ***en absoluto***, ni tan sólo de vez en cuando, ***deberá*** utilizar el Programa de configuración para actualizar la configuración. Todos los nuevos releases de MAS van acompañados de un nuevo release del Programa de configuración. Siga estos pasos para actualizar la configuración:

1. Utilizando la versión de release anterior del Programa de configuración,
   a. Si es necesario, recupere la configuración del Network Utility en el Programa de configuración. Sólo necesitará realizar dicha acción si ha efectuado cambios de línea de mandatos en la configuración desde la última vez que la envió desde el Programa de configuración al Network Utility.
   b. Guarde la configuración como un archivo .CSF (el formato interno del Programa de configuración), utilizando **Save** o **Save as** desde el menú desplegable **Configure**.
2. Utilizando la versión de release nueva del Programa de configuración,
   a. Abra la configuración utilizando **Open** desde el menú desplegable **Configure**. La nueva versión del Programa de configuración actualiza automáticamente la configuración al nuevo release a medida que lo lee.
   b. Guarde la versión de release nueva de la configuración.

9. Consulte el “Capítulo 10. Mantenimiento de software” en la página 109 para obtener información básica y procedimientos relacionados con la actualización de código.

c. Transfiere la nueva versión de release de la configuración al Network Utility y actívela al arrancar el nuevo release de MAS.

Capítulo 7. Manejo de archivos de configuración

Este capítulo describe procedimientos específicos para:
- Ver y gestionar archivos de configuración en el disco duro de un Network Utility
- Transferir archivos de configuración desde fuera del Network Utility al disco duro de éste
- Transferir archivos de configuración desde el disco duro del Network Utility

Para obtener información básica acerca de la configuración del Network Utility, consulte el “Capítulo 3. Realización de la configuración inicial” en la página 25 y el “Capítulo 6. Conceptos y métodos de configuración” en la página 73.

Para obtener detalles acerca de los mandatos individuales introducidos en este capítulo, consulte los capítulos siguientes de la publicación *MAS Guía del usuario de software*:
- ″Using BOOT Config to Perform Change Management″
- ″Configuring Change Management″

Gestión de archivos de configuración en disco

Todos los mandatos para listar y gestionar archivos de configuración en el disco duro del Network Utility están ubicados en el subproceso de arranque Config. El ejemplo siguiente muestra cómo obtener este subproceso y listar los mandatos disponibles:

```
*t 6
                <Intro>
Config>boot
Boot configuration
Boot config>?
ADD description
COPY software
DESCRIBE software VPD
DISABLE boot choices
ENABLE boot choices
ERASE software
LIST software status
LOCK Config File
SET boot information
TFTP software
TIMEDLOAD software
UNLOCK Config File
UPDATE Firmware
EXIT
Boot config>
```

Listado de configuraciones

El mandato **list** es el punto de partida para ver qué archivos de configuración existen en las cuatro posiciones de cada uno de los dos bancos de carga de código. Esta mismo pantalla se integra en diversos mandatos del menú.

```
Boot config>li
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 03 Aug 1998 10:04 |
| CONFIG 1 - AVAIL       |                                 | 04 Aug 1998 13:50 |
| CONFIG 2 - ACTIVE  *   | example config 1                | 04 Aug 1998 13:52 |
| CONFIG 3 - AVAIL       |                                 | 04 Aug 1998 06:41 |
| CONFIG 4 - AVAIL       |                                 | 04 Aug 1998 09:43 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
```

```
| IMAGE - PENDING        |                                 | 05 Aug 1998 03:41 |
| CONFIG 1 - PENDING *   |                                 | 31 Jul 1998 12:59 |
| CONFIG 2 - AVAIL       |                                 | 31 Jul 1998 09:50 |
| CONFIG 3 - AVAIL       |                                 | 31 Jul 1998 09:52 |
| CONFIG 4 - AVAIL       |                                 | 31 Jul 1998 12:50 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

 Auto-boot mode is enabled.   Fast-boot mode is enabled.

Time Activated Load Schedule Information...

The load timer is not currently activated.
Boot config>
```

Los estados de imagen (carga de código) y configuración se definen del modo siguiente:

ACTIVE
: Se ha utilizado el archivo para el arranque actual del Network Utility

AVAIL Se trata de un archivo válido que puede pasar a estar activo (ACTIVE).

CORRUPT
: El archivo no es utilizable. Normalmente esto sucede porque no se ha completado satisfactoriamente una transferencia de archivos a esta posición.

LOCAL
: El archivo sólo se utilizará en la carga o el restablecimiento siguiente. Una vez utilizado, el archivo pasará a estar en estado disponible (AVAIL).

NONE No existe ningún archivo en esta posición (el estado inicial).

PENDING
: El archivo se utilizará en la recarga, el restablecimiento o el encendido siguiente del Network Utility.

Para recordar qué hay en un archivo de configuración determinado, utilice el mandato **add** para entrar una breve descripción.

Cómo activar una configuración

Para hacer que un archivo de configuración determinado pase a estar activo, deberá convertirlo en el archivo de configuración pendiente (PENDING) del banco con la carga de código activa (ACTIVE) o pendiente (PENDING) y, a continuación, rearrancar el Network Utility. Esto se realiza del modo siguiente cuando el archivo ya existe o cuando se crea:

- Si el archivo ya está en disco, utilice el mandato **set** para designar el banco y la posición del archivo de configuración a utilizar para el siguiente arranque.

  Puede especificar si el nuevo valor del banco de origen y de la configuración es simplemente para el siguiente arranque (el estado pasa a ser LOCAL) o para todos los arranques futuros (el estado pasa a ser pendiente (PENDING)).

  Normalmente utilizará el mandato **set** después de transferir un archivo al disco utilizando TFTP o Xmodem.

- Si crea un archivo nuevo utilizando el mandato **write** de talk 6, dicho archivo se convertirá automáticamente en la configuración pendiente (PENDING) en el banco activo (ACTIVE).

  Al efectuar un **write**, el sistema graba la configuración de la memoria activa en la siguiente posición desbloqueada del banco activo (ACTIVE), alternando en secuencia. La posición del archivo no se elige. Si desea evitar que se grabe encima de un archivo determinado, utilice el mandato **lock**.

Dado que el archivo nuevo pasa a estar pendiente (PENDING), puede efectuar un **write** seguido de un **reload** sin prestar atención a la posición concreta utilizada y sin tener que emitir el mandato **set**.

- Si crea un archivo de forma implícita escribiendo **reload** y eligiendo guardar los cambios de configuración, el nuevo archivo se convertirá en la configuración pendiente (PENDING) antes de que continúe el rearranque.

  La secuencia siguiente produce el mismo resultado que si se emite el mandato **write**:

  ```
  *rel y
  The configuration has been changed, save it? (Yes or [No] or Abort):yes
  ```

- Si crea un archivo utilizando la opción **Communicate** del Programa de configuración para transferir directamente una configuración, el nuevo archivo se convertirá en la configuración pendiente (PENDING).

  Esto también funciona igual que si se emite el mandato **write**. Si solicita un rearranque desde el Programa de configuración, esta configuración se activará cuando se produzca el rearranque.

Activación retardada

Existen dos procedimientos para producir una activación temporizada, probablemente desatendida, de una configuración:

- Si está utilizando el Programa de configuración y transfiere la configuración utilizando la opción **Communicate**, puede especificar la fecha y hora en la que el Network Utility deberá rearrancar y activar la configuración.
- Independientemente del método que haya utilizado para crear un archivo de configuración en el disco duro del Network Utility, puede utilizar el mandato **timedload** en el subproceso de arranque Config para planificar una fecha y hora para que el Network Utility rearranque y active una carga de código y una configuración especificadas.

  Si elige la carga de código y configuración actuales, esta función se convierte simplemente en una operación de recarga planificada.

Programas de utilidad de archivo

El subproceso de arranque Config proporciona diversos mandatos de programa de utilidad para gestionar los archivos de configuración (y cargas de código) en disco:

add para entrar una breve descripción de una configuración

copy para copiar una configuración entre bancos y/o posiciones de archivo

erase para eliminar un archivo de configuración y volver a dejar el estado de posición en NONE

lock para impedir que uno de los métodos de creación de archivos se grabe encima del archivo

unlock
para permitir que se utilice otra vez una posición de archivo para un archivo nuevo

Gestión de cambios de firmware

La mayoría de las funciones de gestión de configuración del subproceso de arranque Config también están disponibles en los menús de firmware del Network Utility. Para acceder a ellas, seleccione la secuencia siguiente empezando desde el menú principal de firmware:

- Opción 4, ″Utilities″
- Opción 12, ″Change Management″

Carga de archivos de configuración nuevos

La Tabla 14 resume los modos en que se puede transferir una configuración desde fuera a la unidad de disco duro del Network Utility. SNMP implica una transferencia directa desde el Programa de configuración al Network Utility, mientras que TFTP y Xmodem necesitan que el archivo de configuración esté en una estación de trabajo que actúe como servidor de archivos para el Network Utility.

El método elegido para transferirla al Network Utility dependerá de cómo pueda conectarse al Network Utility, de si está utilizando el Programa de configuración, del software que tenga en la estación de trabajo y de sus propias preferencias. Normalmente, los archivos de configuración del Network Utility son suficientemente pequeños para que los tiempos de transferencia a través de módems de baja velocidad sean razonables.

Tabla 14. Carga de configuraciones

Conexión física	Protocolo de línea	Protocolo de transferencia	Herramienta	Direcciones IP por omisión
Puerto de servicio + módem nuloPuerto de servicio + módem ext Módem PCMCIA	Terminal asínc	Xmodem	Firmware	No aplicable
	SLIP	TFTP	Código-op	Network Utility=10.1.1.2 Estación de trabajo=10.1.1.3
		SNMP	Cfg pgm	
PCMCIA EtherJet LIC Ethernet (10 Mbps) LIC Red en Anillo	IP	TFTP	Código-op Firmware	Network Utility=10.1.0.2 Estación de trabajo=10.1.0.3
		SNMP	Cfg pgm	
Cualquier interfaz de red IP	IP	TFTP	Código-op	Ningún valor por omisión
		SNMP	Cfg pgm	

Las secciones siguientes resumen cada uno de los procedimientos de transferencia de configuración posibles, agrupándolos por la herramienta desde la que se inicia la transferencia.

Utilización del Programa de configuración

Existen dos modos de transferir una configuración del Programa de configuración a un Network Utility.

1. Crear un archivo de configuración de direccionador y luego utilizar el código de operación o firmware del Network Utility como la herramienta desde la que deberá realizar la transferencia.
2. Utilizar SNMP para transferir la configuración a la memoria y al disco duro del Network Utility.

Exportación de un archivo de configuración de direccionador

Después de haber iniciado el Programa de configuración y de haber creado una configuración de Network Utility, vaya a la ventana de navegación (Navigation Window) y:

1. Active el menú desplegable **Configure** y seleccione **Create router configuration**.
2. Elija la vía de acceso de directorio y el nombre de archivo en la estación de trabajo en la que está ejecutando el Programa de configuración, donde desea que se almacene el archivo de configuración de direccionador (.cfg).
3. Pulse en **OK**. El Programa de configuración graba este archivo en disco.
4. Seleccione **Save as** bajo **Configure** para guardar también la configuración en formato .csf, el formato preferido para archivar.

Entonces es responsabilidad suya cargar el archivo en el Network Utility, utilizando el código de operación o el firmware para efectuar la carga. Puede seguir cualquiera de los procedimientos descritos en el apartado “Utilización del código de operación” en la página 86 o el apartado “Utilización del firmware” en la página 88.

Si la estación de trabajo o el PC de Programa de configuración no puede ser el servidor TFTP o Xmodem para la transferencia de archivos en estos procedimientos, deberá trasladar primero el archivo .cfg a una estación de trabajo que pueda actuar de servidor. Puede utilizar cualquier método de transferencia de archivos, por ejemplo FTP, para trasladar el archivo de una estación de trabajo a otra.

Envío directo utilizando SNMP

Para utilizar la transferencia SNMP, deberá configurar el Network Utility con una dirección IP y habilitar SNMP con un nombre de comunidad de lectura-grabación. Cada una de las configuraciones de ejemplo de la “Parte 2. Introducción al Network Utility” en la página 49 muestra cómo configurar una dirección IP y SNMP para esta comunicación, en el Programa de configuración y desde talk 6.

Si desea utilizar SNMP para bajar la primera de las configuraciones del Network Utility, consulte el apartado “Procedimiento B: Configuración inicial del Programa de configuración” en la página 29.

Si ésta no es la primera configuración, asegúrese de que existe al menos una posición de archivo de configuración desbloqueada (distinta de la activa) en el banco de código actualmente activo del disco duro. (Consulte el apartado “Listado de configuraciones” en la página 81 para obtener más información).

Después de haber creado una configuración de Network Utility en el Programa de configuración, utilice el procedimiento siguiente para transferir dicha configuración al Network Utility utilizando SNMP:

1. Active el menú desplegable **Configure** y seleccione **Communications**.
2. En la ventana emergente, seleccione **Single router** si sólo desea enviar la configuración actual a un Network Utility o **Multiple routers** si desea enviar cualquier configuración guardada a cualquier número de direccionadores de destino.
3. En el siguiente panel de un solo direccionador o el panel de lista de múltiples direccionadores, seleccione la opción **Send** y entre la información de direccionamiento necesaria para los direccionadores.

Si lo desea, también puede entrar una fecha y hora para que se reinicie el direccionador con esta configuración. Existen dos modos de efectuar dicha acción:

a. Seleccione **Send** y **Restart router**[10]

   El direccionador almacena la hora de reinicio en la memoria volátil, de modo que si el Network Utility rearranca antes de la hora planificada, la configuración se activa antes.

   Si entra una fecha o una hora que ya ha pasado, el direccionador activará la nueva configuración inmediatamente.

b. Seleccione **Timed config**

   El direccionador almacena la hora de reinicio en la memoria no volátil, de modo que si el Network Utility rearranca antes de la hora planificada, utiliza la configuración actual. La configuración recién bajada no se activará hasta que llegue la hora de reinicio planificada.

   Si entra una fecha o una hora que ya ha pasado, el direccionador almacenará la nueva configuración en disco pero no la activará. Si hay una operación de reinicio ″timed config″ anterior pendiente, ésta se cancelará.

Al establecer la fecha y hora mediante uno de estos métodos no es necesario sincronizar esta fecha y hora con el Network Utility ni tampoco establecer una fecha y hora en el Network Utility. El Programa de configuración convierte la fecha y hora establecidas en un intervalo de tiempo y envía dicho valor al Network Utility.

4. Pulse en **OK** (o **Run** para obtener la lista de múltiples direccionadores) y el Programa de configuración empezará a enviar elementos de datos de configuración al (a los) direccionador(es) especificado(s) utilizando SNMP. El envío empieza de inmediato, independientemente de que se haya especificado una fecha y hora posteriores para que rearranquen los direccionadores de destino.
5. El Programa de configuración proporciona mensajes de estado y resultado acerca de la transferencia. Si tiene problemas y está efectuando el envío a un solo direccionador, es aconsejable que pruebe con el botón **Query router information** en lugar de **Send**. Esta opción recupera una pequeña cantidad de información del direccionador. Puede utilizarla para ver si tiene una vía de acceso de comunicación SNMP al direccionador.

Cuando un direccionador empieza a recibir una configuración mediante SNMP, dicha configuración sustituye cualquier cambio de talk 6 efectuado desde el último rearranque. Cuando la transferencia se ha completado, el Network Utility graba en disco la configuración recibida y la activa basándose en lo seleccionado al iniciar la operación de envío.

Utilización del código de operación

Puede utilizar el código de operación para obtener un archivo de configuración que se ha creado de uno de estos dos modos:

- Se ha exportado del Programa de configuración utilizando el paso 1 en la página 84
- Se ha transferido anteriormente desde este u otro Network Utility

10. También puede efectuar un **Send**, seguido posteriormente de una operación manual **Restart router**.

Tal como muestra la Tabla 14 en la página 84, todos los procedimientos de transferencia de configuración que se pueden iniciar desde el código de operación (código-op) utilizan TFTP como protocolo de transferencia de archivos.

Utilización de TFTP

El procedimiento de código-op para utilizar TFTP para transferir un archivo de configuración al disco duro del Network Utility es:

1. Coloque el archivo de configuración en una estación de trabajo que tenga instalado software de servidor TFTP y esté conectada físicamente al Network Utility en red IP.
2. Acceda al menú principal de firmware utilizando el procedimiento descrito en el apartado “Opciones de arranque: Arranque rápido y obtención de firmware” en la página 46.
3. Configure las direcciones IP que va a utilizar.

   Si está utilizando una interfaz de red estándar que incluye un adaptador Ethernet o de Red en Anillo, utilice el Programa de configuración o talk 6 para configurar una dirección IP para la interfaz del modo normal. (Desde talk 6, utilice **add address** en el subproceso IP). Active este cambio de configuración antes de continuar.

   Si está utilizando la tarjeta PCMCIA EtherJet, use **system set ip** para establecer las direcciones siguientes:
   - Dirección IP: dirección IP para la tarjeta EtherJet
   - Máscara de red: máscara para la subred conectada a la tarjeta EtherJet
   - Dirección de pasarela: dirección IP para la estación de trabajo servidor TFTP

   Si está utilizando SLIP, no puede cambiar las direcciones IP sino que debe utilizar las que se proporcionan en la Tabla 14 en la página 84.
4. Transfiera los archivos

   Desde el indicador *, siga esta secuencia:

   ```
   *t 6
   Config>boot
   Boot configuration
   Boot config>tftp get config
   ```

   Responda a las solicitudes del modo siguiente:
   - Dirección IP de servidor: Ponga la dirección de la estación de trabajo servidor TFTP.
   - Directorio remoto: Ponga el nombre de vía de acceso al directorio de la estación de trabajo servidor donde está el archivo de configuración. Utilice barras inclinadas en la dirección esperada por el servidor. La escritura en mayúsculas y en minúsculas sólo tiene importancia si también tiene importancia en el servidor.
   - Banco de destino: Seleccione el banco A o banco B.
   - Configuración de destino: Seleccione una posición desbloqueada entre 1 y 4.

   Basándose en la dirección IP de servidor y las direcciones IP de interfaz de Network Utility configuradas, el Network Utility seleccionará la interfaz que va a utilizar para comunicarse con el servidor. El Network Utility indicará mediante mensajes de estado si la operación ha sido satisfactoria o anómala según sea apropiado.
5. Rearranque o planifique un rearranque para utilizar la configuración.

   Para activar la nueva configuración inmediatamente, siga el procedimiento siguiente desde el indicador `Boot Config>`:

a. Utilice el mandato **set** a fin de seleccionar la nueva configuración para que se utilice para el siguiente rearranque.
b. Pulse **Control-p** y, a continuación, entre **reload** para rearrancar el Network Utility

Para activar la nueva configuración posteriormente, escriba **timedload activate** desde el indicador `Boot config>` para seleccionar el banco y la nueva configuración y especificar la fecha y hora de rearranque del Network Utility. Puede responder ″no″ a las preguntas sobre carga, porque ya ha realizado este paso.

Consulte en la publicación *MAS Guía del usuario de software* el capítulo ″Configuring Change Management″ para obtener más información sobre los mandatos del procedimiento anterior.

Utilización del firmware

Puede utilizar el firmware para obtener un archivo de configuración que se ha creado de uno de estos dos modos:
- Se ha exportado desde el Programa de configuración utilizando el paso 1 en la página 84
- Se ha transferido anteriormente desde este u otro Network Utility

Tal como muestra la Tabla 14 en la página 84, el firmware soporta los protocolos de transferencia de archivos XMODEM y TFTP.

Utilización de Xmodem

El procedimiento de firmware para transferir un archivo de configuración al disco duro del Network Utility mediante el uso de Xmodem es el siguiente:

1. Coloque el archivo de configuración en la estación de trabajo con el software de emulación de terminal que soporte la sesión actual de consola de usuario.
2. Acceda al menú principal de firmware utilizando los procedimientos descritos en el apartado “Opciones de arranque: Arranque rápido y obtención de firmware” en la página 46.
3. Realice las selecciones de menú en la secuencia siguiente:
   a. System Management Services (menú principal): Opción 4, ″Utilities″
   b. System Management Utilities: Opción 12, ″Change Management″
   c. Change Management Software Control: Opción 12, ″Xmodem software″
   d. Select Type: ″Config″
   e. Select Bank: elija Bank A (Banco A) o Bank B (Banco B)
   f. Select Config: elija una posición desbloqueada

   El firmware le indica cuándo debe iniciar la transferencia de archivos.
4. Vaya al paquete de emulación de terminal e inicie la transferencia del archivo desde el servidor de estación de trabajo, utilizando el nombre que desee. Al iniciar la transferencia, el estado de la posición de archivo cambia a CORRUPT, para indicar que no contiene un archivo de configuración completo. Cuando se completa la transferencia, dicho estado cambia a AVAIL. Puede verificarlo utilizando la opción 7, ″List Software″ del menú de firmware Change Management.
5. Arranque el Network Utility utilizando la configuración que acaba de cargar.

Utilice la opción 9 ″Set Boot Information″ para seleccionar el banco de código de operación actual y la nueva configuración. Pulse **Esc** para obtener el menú principal y, a continuación, **F9** para arrancar el Network Utility con la nueva configuración.

Utilización de TFTP

El procedimiento de firmware para utilizar TFTP para transferir un archivo de configuración a un disco duro de Network Utility es el siguiente:

1. Coloque el archivo de configuración en una estación de trabajo que tenga instalado software de servidor TFTP y esté conectada físicamente al Network Utility en red IP.
2. Acceda al menú principal de firmware utilizando los procedimientos descritos en el apartado “Opciones de arranque: Arranque rápido y obtención de firmware” en la página 46.
3. Configure las direcciones IP que va a utilizar:

   Siga la secuencia de menús:
   a. System Management Services (menú principal): Opción 4, ″Utilities″
   b. System Management Utilities: Opción 11, ″Remote Initial Program Load Setup″
   c. Parámetros de red: Opción 1, ″IP Parameters″

   Establezca las direcciones siguientes:
   - Dirección IP de cliente: dirección IP para la tarjeta de LAN del Network Utility. Ésta es una dirección temporal que no necesita estar relacionada con la dirección de operación del Network Utility para esa interfaz.
   - Dirección IP de servidor: dirección IP del adaptador de LAN de la estación de trabajo
   - Dirección IP de pasarela: dirección IP de cualquier direccionador intermedio o, si no hay ninguno, repita la dirección IP de la estación de trabajo
   - Máscara de red: máscara para la subred conectada a la tarjeta de LAN del Network Utility
4. Inicie la transferencia mediante estas selecciones de menú:
   a. System Management Services (menú principal): Opción 4, ″Utilities″
   b. System Management Utilities: Opción 12, ″Change Management″
   c. Change Management Software Control: Opción 10, ″TFTP software″
   d. Select Type: ″Config″
   e. Select Bank: elija Bank A (Banco A) o Bank B (Banco B)
5. Entre la vía de acceso y el nombre del archivo de configuración de la estación de trabajo
6. Si se le solicita, seleccione la interfaz mediante la cual desea que el firmware efectúe la transferencia de archivos.

   El firmware transfiere el archivo de configuración y proporciona mensajes de estado. Cuando haya terminado, volverá al menú Change Management.
7. Arranque el Network Utility utilizando la configuración que acaba de cargar

   Utilice la opción 9, ″Set Boot Information″, para seleccionar el banco de código de operación actual y la nueva configuración. Pulse **Esc** para obtener el menú principal y, a continuación, **F9** para arrancar el Network Utility con la nueva configuración.

Transferencia de archivos de configuración desde el Network Utility

Puede que desee transferir un archivo de configuración ***desde*** un Network Utility por cualquiera de las razones siguientes:

- Está utilizando la configuración de línea de mandatos y desea hacer una copia de seguridad de la configuración en alguna parte distinta del disco duro del Network Utility.
- Está utilizando la configuración de línea de mandatos y desea exportar el archivo de configuración a otro Network Utility.
- Está utilizando el Programa de configuración y la configuración de línea de mandatos y desea actualizar el archivo de Programa de configuración con cambios recientes de talk 6 (por ejemplo, cambios de reconfiguración dinámicos).

Para todos los procedimientos de código de operación para transferir una configuración a un Network Utility, existe un procedimiento inverso para transferir una configuración desde un Network Utility. Los pasos son casi idénticos, de modo que el procedimiento siguiente lista sólo las diferencias esenciales.

1. Importe un archivo .CFG al Programa de configuración.

   Transfiera el archivo .CFG a la estación de trabajo de Programa de configuración. Efectúe una operación **Read router configuration** en lugar de una operación **Create router configuration**.
2. Utilice SNMP para transferir una configuración al Programa de configuración. Efectúe una operación **Retrieve configuration** en lugar de una operación **Send configuration**.
3. Utilice el TFTP de código de operación para enviar una configuración desde el Network Utility. Escriba **tftp put config** en lugar de **tftp get config**.

No existen procedimientos basados en firmware para transferir una configuración desde un Network Utility.

Capítulo 8. Conceptos y métodos de gestión

Esta publicación utiliza el término *gestión* para indicar todos los modos en que se puede supervisar y controlar lo que está sucediendo en un Network Utility activo. Estos modos incluyen:

- Escritura de mandatos en una consola local o remota para consultar el estado y cambiar el estado de las interfaces y los protocolos
- Supervisión de una anotación cronológica de mensajes de sucesos en ejecución, a través de la misma consola o en un servidor para la anotación cronológica remota
- Utilización de un navegador MIB SNMP para consultar el estado de las interfaces y las funciones del sistema que tienen soporte MIB SNMP asociado
- Utilización de un producto de gestión basado en SNMP y sus aplicaciones para supervisar y controlar interfaces y las funciones del sistema que tienen asociado soporte MIB SNMP
- Utilización de aplicaciones de topología basada en SNMP para supervisar una vista específica de protocolo (por ejemplo, APPN o DLSw) de la red y sus recursos
- Utilización de un producto de gestión basado en SNMP para supervisar trampas SNMP enviadas por el sistema para informar de condiciones de error
- Utilización de un producto de punto focal de alerta SNA (por ejemplo NetView/390) para supervisar alertas SNA enviadas por el sistema para informar de condiciones de error
- Utilización de un producto de gestión SNA (por ejemplo NetView/390) para controlar recursos SNA

Este capítulo proporciona una visión general de estos métodos e introduce algunos de los demás productos que puede utilizar para gestionar el Network Utility.

Mandatos de consola

Para entrar los mandatos que permiten consultar y cambiar el estado del sistema, primero deberá arrancar una conexión de consola local o remota a un Network Utility activo. Para obtener detalles sobre cómo efectuar dicha acción y obtener el indicador *, consulte el “Capítulo 2. Arranque de una consola de usuario” en la página 15.

Una vez que tenga una consola activa, utilice talk 5 para acceder al proceso Console. [11] Desde allí, navegue por los menús y emita mandatos para consultar el estado de las interfaces y los protocolos así como para efectuar cambios de operador dinámicos tales como:

- Inhabilitar y habilitar interfaces
- Reciclar conexiones
- Activar cambios de configuración

Consulte el apartado “Operación (Utilizando talk 5, el proceso Console)” en la página 63 para obtener una visión general de los mandatos de talk 5 y de los tipos de estado que puede ver y cambiar desde la consola de operador. En el capítulo ″The Operating/Monitoring Process (GWCON - Talk 5) and Commands″ de la

11. Si se conecta a un Network Utility que no se ha configurado nunca anteriormente, estará en modalidad de sólo configuración (Config-only) y no podrá entrar en el proceso Console de talk 5. Siga las instrucciones del “Capítulo 3. Realización de la configuración inicial” en la página 25 para configurar el Network Utility por primera vez y arrancar en modalidad de operación normal.

publicación *MAS Guía del usuario de software* se proporcionan detalles completos sobre los mandatos de nivel superior de talk 5.

Mediante la utilización de los mandatos de talk 5 **net**, **protocol** y **feature**, puede entrar en la estructura de menús y utilizar mandatos para supervisar y controlar interfaces así como características y protocolos determinados. Los mandatos de nivel de interfaz de talk 5 se documentan en la publicación *MAS Guía del usuario de software* en los capítulos dedicados a los diferentes tipos de interfaces. Los mandatos de protocolos y características de talk 5 se describen en varios capítulos de la publicación de dos volúmenes *MAS Consulta de configuración y supervisión de protocolos* así como en la publicación *MAS Utilización y configuración de las características*.

Supervisión de mensajes de sucesos

¿Por qué supervisar los sucesos?

Los mandatos de Talk 5 proporcionan una instantánea del estado del Network Utility, pero no pueden producir una anotación cronológica o un rastreo de los sucesos que tienen lugar en el interior del sistema. Para ello utilice el ELS (Event Logging System) (Registro cronológico de sucesos). Mediante la activación de los mensajes ELS correctos y la supervisión de la anotación cronológica de sucesos, puede seguir en tiempo real sucesos tales como los siguientes:

- Interfaces que pasan por fases de prueba, que se activan y se desactivan
- Paquetes de un protocolo determinado que se están enviando y recibiendo
- Enlaces DLC que se activan y desactivan
- Cambio de utilización de CPU en respuesta a la actividad de red
- Conexiones de protocolo de nivel superior (por ejemplo, conexiones de circuito y asociado DLSw) que se activan y desactivan

Mediante la supervisión de los mensajes ELS, puede empezar a responder a algunas preguntas básicas, por ejemplo:

- ¿Está sucediendo algo?
- ¿Por qué no se activa el enlace?
- ¿Detecta mi protocolo el tráfico que está enviando una estación de trabajo?

El Event Logging System es una potente herramienta para depurar problemas básicos de configuración.

Especificación de los sucesos a anotar

Para utilizar los mensajes ELS, primero indique al sistema cuáles son los sucesos de los que desea recibir información entre los miles de sucesos predefinidos. Puede especificar el conjunto de mensajes activos utilizando los criterios siguientes:

Nombre de subsistema
: Puede hacer referencia a todos los mensajes posibles de un componente de software utilizando el nombre abreviado predefinido de dicho componente, por ejemplo IP, TKR o DLS.

Número de suceso
: Puede activar o desactivar mensajes individuales o especificar un rango de números de sucesos. A veces resulta útil activar todos los mensajes de un

subsistema y luego desactivar unos cuantos mensajes especialmente frecuentes dentro de dicho subsistema, para evitar que se oculten mensajes más críticos.

Nivel de anotación cronológica
Puede especificar el nivel de gravedad de los mensajes que desea ver. Por ejemplo, puede que sólo desee ver mensajes de error inusuales o sólo mensajes de rastreo o bien incluir mensajes informativos simples.

Nombre de grupo
Puede especificar el nombre que ha elegido anteriormente al definir un grupo de mensajes.

Además, puede definir filtros en un número de interfaz lógica, de modo que, para cualquier conjunto activo de mensajes, sólo aparezcan en la anotación cronológica aquéllos relacionados con una interfaz determinada.

Especificación del lugar donde anotar sucesos

Al activar mensajes, elija uno de los destinos siguientes para el mensaje:

1. El proceso Monitor

   Para ver los mensajes enviados a este proceso utilice el mandato de **talk 2** desde el indicador *. Consulte el apartado “Anotación cronológica de sucesos (Utilizando talk 2, el proceso Monitor)” en la página 68 para obtener una introducción a la utilización del proceso Monitor.
2. Un servidor remoto de anotación cronológica

   Puede definir cualquier PC o estación de trabajo que soporte un recurso *syslog* estándar para recibir un flujo de paquetes de mensajes de sucesos y guardarlos en un archivo. El Network Utility envía cada mensaje en un paquete UDP/IP a través de una interfaz de red estándar. Dado que el flujo de mensajes de anotación cronológica puede ser muy intenso, normalmente un servidor de anotación cronológica se conecta mediante una LAN al Network Utility.
3. Una trampa SNMP, enviada a una estación de gestión SNMP

   El Network Utility empaqueta el mensaje de suceso en una trampa SNMP específica de empresa de IBM y lo envía en un paquete UDP/IP a través de una interfaz de red estándar.

Activación de la anotación cronológica de sucesos

Desde la línea de mandatos, puede utilizar talk 6 o talk 5 para seleccionar los sucesos que desea anotar y el lugar donde desea anotarlos. Desde cualquiera de los dos procesos, entre en el subproceso **event** para continuar. Si activa sucesos bajo talk 6, los cambios no entrarán en vigor hasta que los grabe en disco y rearranque el Network Utility. Los mensajes para estos sucesos estarán continuamente activos a partir del primer rearranque.

Si activa sucesos desde talk 5, el sistema empieza inmediatamente a generar mensajes para dichos sucesos en el destino especificado (talk 2, el servidor de anotación cronológica o la estación de gestión SNMP). Al rearrancar el Network Utility, dichos mensajes dejan de estar activos. La utilización de talk 5 para activar sucesos es un buen modo de depurar un problema inmediato que pueda tener. Active los sucesos, pase rápidamente a talk 2 para ver qué está sucediendo, etc. Cuando posteriormente efectúe un rearranque, los sucesos se desactivarán sin que tenga que entrar ningún mandato nuevo.

Otra técnica útil de depuración consiste en utilizar el subproceso event de talk 5 para ver estadísticas sobre el número de veces que se ha encontrado cualquier suceso. Estas estadísticas están disponibles incluso para sucesos que no se han activado.

No existe ningún mandato de talk 5 para activar la configuración ELS de talk 6 actual. Si desea la activación inmediata, deberá repetir en talk 5 los mismos mandatos que ha entrado en talk 6.

Desde el Programa de configuración, sólo puede configurar el Network Utility para realizar la anotación cronológica remota en un sistema principal. No puede configurar qué sucesos ELS están activos o dirigir sucesos ELS a un destino determinado. Aunque el Programa de configuración conserva esta información de configuración, si recupera una configuración de un Network Utility, debe modificar otras partes de la configuración utilizando el Programa de configuración y grabar la restitución de la configuración.

Desde una estación de gestión de SNMP, puede utilizar SET para controlar la mayoría de las funciones de configuración ELS que utilizan un MIB ELS específico de empresa.

Algunos de los mandatos clave para activar y controlar sucesos ELS, se presentan en el apartado “Supervisión de sucesos” en la página 103. Para obtener una explicación detallada de los conceptos ELS y los mandatos de talk 6 y talk 5 asociados, consulte la publicación *MAS Guía del usuario de software* capítulo ″Configuring and Monitoring the Event Logging System (ELS)″. Para obtener la descripción de cada mensaje ELS individual, consulte la publicación *Guía de mensajes del sistema para el registro cronológico de sucesos* en CD-ROM o en la Web.

Soporte de Simple Network Management Protocol (SNMP)

SNMP es un protocolo estándar de la industria que utilizan las estaciones de gestión para consultar y establecer información de configuración, control y estado en un nodo gestionado. En el contexto de Network Utility, la estación de gestión sería normalmente un PC o una estación de trabajo con un producto de software de gestión SNMP instalado. El nodo gestionado sería el Network Utility.

Entre la estación de gestión y el nodo gestionado fluyen peticiones y respuestas de SNMP dentro de paquetes UDP a través de una red IP. En general, la estación de gestión inicia la comunicación enviando peticiones de información y peticiones para establecer elementos de datos en nuevos valores. El nodo gestionado simplemente lleva a cabo estas peticiones y responde a las mismas. Sin embargo, un nodo gestionado puede enviar un mensaje no solicitado llamado *trampa* para informar sobre un suceso. Un Network Utility puede enviar una trampa para informar sobre sucesos como, por ejemplo, un rearranque del sistema o la desactivación de una interfaz.

Una *Base de la información de gestión (MIB)* es un depósito de información virtual que define los elementos de datos del nodo gestionado a los que se puede acceder desde la estación de gestión. Las MIB se definen en archivos de descripción estrictamente formateados que pueden ser leídos por las personas y por el software de estación de gestión.

Un producto de nodo gestionado *soporta* una MIB cuando su software puede gestionar satisfactoriamente peticiones SNMP de elementos de datos documentados en la MIB y recuperar o establecer sus correspondientes elementos de datos internos. El archivo de descripción de MIB define para cada elemento de datos si la estación de gestión sólo puede leerlo o puede modificar su valor. A veces, un producto elige permitir sólo el acceso de lectura a un elemento de datos que la MIB documenta como grabable. Deberá consultar la documentación del producto para conocer el nivel de acceso de un producto determinado.

La mayoría de los tipos de interfaz y protocolos estándares de la industria tiene una MIB IETF estándar asociada con un número RFC. Las MIB estándares definen elementos de datos que son comunes a la mayoría de las implementaciones del tipo de interfaz o protocolo asociado. Los proveedores no siempre pueden esperar a que una MIB alcance el estado RFC estándar dentro de IETF y a veces envían soporte para una versión de *Internet Draft* (Borrador de Internet) preestándar de la MIB.

Además de las MIB estándares, muchos proveedores de productos desarrollan sus propias MIB para definir elementos de datos que son exclusivos de sus productos. Por ejemplo, el Network Utility soporta las MIB que dan acceso a información de memoria y utilización de CPU, para la cual no existe ninguna MIB estándar. En lenguaje de SNMP, estas MIB de proveedor se denominan MIB *específicas de empresa*.

Soporte de MIB

El Network Utility de IBM soporta un amplio conjunto de MIB estándares y específicas de empresa para supervisar y gestionar recursos. La lista actual asciende a una cifra entre 40 y 50 MIB.

Puede encontrar un archivo ″README″ que documenta el soporte MIB del Network Utility accediendo al directorio de release de software apropiado en la World Wide Web en:

```
ftp://ftp.networking.raleigh.ibm.com/pub/netmgmt/netu
```

En el mismo directorio, puede encontrar los propios archivos de descripción de MIB, que pueden recogerse con FTP y cargarse en una estación de gestión. Siempre que es posible los archivos se compilan en formato SNMP Versión 1, para que sean compatibles con la más amplia variedad posible de software de estación de gestión.

Para las MIB estándares e Internet Draft, el proceso de compilación elimina el texto explicativo de introducción y el formato de página que ayuda a hacer que una MIB sea más legible. Para obtener la versión completa precompilada de una MIB Internet Draft o RFC, recójala de una ubicación FTP IETF como recogería cualquier RFC o Internet Draft. Puede empezar en el URL siguiente y seguir los enlaces al RFC o al depósito de Internet Draft:

```
http://www.ietf.org
```

Las MIB siguientes son nuevas para este release:

- **MIB de túneles de capa 2**

  La MIB de túneles de capa 2 (Layer 2 Tunneling MIB) es una MIB de empresa de IBM que permite ver información acerca de los túneles de la capa 2 y las estadísticas asociadas a ellos. Existen trampas para los inicios y las detenciones de túnel y las anomalías de autentificación. También se pueden emitir

inicializaciones a una MIB de prueba a fin de comprobar si se puede establecer el túnel, basándose en la información de configuración para dicho túnel. Existe una MIB de prueba que permite determinar el tiempo de respuesta para la transmisión por túnel.

- **MIB de políticas de control**

  La MIB de políticas de control es una MIB empresarial de IBM que básicamente contiene la información de políticas que se ha cargado en la base de datos de políticas del direccionador. Esta MIB permite determinar si tales políticas se cargarona partir de una configuración local, de un servidor LDAP o de ambos. La MIB lleva un registro del número de veces que se ha activado una política de control, así como de las negociaciones de IPSec e IKE que tienen lugar. La información de negociaciones se puede volver a indexar en la MIB IPSec/IKE cuando se quiere obtener información más específica de estas negociaciones. También es posible examinar los parámetros de configuración LDAP, tanto los de administración como los de operación. La MIB permite también inicializar algunos parámetros LDAP y, en consecuencia, cambiar la configuración. Contiene asimismo un objeto que hace que la base de datos de políticas se renueve cuando se inicializa. Existe otra MIB de prueba que permite inicializar los selectores para efectuar una consulta de políticas (Dirección IP de origen y destino, protocolo, número de puerto y byte DS) y de este modo determinar las políticas y acciones que se originarían mediante una consulta con dichos selectores.

- **MIB IPSec/IKE**

  La MIB IPSec/IKE es una MIB de empresa de IBM que permite ver la información de negociación activa para la fase I y la fase II de IKE. También proporciona tablas para las estadísticas de IPSec para el cifrado y descifrado así como para los errores. Existen trampas para los inicios y las detenciones de túnel y las anomalías de autentificación y descifrado. La MIB también visualiza información acerca de las subredes y aplicaciones que se están protegiendo e información de la identificación local y remota de las pasarelas de seguridad.

Cómo empezar

En el Network Utility

Antes de que una estación de gestión SNMP pueda comunicarse con el Network Utility, deberá configurar SNMP en el Network Utility con el acceso apropiado habilitado. Puede utilizar el Programa de configuración, talk 6 o talk 5 para habilitar SNMP y definir un *nombre de comunidad* que otorgue acceso a una o más estaciones de gestión. Desde talk 6 o talk 5, utilice **protocol snmp** para acceder a los subprocesos Config y Console y trabajar con SNMP. Como se muestra en el paso 3 en la página 27, también puede utilizar Quick Config para habilitar SNMP y definir un nombre de comunidad de lectura o de lectura y grabación.

Consulte en la publicación *MAS Consulta de configuración y supervisión de protocolos Volumen 1* los capítulos ″Using SNMP″ y ″Configuring and Monitoring SNMP″ para obtener más información básica así como una descripción de los mandatos SNMP de talk 6 y talk 5.

En la estación de gestión

Antes de que una estación de gestión pueda proporcionar soporte significativo de un nodo gestionado, debe conocer cuáles son las MIB que soporta dicho nodo gestionado. No tiene que realizar ninguna acción si está utilizando cualquiera de

los productos de IBM descritos en el apartado “Productos IBM Nways Manager” en la página 98 . Cada uno de ellos ya tiene compiladas las MIB que el Network Utility soporta.

Si está utilizando algún otro producto de gestión, puede que tenga que preparar dicha información. Las estaciones de gestión proporcionan normalmente un recurso para cargar módulos MIB compilados en la estación. Cuando esté preparando una estación de gestión para gestionar el Network Utility, defínala para que lea todas las MIB del directorio apropiado bajo el URL proporcionado en el apartado “Soporte de MIB” en la página 95.

Si tiene la intención de enviar trampas desde el Network Utility a la estación de gestión, puede que también necesite definir la estación de gestión para que emita mensajes o realice acciones específicas al recibir una trampa.

Soporte de alertas SNA

La SNA (Systems Network Architecture) (Arquitectura de Red de Sistemas) de IBM define un amplio conjunto de flujos de protocolos para la gestión de productos de red. Una parte clave de dicha arquitectura es la posibilidad de que el nodo gestionado envíe un informe de errores o sucesos no solicitado, llamado *alerta*, a una estación de gestión SNA. Una alerta contiene una secuencia de submensajes que permiten al producto de gestión proporcionar a un operador información como la siguiente:

- La identidad del nodo que ha creado la alerta
- El error o suceso que ha activado la alerta
- Varias causas posibles del problema
- Acciones correctivas posibles

El producto de gestión SNA utilizado más comúnmente para recibir alertas es NetView/390. En una arquitectura SNA, un producto de este tipo se denomina *punto focal* de alerta. Un producto de la red que puede recibir y reenviar alertas en nombre de otros productos se denomina *punto de entrada*.

Cuando el Network Utility se utiliza como nodo de red APPN, tiene la posibilidad de establecer sesiones LU6.2 con puntos focales de alerta y enviar alertas SNA nativas para informar sobre condiciones de error en el sistema y en la red. A continuación se indican algunos de los cerca de 30 sucesos predefinidos que desencadenan una alerta desde la función APPN del Network Utility:

- Anomalía de definición de sesión
- XID no válido recibido, error de protocolo XID
- Error de protocolo o configuración HPR o DLUR
- Anomalía de sesión CP-CP
- Escasez de recursos
- Error de protocolo de subcomponente

Si se produce uno de estos sucesos y el Network Utility no tiene ninguna sesión actual de punto focal en la que enviar la alerta, pone en cola la alerta para transmitirla posteriormente. Puede configurar la longitud de esta cola de ″alertas retenidas″. No puede configurar cuál de estos sucesos desencadenará una alerta.

La sesión LU6.2 en la que fluyen las alertas puede establecerla el punto focal o el Network Utility. No tiene que configurar ningún parámetro especial en el Network Utility APPN para habilitarlo para que acepte una sesión de un punto focal de alerta y para que envíe alertas. Si desea que el Network Utility defina activamente

sesiones y reenvíe alertas, configure el nombre de uno o más puntos focales *implícitos* como parte de la configuración APPN. Si no se puede establecer la comunicación con el punto focal primario, el Network Utility intentará comunicarse con los otros nombres configurados.

Además de enviar alertas de los sucesos que ha detectado, el Network Utility puede servir de punto de entrada SNA y reenviar alertas en nombre de otros nodos SNA con los que tiene sesiones. No es necesaria ninguna configuración para habilitar esta función.

Cómo empezar

Puede utilizar el Programa de configuración o talk 6 para configurar nombres de punto focal si desea que el Network Utility active las sesiones de punto focal. Desde talk 6, utilice **protocol appn** para acceder al subproceso Config para trabajar con APPN y, a continuación utilice el mandato **add focal-point**.

Para obtener más información básica, consulte en la publicación *MAS Consulta de configuración y supervisión de protocolos Volumen 2* las secciones de APPN ″Entry Point Capabilities for APPN-related Alerts″, ″Configurable Held Alert Queue″ e ″Implicit Focal Point″. Los nombres de mandatos se proporcionan en la sección ″Router Configuration Process″ del mismo capítulo.

Productos de gestión de red

Los flujos de gestión SNMP y SNA necesitan un producto independiente del Network Utility para gestionar una pantalla de la red y del Network Utility, para consultar el estado del Network Utility o para recibir informes de sucesos no solicitados del Network Utility. Esta sección lista algunos de los productos que puede utilizar para efectuar dichas tareas.

Navegadores MIB de SNMP

Un *navegador MIB* es una pequeña aplicación de PC o estación de trabajo que puede cargar definiciones de MIB, consultar o establecer elementos de datos en un nodo gestionado y descodificar valores y resultados devueltos para convertirlos a un formato que se pueda leer fácilmente. En términos de SNMP, es una estación de gestión, pero un navegador MIB carece de la potencia y sofisticación de una plataforma de gestión SNMP totalmente desarrollada como las que se describen en la sección siguiente. Normalmente, los navegadores MIB se empaquetan como parte de dichas plataformas pero también pueden ser productos autónomos.

Productos IBM Nways Manager

Los siguientes productos de gestión de red SNMP de IBM están específicamente destinados a gestionar el Network Utility y una amplia variedad de otros productos de red IBM y no IBM. Cada uno de ellos proporciona una vista topológica gráfica de los recursos de red, con un estado codificado en color de los recursos y un estado general de cada red. Cada uno soporta el descubrimiento automático de recursos de red y las actualizaciones automáticas en una mapa de redes en respuesta a cambios de red.

IBM Nways Manager para AIX

Este producto, que está diseñado para gestionar entornos de red de tamaño mediano a grande, se ejecuta en una estación de trabajo que ejecute AIX, la versión de IBM de UNIX. Nways Manager para AIX se ejecuta en Tivoli TME 10 NetView, que anteriormente se conocía como ″NetView para AIX″ y ″NetView/6000″. Las funciones de Tivoli TME 10 NetView como plataforma de gestión de red permiten, por ejemplo, la gestión de topologías LAN, el registro de anomalías y sucesos y el registro de errores. Cuando se combina con el SNA Server para AIX de IBM, Tivoli TME 10 NetView también puede correlacionar trampas SNMP con alertas SNA. Esto permite al Network Utility transmitir alertas SNA prácticamente sobre cualquier suceso ELS definido.

Nways Manager para AIX proporciona las posibilidades siguientes además de las funciones básicas de Tivoli TME 10 NetView:

- Una aplicación de gestión específica de Network Utility

  Al seleccionar un Network Utility en la vista de topología de red, se ve un gráfico del panel frontal del Network Utility, con el estado de interfaz codificado en color. Una ventana de navegación situada al lado le permite acceder a toda la información de MIB de SNMP proporcionada por Network Utility, en formato gráfico o tabular. Esta aplicación le permite:
  - Ver o cambiar el estado del adaptador y de la interfaz
  - Visualizar estadísticas a nivel de componente o de interfaz
  - Supervisar de un vistazo y en tiempo real el estado codificado en color en tiempo real de un solo vistazo
  - Definir y supervisar umbrales de rendimiento
  - Definir y supervisar estadísticas históricas y en tiempo real
  - Supervisar sucesos en tiempo real

  Desde la aplicación Network Utility, puede arrancar:

  - El Programa de configuración gráfico de 2216/Network Utility para configurar el sistema
  - Una sesión Telnet en el Network Utility, para poder utilizar la interfaz de la línea de mandatos para configurar, supervisar y controlar el Network Utility

  Dado que la aplicación de gestión Network Utility está basada en Java, para utilizarla no es necesario que el usuario esté en la estación de trabajo que ejecuta Nways Manager. Puede arrancar la aplicación desde un PC o una estación de trabajo que ejecute un navegador Web conforme con JDK, que esté conectado a través de la intranet o Internet a la estación de trabajo principal Nways Manager. Para obtener detalles sobre qué navegadores Web y versiones de JDK se necesitan, consulte los prerrequisitos del producto Nways Manager en:

  ```
  http://www.networking.ibm.com/netmgt
  ```

  El soporte de gestión de Java incluye la visualización de estado del Network Utility en tiempo real y la posibilidad de realizar gestión de rendimiento. Por razones de seguridad, no puede arrancar el Programa de configuración desde un navegador web Java.

- Agentes inteligentes distribuidos

  A fin de proporcionar soporte para redes mayores, puede utilizar sistemas distintos de la estación de trabajo Nways Manager para sondear los nodos gestionados de la red. La descarga del sondeo de la estación de trabajo de gestión libera su procesador para realizar otras tareas y libera anchura de banda de red porque el sondeo se coloca más cerca de los dispositivos que se están

sondeando. Estos ″agentes″ del gestor pueden configurarse para que informen a Nways Manager cuándo se están excediendo los umbrales.

El software de agente inteligente está basado en Java y se baja de Nways Manager. Los agentes pueden colocarse en cualquier estación de trabajo habilitada para Java (máquina virtual Java) de la red. Nways Manager también puede utilizar las posibilidades de sondeo distribuidas proporcionadas por el Gestor de nivel medio TME 10.

- Soporte de topología APPN

  Nways Manager para AIX proporciona una vista a nivel de APPN de la topología de la red. Puede descubrir recursos APPN participantes, examinarlos y ver su estado como iconos codificados en color. También se proporcionan sucesos de errores y de rendimiento de protocolo APPN (datos y gráficos). Esta aplicación no presenta topologías de Extended Border Node (Nodo de borde extendido) o Branch Extender (Extensor de bifurcación).

- Soporte de topología DLSw

  Nways Manager para AIX también puede mostrarle una vista de la red de topología DLSw, incluyendo conectividad DLSw, recursos y estado codificado en color. La topología se renueva a medida que se descubren nodos nuevos. Esta aplicación no presenta la topología de grupos de multidistribución DLSw IP.

- Soporte de VLAN, ATM y RMON

  Nways Manager para AIX tiene un amplio soporte para productos que implementan LAN virtuales, para redes ATM y para reunir, correlacionar y visualizar datos de puntas de prueba RMON y ECAM.

- Aplicación de gestión VPN

  La Aplicación de gestión VPN (Virtual Private Network) (Red privada virtual) Nways proporciona un amplio conjunto de funciones de Supervisión, Información de sucesos, Resolución de problemas, Control de operación y Arranque de aplicaciones. La versión inicial está específicamente destinada a proporcionar supervisión y control de operación de las posibilidades VPN para el Direccionador IBM 22xx y utiliza Objetos MIB privados al proporcionar sus funciones dado que no existen actualmente Objetos MIB estándares.

  La Aplicación de gestión VPN Nways se concentra en tres Componentes VPN:

  – Túneles VPN
  – Clientes VPN
  – Políticas

  La función de Supervisión le permite ver Túneles VPN activos y anteriores, ver Clientes VPN activos y anteriores y ver Políticas VPN definidas y activas. La función de Información de sucesos le informa cuándo se inicia un Túnel VPN y cuándo el Dispositivo VPN experimenta un Ataque contra la seguridad. La función de Control de operación le permite inhabilitar/desactivar un Túnel VPN, inhabilitar/desactivar un Cliente VPN y renovar Políticas VPN. La función de Resolución de problemas le permite ejecutar ping para proxy en un dispositivo VPN y ver Anotaciones cronológicas de anomalías de sucesos VPN. La función de Arranque de aplicaciones proporcionará la posibilidad de arrancar diversas aplicaciones de gestión de red relacionadas, por ejemplo PSM/JMA del dispositivo.

La primera versión de Nways Manager para AIX con soporte específico para Network Utility es la Versión 1.2.2.

Para obtener más información sobre Nways Manager para AIX incluidas las especificaciones y los requisitos del sistema, vaya a:

http://www.networking.ibm.com/cma/cmaprod.html

Las páginas de esta ubicación describen los componentes de Nways Manager para AIX que se venden por separado e indican qué componentes efectúan determinadas funciones entre las descritas más arriba.

IBM Nways Workgroup Manager para Windows NT

El Workgroup Manager, diseñado para gestionar entornos de red de tamaño pequeño a grande, es una aplicación Windows NT nativa de 32 bits que opera en NT Versión 4.0. A diferencia de Nways Manager para AIX, Workgroup Manager es completo e independiente y no utiliza ninguna plataforma de gestión de red subyacente. Por consiguiente, debe proporcionar él solo diversas funciones de plataforma.

Las funciones clave de Nways Workgroup Manager para Windows NT incluyen:
- Descubrimiento automático de la red IP
- Vistas gráficas de topología de red en tiempo real
- Posibilidad de examinar, actualizar y compilar las MIB
- Estado de red y dispositivo agregado y codificado en color en tiempo real
- Detalles de problemas
- Gestión de trampas, incluyendo la especificación de gravedad de trampa
- Compilador de trampas
- Configuración y notificación de sondeo
- Configuración y notificación de umbral de rendimiento
- Gestión de inventario
- Recogida y presentación de estadísticas históricas y en tiempo real
- Aplicación de gestión VPN

Nways Workgroup Manager para Windows NT soporta exactamente la misma aplicación de gestión Java específica de Network Utility que Nways Manager para AIX. Puede ejecutar la aplicación de gestión Network Utility desde un navegador web con capacidad para Java. Nways Workgroup Manager para Windows NT también soporta Agentes inteligentes distribuidos.

Nways Workgroup Manager para Windows NT no soporta las aplicaciones de topología DLSw y APPN que soporta Nways Manager para AIX. La visualización de la topología de Nways Workgroup Manager para Windows NT se basa en la conectividad IP entre los nodos gestionados.

La primera versión de Nways Workgroup Manager para Windows NT con soporte específico para Network Utility es la Versión 1.1.2.

IBM Nways Manager para HP-UX

Este producto, diseñado para gestionar entornos de red de tamaño medio a grande, se ejecuta en una estación de trabajo que funcione bajo HP-UX, la versión de Hewlett Packard de UNIX. Nways Manager para HP-UX se ejecuta sobre el software de plataforma de gestión *Network Node Manager* de HP, conocido anteriormente como ″HP OpenView″.

En este entorno, el gestor de nodos de red proporciona las funciones básicas de plataforma de gestión, incluyendo la visualización de topología, la gestión de trampas, etc. A diferencia de Nways Manager para AIX, permite asociar dispositivos de red IBM con la aplicación de gestión Nways Manager para HP-UX apropiada.

Desde Nways Manager para HP-UX, puede arrancar las mismas aplicaciones de gestión Java específicas de Network Utility que desde Nways Manager para AIX. Nways Manager para HP-UX también soporta Agentes inteligentes distribuidos.

Nways Manager para HP-UX no soporta las aplicaciones de topología DLSw y APPN que soporta Nways Manager para AIX.

La primera versión de Nways Manager para HP-UX con soporte específico para Network Utility es la Versión 1.2.

NetView/390

NetView/390 es un producto de gestión basado en sistema principal para gestionar redes SNA de tamaño medio a grande. Existen varios modos de utilizar NetView/390 para gestionar un Network Utility y los productos SNA que puede conectar al sistema principal:

- Controlar los recursos SNA (activando y desactivando enlaces, las PU y las LU)
  - Cuando el Network Utility está ejecutando DLSw, NetView/390 puede controlar los enlaces que DLSw está representando y las PU y las LU de estaciones finales SNA remotas.
  - Cuando el Network Utility está ejecutando el soporte de servidor TN3270, NetView/390 puede controlar las PU y las LU locales representadas en el Network Utility.
  - Cuando el Network Utility está ejecutando DLUR para nodos en sentido directo, NetView/390 puede controlar las PU y las LU a las que el Network Utility está sirviendo y los enlaces entre el Network Utility y dichos nodos.
  - Cuando el Network Utility está estableciendo puentes para el tráfico de estaciones finales SNA, NetView/390 puede controlar las PU y las LU de estación final.
  - Cuando el Network Utility está ejecutando APPN, DLSw o estableciendo puentes para el tráfico SNA, NetView/390 puede controlar los enlaces adyacentes entre el sistema principal y el Network Utility.
  - Cuando el Network Utility está ejecutando la función de pasarela directa LSA, NetView/390 puede controlar los enlaces de LAN que parecen ser locales en VTAM, así como las PU y las LU de las estaciones finales SNA conectadas.
- Supervisar la topología y los errores de red
  - NetView/390 puede ser el punto focal de alertas cuando el Network Utility está sirviendo de nodo APPN, tanto para las alertas que genera el Network Utility como para las que reenvía desde otros nodos.
  - Cuando el Network Utility está ejecutando DLSw, DLUR o estableciendo puentes para el tráfico SNA, NetView/390 puede recibir alertas, información de tiempo de respuesta o cualquier otro flujo SSCP-PU de una PU de sentido directo.
  - NetView/390 puede ser el punto focal de alerta para trampas de Network Utility que han sido convertidas en alertas por Tivoli TME 10 NetView y el SNA Server para AIX.
  - Mediante los productos relacionados*SNA Topology Manager*, *APPN Accounting Manager* y *APPN Topology Integrator*, NetView/390 puede adquirir y supervisar la topología de una red APPN incluyendo el Network Utility y otros productos APPN que admitan el protocolo SNMP.

Capítulo 9. Tareas generales de gestión

Este capítulo proporciona procedimientos y mandatos para operaciones importantes del Network Utility. Sirve como suplemento de algunas de las presentaciones de conceptos proporcionadas en capítulos anteriores.

Supervisión de sucesos

Esta sección complementa la información básica sobre la anotación cronológica y la visualización de sucesos proporcionada en el apartado “Anotación cronológica de sucesos (Utilizando talk 2, el proceso Monitor)” en la página 68 y en el apartado “Supervisión de mensajes de sucesos” en la página 92. Introduce los mandatos que controlan qué sucesos se anotan y dónde se anotan.

Acceso al sistema de anotación cronológica de sucesos

Debe utilizar la interfaz de la línea de mandatos para activar la anotación cronológica de sucesos. Desde el Programa de configuración, sólo puede configurar parámetros generales de anotación cronológica remota.

En el indicador principal de talk 5 o talk 6, escriba **event** para entrar en el subproceso Console o Config de ELS, respectivamente. Esencialmente verá los mismos mandatos tanto si está trabajando bajo talk 5 como bajo talk 6. Los mandatos de Talk 5 ELS entran en vigor inmediatamente y son bastante útiles para activar mensajes a fin de depurar un flujo determinado de un sistema en ejecución. Desde talk 6, configure los sucesos que desea que se anoten siempre, para no tener que activarlos cada vez que rearranque el Network Utility.

Mandatos para controlar la anotación cronológica de sucesos

Existen seis mandatos básicos para activar y desactivar la anotación cronológica de sucesos, dos para cada uno de los tres destinos posibles de los mensajes de anotación cronológica:

- **disp** y **nodisp** controlan qué sucesos se anotan localmente en talk 2
- **trap** y **notrap** controlan qué sucesos generan trampas SNMP
- **remote** y **noremote** controlan qué sucesos se anotan de forma remota en un sistema principal habilitado para syslogd

Todos estos mandatos utilizan el mismo método para especificar qué sucesos deben activarse o desactivarse. A continuación del nombre del mandato en la línea de mandatos, normalmente se escribe una de las opciones siguientes (existen otras):

- **event** *subsistema.númerosuceso*, para especificar un suceso individual predefinido

  subsistema es el nombre de un componente funcional conocido en ELS, por ejemplo ″dls″ para DLSw o ″esc″ para ESCON. Puede escribir **li sub** para obtener una lista de los nombres de subsistemas ELS.

  númerosuceso es el número de un suceso predefinido, escrito con ceros iniciales. Puede escribir **li sub** *subsistema* para obtener una lista rápida de los sucesos de un subsistema determinado.
- **sub** *subsistema nivel_anotacióncronológica*, para especificar algún conjunto de sucesos predefinidos de un subsistema ELS

subsistema es el nombre del subsistema ELS descrito anteriormente. El valor ″all″ selecciona todos los subsistemas.

nivel_anotacióncronológica es opcional y toma por omisión ″standard″, que incluye todos los mensajes informativos inusuales y de error. El valor ″all″ selecciona todos los mensajes del subsistema.

La lista siguiente proporciona unos ejemplos de estos mandatos:

disp sub all
Habilita la anotación cronológica en talk 2 de todos los mensajes informativos inusuales y de error de todos los subsistemas ELS. Éste es un mandato apropiado para configurar en talk 6.

rem sub dls
Habilita la anotación cronológica remota de todos los mensajes informativos inusuales y de error del subsistema DLS. Necesitará configurar por separado el sistema principal de destino para la anotación cronológica remota.

disp sub sdlc all
Habilita la anotación cronológica en talk 2 de todos los mensajes del subsistema SDLC. Puede que habilite todos los mensajes al intentar rastrear una situación de error.

nodisp ev sdlc.008
Inhabilita la anotación cronológica en talk 2 de un mensaje SDLC particularmente informal, que puede estar impidiendo ver mensajes más importantes de la anotación cronológica de errores.

trap ev dls.475
Habilita el envío de una trampa SNMP cuando se produce un suceso de error DLSw QLLC determinado.

Para obtener información detallada sobre estos mandatos, sobre el modo de configurar la anotación cronológica remota, sobre qué son los niveles de anotación cronológica, etc., consulte el apartado ″Using the Event Logging System (ELS)″ del manual *MAS Guía del usuario de software*.

Supervisión de la utilización de memoria

Esta sección describe cómo se utiliza la memoria de Network Utility y cómo se puede supervisar el estado de la misma.

Uso de la memoria de Network Utility

Un Network Utility se envía con 256 o 512 MB de memoria principal. Al arrancar el sistema, éste carga el código de operación del disco en esta memoria, tomando una cantidad determinada de espacio de memoria para cada módulo de carga. Una vez que se ha cargado el código de operación, el sistema subdivide la memoria restante entre APPN/TN3270 (si se ha configurado) y la función de direccionamiento. La función de direccionamiento incluye la pasarela de canal, TCP, DLSw e IP; en resumen, todas las funciones excepto la de servidor TN3270 y APPN.

Al configurar APPN desde el Programa de configuración o la línea de mandatos, puede especificar la cantidad de memoria que se debe reservar para APPN. En Network Utility, este valor está preestablecido en la memoria necesaria para una

configuración máxima de servidor TN3270E[12].Este valor también debe ser razonable para las aplicaciones APPN no TN3270, de modo que no necesita cambiarlo. Si la configuración no permite APPN, el Network Utility no toma en cuenta el valor configurado y no reserva memoria para APPN. Si la configuración permite APPN, el Network Utility asigna a APPN la cantidad especificada de memoria y entonces asigna toda la memoria restante a la función de direccionamiento.

Puede supervisar la utilización de memoria en un Network Utility en ejecución desde una consola de línea de mandatos o desde una estación de gestión SNMP. De cualquiera de los dos modos, podrá examinar por separado el estado de memoria APPN y el estado de memoria de función de direccionamiento. Una vez que se ha cargado el sistema, estas particiones de memoria quedan fijas y se gestionan de forma independiente.

Supervisión de memoria desde la línea de mandatos

Para supervisar la memoria de función de direccionamiento desde la línea de mandatos:

1. En el indicador *, escriba **talk 5** y pulse **Intro** para obtener el indicador +.
2. Escriba **mem** para ver estadísticas generales y detalladas sobre la utilización actual de la memoria. La salida utiliza el término *heap* (almacenamiento dinámico) para hacer referencia a la memoria que está utilizando la función de direccionamiento.

Para supervisar memoria APPN/TN3270 desde la línea de mandatos:

1. Desde el indicador *, escriba **talk 5** y pulse **Intro** para obtener el indicador +.
2. Desde el indicador +, escriba **p appn** y pulse **Intro** para obtener el subproceso Console de APPN.
3. Escriba **mem** y pulse **Intro** para ver estadísticas de resumen y detalladas sobre la utilización de memoria APPN. La salida divide la memoria APPN en varias partes y muestra el estado de cada parte.

Supervisión de memoria utilizando SNMP

El Network Utility soporta MIB específicas de empresa de IBM que proporcionan acceso a la información de utilización de memoria para la función de direccionamiento y para APPN/TN3270.

Los productos de Nways Manager descritos en el apartado “Productos IBM Nways Manager” en la página 98 proporcionan soporte estadístico completo para las particiones de memoria de función de direccionamiento y APPN. Para cada una de las particiones, puede ver información de utilización histórica y en tiempo real. Puede definir umbrales de alarma para cada uno de los porcentajes de utilización, de forma que se le pueda informar cuando la utilización de memoria alcance un determinado nivel.

También puede configurar el Network Utility desde la línea de mandatos para que envíe una trampa SNMP cuando la memoria de función de direccionamiento disponible esté por debajo de un umbral determinado. Desde el indicador de talk 6

12. Con la introducción de soporte para 512 MB, el Programa de configuración supone por omisión que el Network Utility de destino tiene 512 MB de memoria, pero si detecta que tiene 256 MB, se ajusta automáticamente para ese valor. No es necesario que cambie el valor por omisión del Programa de configuración.

Config>, escriba el mandato **patch mosheap-lowmark** y proporcione el valor de porcentaje si desea cambiarlo del valor por omisión de 10%.

Supervisión de la utilización de la CPU

Esta sección describe cómo controlar la supervisión de la CPU y obtener informes de talk 5 o mensajes directos periódicos en la anotación cronológica de talk 2.

Acceso a la supervisión de rendimiento

En el indicador principal de talk 5 o talk 6, escriba **perf** para entrar en la Consola de supervisión de rendimiento o en el subproceso Config, respectivamente. Desde talk 6 y desde el Programa de configuración, puede habilitar o inhabilitar la supervisión de utilización de la CPU y establecer sus parámetros de operación como parte de la configuración de Network Utility. Desde talk 5, puede hacer que los mismos cambios entren en vigor inmediatamente y obtener informes sobre la utilización de la CPU en un Network Utility en ejecución.

Supervisión de la utilización de la CPU desde la línea de mandatos

Una vez que esté en el indicador PERF Console>, estarán disponibles los mandatos siguientes:

report Proporcionar un resumen de la utilización actual de la CPU, los niveles máximos alcanzados y la distribución histórica de valores.

enable cpu, disable cpu
Controlar la recopilación general de información de utilización de CPU. Por omisión, el Network Utility se ejecuta con la utilización de CPU habilitada, con un impacto insignificante en el rendimiento del sistema. Si está ejecutando funciones de servidor TN3270 con Asignador de tareas de red, es particularmente importante dejar habilitada la utilización de CPU.

enable t2, disable t2
Controlar la generación de un mensaje ELS periódico en talk 2 que muestra la utilización actual de CPU. Si habilita este mensaje, se evita tener que escribir repetidamente el mandato **report** para supervisar la utilización de CPU.

set, list, clear
Establecer la ventana de tiempo para la recopilación de estadísticas. Ver los valores actuales de todos los valores. Restablecer las estadísticas.

Están disponibles los mismos mandatos o parámetros desde talk 6 y el Programa de configuración, a excepción de **clear** y **report**.

Para obtener más información sobre estos mandatos y ejemplos de su salida, consulte el apartado ″Configuring and Monitoring Performance″ en la publicación *MAS Guía del usuario de software*.

Supervisión de la utilización de la CPU mediante el SNMP

El Network Utility soporta una MIB específica de empresa de IBM que proporciona acceso a la información histórica y actual de la utilización de la CPU.

Los productos de Nways Manager descritos en el apartado “Productos IBM Nways Manager” en la página 98 proporcionan soporte estadístico completo para la utilización de CPU del Network Utility. Puede ver información histórica y en tiempo real. Puede definir umbrales de alarma basándose en porcentajes de utilización de la CPU, para poder así ser informado cuando ésta alcance un determinado nivel.

Capítulo 10. Mantenimiento de software

Este capítulo describe lo que es necesario saber para recibir e instalar arreglos para solucionar problemas de software del Network Utility y para actualizar a nuevos releases de software que contienen funciones nuevas.

Esta información incluye:
- Cómo se denomina y se empaqueta el software
- Cómo bajar nuevas versiones de software desde la World Wide Web
- Cómo cargar software en el Network Utility
- Cómo solicitar soporte y servicio para el producto

Versiones y empaquetado de software

Denominación de versión

El software que opera el Network Utility se denomina *Multiprotocol Access Services* o MAS. MAS también opera en el IBM 2216-400, pero hay diferentes paquetes de MAS independientes para cada producto. Los paquetes de MAS para el Network Utility se caracterizan por:

- Los valores de configuración preestablecidos, para ajustar el Network Utility para las aplicaciones a las que está destinado.
- El empaquetado de funciones especializado orientado hacia los usos clave del Network Utility. Por ejemplo, algunas de las funciones generales de direccionamiento multiprotocolo del 2216-400, tales como IPX, Appletalk, Banyan Vines y DECNet, no están disponibles en los paquetes del Network Utility.

Los niveles específicos de MAS se identifican por los números siguientes:

Versión
: Un nuevo release de funciones necesita a veces un número de versión nuevo. En algunas ocasiones, esto está relacionado con un aumento de precio, pero también puede estar relacionado con un cambio en el modo en que IBM distribuye el software. Un nuevo número de versión no significa que el release tenga más funciones nuevas que un release que sólo tenga un número de release nuevo.

Release
: Este número cambia con cada nuevo release de funciones.

Modificador
: Este número indica que se trata de un nuevo release donde se incorpora un pequeño cambio para otro release nuevo que incluye un mayor número de funciones. Va colocado detrás del punto decimal en el formato ″MAS Vv.r Mod m PTF p″.

PTF Este número representa un nivel de mantenimiento, descrito a continuación.

La base de código inicial para Network Utility es: MAS V3R1.0 PTF 1. Dado que IBM utiliza la misma numeración de release que para los paquetes 2216-400 de MAS, se puede correlacionar fácilmente el nivel de función y mantenimiento de software en los dos productos.

Para ver el nivel de software del código que se está ejecutando activamente en el Network Utility, vaya al menú básico de talk 5 y escriba **c** (de ″configuración″). La parte de versión de software de la salida de este mandato utiliza el formato ″MAS Vv.r Mod m PTF p″.

Para ver el nivel de software de las cargas de código en el disco duro del Network Utility, vaya al menú básico de talk 6, escriba **boot** para entrar en el subproceso de arranque Config y, a continuación, escriba **describe**.

Niveles de mantenimiento

Cuando acceda a las páginas de la World Wide Web que contienen versiones recientes del software Network Utility, verá algunos de los términos siguientes para diferentes niveles de mantenimiento de los paquetes de Network Utility:

Nivel de GA
: El primer nivel de software que ha quedado disponible en general (″generally available″) para los clientes de IBM. Éste es el nivel enviado inicialmente en el disco duro de los nuevos sistemas Network Utility. El software de nivel GA se somete a unas dilatadas pruebas a nivel de producto y a nivel de sistema antes de entregarse. La disponibilidad general corresponde normalmente a una Versión o Release nuevo del software (el release inicial de Network Utility en un PTF es una excepción a esta regla).

PTF
: Release de mantenimiento importante (″program temporary fix″) (arreglo temporal de programa) que acumula un gran número de arreglos y se somete a un prueba de regresión de la mayoría de las principales funciones de software. Cuando un release ha sido utilizado durante un tiempo, normalmente IBM empieza a enviar un PTF estable en el disco duro de los productos nuevos.

EPTF
: Pequeño release de mantenimiento (″emergency PTF″) (PTF de emergencia) que se entrega de forma más frecuente, incluye menos arreglos y se somete a una prueba de regresión de las áreas específicas afectadas por los arreglos.

Los PTF y los EPTF son acumulativos, en el sentido de que cada uno reemplaza a todos los PTF y EPTF anteriores. Sólo necesita instalar el PTF o EPTF más reciente para obtener todos los arreglos anteriores.

Empaquetado de características

Existen dos paquetes de características del software de Network Utility, que corresponden a los dos modelos diferentes de Network Utility:

Modelo	Descripción
TX1	Código base, incluyendo función VPN, IP, APPN y DLSw
TN1	Código base más función de servidor TN3720E

En función del modelo que haya comprado, el Network Utility viene precargado con el paquete de software adecuado en ambos bancos del disco duro. Al cargar un nuevo nivel de mantenimiento de software, se carga el mismo paquete que ya está en el Network Utility.

Tenga en cuenta que sólo existe una versión del Programa de configuración y que ésta soporta las funciones de software de todos los paquetes de software. Si configura funciones que no se soportan en el paquete de software que tiene en el direccionador, el software del direccionador no tendrá en cuenta dicha parte de la configuración.

Desde la línea de mandatos, no puede configurar o supervisar funciones de software que no existan en el software que está ejecutando.

Obtención de acceso Web al software

Para actualizar el software Network Utility, primero deberá bajar el nivel de mantenimiento apropiado de la World Wide Web. Para encontrar el nuevo software, empiece con la página principal del producto Network Utility en:

```
http://www.networking.ibm.com/networkutility
```

Pulse en **Support** y, a continuación, **Downloads** para obtener la información y los enlaces siguientes:

- Información general sobre cómo acceder al software
- Procedimientos detallados para bajar e instalar el software
- Enlace a los últimos niveles de mantenimiento del Programa de configuración, con archivos README asociados
- Enlaces a los últimos niveles de mantenimiento de MAS, con archivos de contenido de PTF o EPTF asociados

Al seguir los enlaces a un nivel de mantenimiento determinado del Programa de configuración, puede acceder a versiones binarias empaquetadas del Programa de configuración de 2216/Network Utility para cada uno de los sistemas operativos soportados. Cualquier persona puede bajar dichos archivos. El archivo README asociado proporciona instrucciones para desempaquetar e instalar la nueva versión del Programa de configuración.

Al seguir los enlaces a un nivel de mantenimiento determinado de MAS, puede acceder a versiones binarias comprimidas empaquetadas de cada una de las características de software del Network Utility listadas anteriormente.

Necesitará un id y una contraseña de cliente de IBM Networking para poder bajar estos archivos. Cree el id y la contraseña usted mismo registrándose en la Web y podrá utilizarlos inmediatamente para bajar archivos. Este id y esta contraseña cubren múltiples productos IBM Networking y le permiten suscribirse para recibir notificaciones de actualizaciones del producto por correo electrónico. Si no los tiene, las páginas Web le llevarán a la página de inscripción la primera vez que baje un paquete de código Network Utility.

Bajada y desempaquetado de archivos

Las páginas Web para bajar un release de mantenimiento de MAS concreto contienen archivos para cada una de las características de software soportadas. Cada archivo contiene un conjunto completo de software para Network Utility. Al instalar un nivel de mantenimiento de software Network Utility, se sustituye por completo todo el software existente por el nuevo nivel.

Para bajar el software de un archivo determinado y transferirlo al direccionador:

1. Utilice el navegador Web para bajar el archivo completo en binario a la estación de trabajo.
2. Transfiera el archivo a la estación de trabajo desde la que lo cargará en el direccionador. Ésta se denomina *estación de trabajo servidor* porque actúa como servidor de archivos del direccionador. Puede utilizar FTP o cualquier otro método de transferencia de archivos para efectuar este paso.
3. En la estación de trabajo servidor, desempaquete el archivo individual bajado en diversos archivos de software de direccionador. Estos archivos se denominan *módulos de carga* y tienen la extensión de archivo ″ld″ (o ″LD″ si el sistema no soporta mayúsculas y minúsculas combinadas).
4. Utilizando TFTP o Xmodem, transfiera los módulos de carga al direccionador.

En función del release de MAS, la página Web puede contener dos archivos para cada característica de software, cada uno de ellos creado por un programa de utilidad de empaquetado diferente. Elija la versión que pueda desempaquetar el software de la estación de trabajo servidor. Normalmente, la elección se efectúa del modo siguiente:

Sistema operativo servidor	Formato de archivo	Mandato de desempaquetado
DOS, Windows u OS/2	.zip	pkunzip
UNIX o AIX	.tar	tar -xvf

Al desempaquetar el software de direccionador, asegúrese de que todos los archivos ″.ld″ estén en el mismo directorio y tengan permisos de sistema de archivos para proporcionar el acceso de lectura apropiado. No cambie los nombres de ninguno de los archivos .ld. No mezcle archivos entre paquetes de características Network Utility diferentes o entre niveles de mantenimiento diferentes del mismo paquete. Mantenga cada paquete separado y diferenciado con un nombre de vía de acceso diferente en la estación de trabajo servidor.

Carga de código de operación nuevo

El código de operación (código-op, para abreviar) es el software que ejecuta las funciones normales de reenvío de paquetes y servicios del sistema de Network Utility. El código-op incluye el sistema operativo base, los protocolos, las características, los diagnósticos y el código de interfaz de línea de mandatos. La inmensa mayoría de los cambios de software incluidos en los PTF y los EPTF son para el código de operación.

Para cargar y activar código de operación nuevo, deberá:

1. Transferir los módulos de carga desempaquetados de la estación de trabajo servidor a uno de los dos bancos de código-op del disco duro del Network Utility.
2. Establecer el direccionador para que arranque desde el banco que tiene el nuevo código-op.
3. Rearrancar el direccionador o planificarlo para que arranque en una fecha y hora posteriores.

La Tabla 15 en la página 113 resume los diferentes modos en que puede transferir código de operación desde una estación de trabajo servidor a un disco duro de Network Utility. El método elegido dependerá del modo en que pueda conectar la

estación de trabajo al direccionador, del software que tenga en la estación de trabajo y de sus propias preferencias. He aquí unos puntos importantes que se deberán tener en cuenta:

- El tamaño de todos los archivos .ld combinados es de más de 10 MB. Si puede utilizar una LAN o una interfaz de red en lugar del módem o puerto de servicio, deberá hacerlo para evitar tener que pasar horas transfiriendo archivos.
- Los métodos basados en TFTP del código-op y del firmware transfieren automáticamente todos los archivos .ld en una sola operación. Con Xmodem, deberá especificar manualmente el nombre de cada uno de los aproximadamente 20 archivos .ld que componen una carga de software.

Tabla 15. Carga de código de operación

Conexión física	Protocolo de línea	Protocolo de transferencia	Herramienta	Direcciones IP por omisión
Puerto servicio + módem nulo Puerto servicio + módem ext Módem PCMCIA	Terminal asíncrona	Xmodem	Firmware	No aplicable
	SLIP	TFTP	Código-op	Network Utility=10.1.1.2 Estación de trabajo=10.1.1.3
PCMCIA EtherJet LIC Ethernet (10 Mbps) LIC Red en Anillo	IP	TFTP	Código-op Firmware	Network Utility=10.1.0.2 Estación de trabajo=10.1.0.3
Cualquier interfaz de red IP	IP	TFTP	Código-op	Ningún valor por omisión

Utilización del código de operación

Tal como muestra la Tabla 15, todos los procedimientos de transferencia que puede iniciar desde el código-op utilizan TFTP como protocolo de transferencia de archivos.

Utilización de TFTP

El procedimiento de código-op para utilizar TFTP para transferir archivos de código-op y firmware a un disco duro de Network Utility es el siguiente:

1. Configure las direcciones IP que va a utilizar.

   Si está utilizando una interfaz de red estándar que incluye un LIC Ethernet o de Red en Anillo, utilice el Programa de configuración o talk 6 para configurar una dirección IP para la interfaz del modo normal. (Desde talk 6, utilice **add address** en el subproceso IP). Active este cambio de configuración antes de continuar.

   Si está utilizando la tarjeta PCMCIA EtherJet, use **system set ip** para establecer las direcciones siguientes:
   - Dirección IP: dirección IP para la tarjeta EtherJet
   - Máscara de red: máscara para la subred conectada a la tarjeta EtherJet
   - Dirección de pasarela: dirección IP de cualquier direccionador intermedio para comunicarse con la estación de trabajo servidor TFTP o dirección IP de la propia estación de trabajo si no hay ningún direccionador intermedio.

   Si está utilizando SLIP, no puede cambiar las direcciones IP sino que debe utilizar las que se proporcionan en la Tabla 15.

2. Transfiera los archivos de código de operación y firmware.

   Desde el indicador *, siga esta secuencia:

   ```
   *t 6
   Config>boot
   Boot configuration
   Boot config>tftp get load mod
   ```

Responda a las solicitudes del modo siguiente:

- Dirección IP de servidor: Ponga la dirección de la estación de trabajo servidor TFTP.
- Directorio remoto: Ponga el nombre de vía de acceso al directorio de la estación de trabajo servidor donde están todos los archivos .ld. Utilice barras inclinadas en la dirección esperada por el servidor. La escritura en mayúsculas y en minúsculas sólo tiene importancia si también tiene importancia en el servidor.
- Banco de destino: Seleccione el banco A o el banco B. No puede seleccionar el banco actualmente activo.

Basándose en la dirección IP de servidor y en las direcciones IP de interfaz de Network Utility configuradas, el direccionador seleccionará las interfaces que utilizará para comunicarse con el servidor. El direccionador proporciona mensajes de estado que indican si la operación ha sido satisfactoria o anómala según sea apropiado.

3. Coloque el archivo de configuración en el banco de destino

   Transfiera el archivo de configuración que desea a una posición del banco donde acaba de poner la nueva carga de código. Si la nueva carga de código es un release de MAS nuevo, consulte el apartado “Migración de una configuración a un nuevo release de MAS” en la página 79 para obtener información básica importante acerca de este paso.
   - Si la nueva carga de código no es un release de MAS nuevo o si sólo utiliza la interfaz de la línea de mandatos para configurar el Network Utility, utilice el mandato **copy config** para copiar la configuración actual en un lugar donde la carga nueva pueda obtenerla.
   - Si la nueva carga de código es un release de MAS nuevo y usted no utiliza el Programa de configuración, utilícelo para actualizar la configuración. A continuación utilice el mandato **tftp get config** (o cualquiera de los demás métodos descritos en el apartado “Carga de archivos de configuración nuevos” en la página 84) para transferir la configuración actualizada al banco de destino.
4. Rearranque o planifique un rearranque

   Para activar la nueva carga inmediatamente, utilice el procedimiento siguiente, empezando desde el indicador **Boot config>**:
   a. Utilice el mandato **set** para seleccionar el banco que acaba de cargar para reiniciarlo a continuación y para seleccionar la configuración que acaba de copiar o transferir.
   b. Pulse **Control-p** y, a continuación, escriba **reload** para rearrancar el direccionador.

   Para activar la nueva carga posteriormente, escriba **timedload activate** en el indicador **Boot config>** para seleccionar el banco y la configuración y para especificar la fecha y hora para que rearranque el direccionador. Puede responder ″no″ a las preguntas relacionadas con la carga del banco, porque ya ha realizado este paso.

Consulte en la publicación *MAS Guía del usuario de software* el capítulo ″Configuring Change Management″ para obtener más información sobre los mandatos del procedimiento anterior.

Utilización del firmware

Tal como muestra la Tabla 15 en la página 113, puede utilizar Xmodem o TFTP desde el firmware para transferir código-op al disco duro del Network Utility. No se recomienda utilizar Xmodem porque las velocidades de módem son demasiado lentas para estos grandes archivos de código-op y Xmodem necesita una interacción regular. Cuando se trabaja desde el firmware, el método de transferencia preferido es TFTP a través de interfaces de LAN. No obstante, esta sección resume todos los procedimientos posibles por si necesita utilizarlos.

Utilización de Xmodem

El procedimiento de firmware para utilizar Xmodem para transferir archivos de código-op y firmware a un disco duro de Network Utility es el siguiente:

1. Acceda al menú principal de firmware utilizando los procedimientos descritos en el apartado “Opciones de arranque: Arranque rápido y obtención de firmware” en la página 46.
2. Seleccione las opciones de menú en la secuencia siguiente:
   a. System Management Services (menú principal): Opción 4, ″Utilities″
   b. System Management Utilities: Opción 12, ″Change Management″
   c. Change Management Software Control: Opción 12, ″XMODEM software″
   d. Select type: ″Load Image″
   e. Select bank: elija Bank A (Banco A) o Bank B (Banco B)

   El firmware le indica cuándo debe iniciar la transferencia de archivos.
3. Vaya al paquete de emulación de terminal e inicie la transferencia del archivo LML.ld desde el servidor de estación de trabajo.
4. Después de transferir LML.ld, deberá transferir de uno en uno los demás módulos ″.ld″ de la estación de trabajo. LML.ld debe ser el primero, pero después de éste el orden de los demás no importa. Deberá incluir Firm.ld.

   Al empezar la transferencia de archivos, el estado del banco cambia a CORRUPT, para indicar que no contiene una carga de código válida completa. Cuando el Network Utility ha recibido el último módulo de carga, el estado del banco cambia a AVAIL. Puede verificar si esto ha sucedido utilizando la opción 7, ″List Software″, en el menú de firmware Change Management.
5. Arranque el direccionador utilizando el código-op que acaba de cargar.

   Utilice la Opción 9 ″Set Boot Information″ para seleccionar el nuevo banco de código-op (y configuración) desde el que arrancará. Pulse **Esc** para acceder al menú principal y, a continuación, **F9** para arrancar el Network Utility con el nuevo código-op.

Utilización de TFTP

El procedimiento de firmware para utilizar TFTP para transferir archivos de código-op y firmware a un disco duro de Network Utility es el siguiente:

1. Acceda al menú principal de firmware utilizando los procedimientos descritos en el apartado “Opciones de arranque: Arranque rápido y obtención de firmware” en la página 46.
2. Configure las direcciones IP que va a utilizar:

   Siga la secuencia de menús:
   a. System Management Services (menú principal): Opción 4, ″Utilities″
   b. System Management Utilities: Opción 11, ″Remote Initial Program Load Setup″
   c. Parámetros de red: Opción 1, ″IP Parameters″

Establezca las direcciones siguientes:
- Dirección IP de cliente: dirección IP para la tarjeta de LAN del Network Utility. Ésta es una dirección temporal que no necesita estar relacionada con la dirección de operación del direccionador para esa interfaz.
- Dirección IP de servidor: dirección IP del adaptador de LAN de la estación de trabajo
- Dirección IP de pasarela: dirección IP de cualquier direccionador intermedio o, si no hay ninguna, repita la dirección IP de la estación de trabajo
- Máscara de red: máscara para la subred conectada a la tarjeta de LAN del Network Utility

3. Inicie la transferencia mediante estas selecciones de menú:
   a. System Management Services (menú principal): Opción 4, ″Utilities″
   b. System Management Utilities: Opción 12, ″Change Management″
   c. Change Management Software Control: Opción 10, ″TFTP software″
   d. Select Type: ″Load Image″
   e. Select Bank: elija Bank A (Banco A) o Bank B (Banco B)
   f. Select Load Type: ″Modules″
4. Entre la vía de acceso en la estación de trabajo al directorio que contiene todos los módulos de carga.
5. Si se le solicita, seleccione la interfaz mediante la cual desea que el firmware efectúe la transferencia de archivos.

   El firmware transfiere de uno en uno cada módulo de carga y proporciona mensajes de estado. Cuando haya terminado, volverá al menú Change Management.
6. Arranque el direccionador utilizando el código-op que acaba de cargar.

   Utilice la Opción 9 ″Set Boot Information″ para seleccionar el nuevo banco de código-op (y configuración) desde el que arrancará. Pulse **Esc** para acceder al menú principal y, a continuación, **F9** para arrancar el Network Utility con el nuevo código-op.

Actualización del firmware

Introducción

El firmware es software de bajo nivel que controla la lógica de encendido y arranque del Network Utility. Reside en la memoria instantánea no volátil en lugar de en el disco duro, de modo que en caso de producirse una anomalía, por ejemplo la carga en disco de software de operación, pueda recuperar archivos de configuración y software nuevos y volver a estar activo y en ejecución. *Actualizar* el firmware significa grabar una nueva versión del mismo en la memoria instantánea, sustituyendo la versión anterior.

Es necesario actualizar el firmware en dos circunstancias:

1. IBM envía un PTF o EPTF necesario para arreglar un problema y dicho PTF o EPTF necesita una actualización del firmware. La documentación asociada con cada PTF o EPTF indica si es necesario o no la actualización del firmware.
2. Desea instalar un nuevo release funcional de MAS. Para pasar a un nuevo release se necesita casi siempre una actualización del firmware.

En las páginas Web de bajada de código de Network Utility, no existen archivos independientes que contengan nuevas versiones del firmware. En lugar de ello, el firmware es uno de los módulos de carga empaquetados en los archivos .zip y .tar junto con los módulos de carga de código de operación. El módulo de carga de

firmware tiene el nombre de archivo ″Firm.ld″. Cada PTF y EPTF contiene un nuevo archivo Firm.ld, incluso si el contenido de ese archivo es igual al de un nivel de mantenimiento anterior.

Al seguir los procedimientos descritos en el apartado “Bajada y desempaquetado de archivos” en la página 111 y el apartado “Carga de código de operación nuevo” en la página 112, se baja una nueva versión de firmware de la web y se transfiere al Banco A o Banco B del disco duro. La colocación de Firm.ld en un banco de disco y el rearranque desde dicho banco no tienen en absoluto ningún efecto en el firmware activo, que se ejecuta desde la memoria instantánea. Para actualizar a firmware nuevo, deberá grabar el nuevo firmware en la memoria instantánea.

Visión general de los procedimientos

Existen dos métodos generales para bajar firmware nuevo de la Web y colocarlo en la memoria instantánea del Network Utility. El método recomendado consiste en realizar la actualización de firmware junto con la instalación del nuevo código de operación, como se indica a continuación:

1. Baje el nivel de mantenimiento nuevo del código-op y del firmware de la Web a un servidor local, como se describe en el apartado “Bajada y desempaquetado de archivos” en la página 111.
2. Transfiera los nuevos ″.ld″ de código-op y firmware a un banco del disco duro del Network Utility, utilizando uno de los procedimientos TFTP o Xmodem descritos en el apartado “Carga de código de operación nuevo” en la página 112.
3. Grabe en la memoria instantánea la copia de Firm.ld que ya está ahora en disco, utilizando uno de los procedimientos descritos en el apartado “Procedimientos de disco local”.

Además del método recomendado, también puede transferir sólo el firmware al Network Utility de forma independiente y grabarlo en la memoria instantánea sin transferir ni activar también el código de operación. Para ello, efectúe lo siguiente:

1. Baje el nivel de mantenimiento nuevo del código-op y del firmware de la Web a un servidor local, como se describe en el apartado “Bajada y desempaquetado de archivos” en la página 111. No existe ningún modo de bajar sólo el firmware de la Web, porque está empaquetado con el código de operación.
2. Transfiera sólo Firm.ld a una ubicación que no sea un banco del disco duro de Network Utility y grábelo en la memoria instantánea en el mismo procedimiento. Puede utilizar Xmodem o TFTP para la transferencia de archivos, como se describe en el apartado “Procedimientos de transferencia de archivos” en la página 119.

La transferencia independiente de firmware no es el método de actualización recomendado, simplemente porque duplica la transferencia de archivo Firm.ld que ya se ha efectuado al instalar el código de operación nuevo en el banco A o B del disco duro. Los procedimientos de disco local son más rápidos y más simples.

Procedimientos de disco local

Siga uno de estos procedimientos después de haber transferido ya un nuevo conjunto de código de operación y firmware al banco A o B del disco duro, para activar el firmware en ese banco del disco.

Utilización del código de operación

Nota: Este procedimiento sólo está disponible cuando se está ejecutando el código de operación MAS V3.2 o posterior. Si va a instalar dicho nivel por primera vez, deberá rearrancar en el nuevo código de operación antes de poder utilizar este procedimiento para actualizar el firmware al mismo nivel.

1. Escriba **talk 6** y, a continuación, **boot** para activar el subproceso Config de arranque.
2. Escriba **update** para iniciar la actualización de firmware
3. Cuando se le solicite, seleccione el banco (A o B) al que ha transferido el nuevo nivel de código de operación y firmware.

   Existe también una opción ″P″, que se puede utilizar para volver a grabar en la memoria instantánea un nivel de firmware válido que se ha guardado anteriormente en disco (no en el banco A ni en el B). Puede seleccionar esto si la memoria instantánea se corrompe (quizá el sistema se ha quedado sin alimentación durante una grabación en memoria instantánea) y desea volver al nivel de firmware anterior.
4. El sistema graba en la memoria instantánea el nuevo nivel de firmware desde la ubicación de origen especificada y crea automáticamente una ″imagen de recuperación″ nueva (la que se ha seleccionado con ″P″) según sea oportuno. No apague la alimentación del Network Utility mientras se esté actualizando el firmware en la memoria instantánea.

El mandato **update** graba el nuevo nivel de firmware en la memoria instantánea, pero el firmware actualizado no empieza a ejecutarse hasta el siguiente rearranque. Por consiguiente, el modo más fácil de instalar un nuevo nivel de mantenimiento que requiere actualización de firmware desde el indicador `Boot config>` es el siguiente:

1. Utilice **tftp get load m** para transferir el código-op y el firmware nuevos a disco
2. Utilice **update** para grabar el nuevo firmware en la memoria instantánea
3. Utilice **copy** para copiar el archivo de configuración en el nuevo banco de código
4. Utilice **set** para seleccionar el nuevo banco de código para el siguiente arranque
5. Teclee **Control-p** y luego **reload** para rearrancar el Network Utility para utilizar el nuevo firmware y el nuevo código de operación al mismo tiempo.

Utilización del firmware

Una vez que ha transferido un nuevo nivel de código de operación y firmware al banco A o B del disco, rearranque para utilizar el nuevo código de operación pero deténgase en el firmware anterior para grabar en la memoria instantánea el firmware nuevo de este modo:

1. Acceda al menú principal de firmware utilizando los procedimientos descritos en el apartado “Opciones de arranque: Arranque rápido y obtención de firmware” en la página 46.
2. Seleccione las opciones del menú en la secuencia siguiente:
   a. System Management Services (menú principal): Opción 4, ″Utilities″
   b. System Management Utilities: Opción 7, ″Update System Firmware″
   c. F/W Update Options: Opción 3, ″Use a Local Image File″

   El firmware solicita un nombre de archivo local. Entre uno de:
   c:\sys0\firm.ld para el Banco A
   c:\sys1\firm.ld para el Banco B

3. Responda ″yes″ a la pregunta ″Do you want to continue?″ Entonces el firmware empieza a grabar el nuevo firmware en la memoria instantánea.
4. Espere y no apague el sistema mientras continúa la actualización.
5. Al terminarse, pulse **Intro** para reiniciar el sistema. El nuevo firmware arrancará con el código de operación nuevo si ha habilitado el arranque automático en el paso 1 de este procedimiento.

Procedimientos de transferencia de archivos

Siga uno de estos procedimientos para transferir sólo el firmware de un servidor TFTP o Xmodem local al Network Utility y para activar dicho firmware. Tal como se muestra en la Tabla 10-2, se utiliza la interfaz de usuario de firmware anterior en ambos procedimientos para iniciar la transferencia de archivos a través de cualquiera de los diversos tipos de conexión. Como se ha descrito en el apartado “Visión general de los procedimientos” en la página 117, los procedimientos de disco local pueden ser más rápidos que estos procedimientos.

Tabla 16. Carga de firmware

Conexión física	Protocolo de línea	Protocolo de transferencia	Herramienta	Direcciones IP por omisión
Puerto servicio + módem nulo Puerto servicio + módem ext Módem PCMCIA	Terminal asínc	Xmodem	Firmware	No aplicable
PCMCIA EtherJet LIC Ethernet (10 Mbps) LIC Red en Anillo	IP	TFTP	Firmware	Network Utility=10.1.0.2 Estación de trabajo=10.1.0.3

Utilización de Xmodem

El procedimiento de firmware para utilizar Xmodem para transferir archivos de código-op y firmware a un disco duro de Network Utility es el siguiente:

1. Acceda al menú principal de firmware utilizando los procedimientos descritos en el apartado “Opciones de arranque: Arranque rápido y obtención de firmware” en la página 46.
2. Seleccione las opciones del menú en la secuencia siguiente:
   a. System Management Services (menú principal): Opción 4, ″Utilities″
   b. System Management Utilities: Opción 12, ″Change Management″
   c. Change Management Software Control: Opción 12, ″XMODEM software″
   d. Select type: ″Load Image″
   e. Select bank: elija Bank A o Bank B

   El firmware le indica cuándo debe iniciar la transferencia de archivos.
3. Vaya al paquete de emulación de terminal e inicie la transferencia del archivo LML.ld desde el servidor de estación de trabajo.
4. Después de transferir LML.ld, deberá transferir de uno en uno los demás módulos ″.ld″ de la estación de trabajo. LML.ld debe ser el primero, pero después de éste el orden de los demás no importa. Deberá incluir Firm.ld.

   Al empezar la transferencia de archivos, el estado del banco cambia a CORRUPT, para indicar que no contiene una carga de código válida completa. Cuando el Network Utility ha recibido el último módulo de carga, el estado del banco cambia a AVAIL. Puede verificar si esto ha sucedido utilizando la opción 7, ″List Software″, en el menú de firmware Change Management.
5. Arranque el direccionador utilizando el código-op que acaba de cargar.

Utilice la Opción 9 ″Set Boot Information″ para seleccionar el nuevo banco de código-op (y configuración) desde el que arrancará. Pulse **Esc** para acceder al menú principal y, a continuación, **F9** para arrancar el Network Utility con el nuevo código-op.

Utilización de TFTP

El procedimiento de transferencia y actualización de archivos de firmware utilizando TFTP es el siguiente:

1. Acceda al menú principal de firmware utilizando los procedimientos descritos en el apartado “Opciones de arranque: Arranque rápido y obtención de firmware” en la página 46.
2. Configure las direcciones IP que va a utilizar:

   Siga la secuencia de menús:
   a. System Management Services (menú principal): Opción 4, ″Utilities″
   b. System Management Utilities: Opción 11, ″Remote Initial Program Load Setup″
   c. Parámetros de red: Opción 1, ″IP Parameters″

   Establezca las direcciones siguientes:
   - Dirección IP de cliente: dirección IP para la tarjeta de LAN del Network Utility. Ésta es una dirección temporal que no necesita estar relacionada con la dirección de operación del direccionador para esa interfaz.
   - Dirección IP de servidor: dirección IP del adaptador de LAN de la estación de trabajo
   - Dirección IP de pasarela: dirección IP de cualquier direccionador intermedio o, si no hay ninguna, repita la dirección IP de la estación de trabajo
   - Máscara de red: máscara para la subred conectada a la tarjeta de LAN del Network Utility
3. Inicie la transferencia con la secuencia siguiente de selecciones de menú:
   a. System Management Services (menú principal): Opción 4, ″Utilities″
   b. System Management Utilities: Opción 7, ″Update System Firmware″
   c. F/W Update Options: Opción 1, ″TFTP a Remote Image File″

   Entre los nombres de archivo siguientes:
   - Nombre de archivo local: elija un nombre para un archivo temporal que se almacenará en el directorio raíz del disco duro del Network Utility. No proporcione ningún nombre de vía de acceso. Utilice una extensión de nombre de archivo de 3 caracteres o menos.
   - Nombre de archivo remoto: vía de acceso y nombre de archivo (que debe ser ″Firm.ld″) del módulo de carga de firmware de la estación de trabajo. Deberá estar en el directorio donde ha desempaquetado el archivo .zip o .tar que ha bajado de la Web.

   Después de seleccionar el adaptador y el puerto que deberá utilizar el firmware, el direccionador inicia la operación de obtención de TFTP.
4. Cuando TFTP se complete, responda ″yes″ a la pregunta ″Do you want to continue?″ en la consola de firmware. Entonces el firmware empezará a grabar el nuevo firmware en la memoria instantánea.
5. Espere y no apague el sistema mientras continúa la actualización.
6. Al terminarse, pulse **Intro** para reiniciar el sistema. El nuevo firmware arrancará con el código de operación actual.

Cómo solicitar soporte y servicio

Si ha comprado el Network Utility en un concesionario o business partner de IBM, póngase en contacto con ellos para averiguar cómo recibir soporte y servicio.

Si ha comprado el Network Utility en IBM, están disponibles las siguientes formas de ayuda:

- Servicio y soporte de problemas de hardware o código

  Para obtener soporte telefónico:
  - En EE.UU. - llame al 1 800 IBM-SERV (1 800 426–7378).
  - Fuera de EE.UU. - póngase en contacto con el servicio técnico de IBM local para obtener el número de teléfono de su país.

  Antes de llamar, tenga disponibles el tipo de máquina, el modelo y el número de serie de la placa posterior del Network Utility. Si tiene un problema de software, puede que necesite tener disponibles un servidor TFTP y una conexión de Internet para transferir un vuelco de memoria del Network Utility y enviarlo al personal de soporte de IBM.

  También puede acceder al soporte y servicio de IBM a través de la World Wide Web en:

  `http://www.networking.ibm.com/support/networkutility`

  Seleccione el producto Network Utility para obtener indicaciones técnicas, sugerencias, FAQ y actualizaciones de código del producto. Además, puede suscribirse para recibir notificación de las futuras actualizaciones de código.
- Ayuda para la configuración y preguntas sobre cómo realizar tareas para instalaciones iniciales
  - En EE.UU. - llame al 1 800 IBM-SERV (1 800 426-7378). Este servicio es gratuito.
  - Fuera de EE.UU. - póngase en contacto con el servicio técnico de IBM local. Este servicio puede no ser gratuito fuera de EE.UU.
- Contratos de servicio y soporte para diseño, planificación o determinación de problemas de red
  - En EE.UU. - llame al 1-800-IBM-SERV (1 800 426-7378).
  - Fuera de EE.UU. - póngase en contacto con el servicio técnico de IBM local.

Parte 3. Datos específicos de configuración y gestión

Capítulo 11. Visión general

Este capítulo es una introducción a la parte del manual titulada “Parte 3. Datos específicos de configuración y gestión” en la página 123. Proporciona una visión general de las posibles aplicaciones del Network Utility y describe cómo documentan los demás capítulos algunas de estas aplicaciones.

Funciones principales del Network Utility

Mediante la utilización de la tecnología de software Multiprotocol Access Services de IBM el Network Utility soporta diversas funciones de red. El Network Utility está específicamente diseñado para funciones que utilizan de forma intensiva la CPU y la memoria en posiciones de red que necesitan un pequeño número de interfaces físicas.

Las aplicaciones clave del Network Utility por modelo incluyen:

Modelo TN1 - Servidor TN3270E de Network Utility

Servidor TN3270E

La función de Servidor TN3270E proporciona acceso de aplicación de sistema principal SNA a los usuarios de escritorio IP.

Se pueden colocar uno o más Network Utilities en una oficina regional o un centro de datos de sistema principal para proporcionar acceso para un número mediano a grande de clientes TN3270 distribuidos por toda una red IP.

Network Utility Modelo TN1 también soporta todas las funciones del Modelo TX1.

Modelo TX1 - Transporte de Network Utility

Conmutación de enlace de datos (Data Link Switching (DLSw)

DLSw proporciona conectividad de estación final SNA nativa (estación de trabajo, controlador, FEP o sistema principal) en redes troncales IP. También efectúa conversión de tipo DLC como la que se realiza en productos FRAD y X.25 PAD.

Se pueden colocar uno o más Network Utilities en una oficina regional o un centro de datos de sistema principal para terminar conexiones TCP de direccionadores DLSw más pequeños en muchas sucursales.

Red avanzada de igual a igual (Advanced Peer to Peer Networking) (APPN)

APPN proporciona conectividad de estación final SNA nativa (estación de trabajo, controlador, FEP o sistema principal) en redes troncales SNA. La característica *Enterprise Extender* permite esta misma conectividad en redes troncales IP.

Se pueden colocar Network Utilities en cualquier lugar donde se necesite un nodo de red APPN de alta capacidad. Puede colocar uno en el borde una red IP para recibir tráfico de otros productos Enterprise Extender. Un Network Utility también puede proporcionar la función ampliada de nodo de borde cuando conecta dos redes APPN diferentes.

Pasarela de canal (Channel Gateway)

El Network Utility soporta adaptadores ESCON (cable de fibra óptica) y de Canal paralelo (cable de código y bus). Mediante el uso de uno de estos adaptadores, un Network Utility puede servir de pasarela direccionando el tráfico SNA e IP de un sistema principal S/390 a las LAN locales, a una red ATM o a una línea serie de alta velocidad.

Asignador de tareas de red (Network Dispatcher)

Esta función permite a diversos servidores de aplicaciones basados en IP (por ejemplo, servidores TN3270, servidores web HTTP o servidores FTP) presentar una sola aparición de dirección IP a estaciones de trabajo clientes de una intranet o de Internet. La función de asignador de tareas de red contesta satisfactoriamente las peticiones de conexión TCP de estos clientes y las direcciona a un servidor disponible. Proporciona equilibrio de carga entre los servidores y alta disponibilidad de ″servidor lógico″ ignorando los servidores físicos anómalos.

El Network Utility puede colocarse en un centro de datos de sistema principal delante de los sistemas principales que proporcionan estas funciones de servidor o delante de múltiples Network Utility Modelo TN1 que estén proporcionando función de Servidor TN3270E.

Conversión de soporte de alta velocidad

El Network Utility puede servir de puente de alta velocidad entre interfaces en sus adaptadores soportados.

Red privada virtual (Virtual Private Networking) (VPN)

La función VPN consta de un conjunto de protocolos de túnel y seguridad: L2TP, L2F, PPTP, IPSEC, IKE, PKI, Diffserv y LDAP. Si se toman juntos, estos protocolos permiten configurar a un Network Utility para que utilice la Internet pública como una extensión de la propia red privada de una empresa en lugar de utilizar las WAN y las LAN. Cuando se configura de este modo, el Network Utility puede actuar como punto de terminación de túnel para el tráfico de red en las oficinas remotas, los proveedores y los clientes de una empresa. Las políticas de seguridad configuradas en el direccionador determinan dinámicamente si el tráfico de red necesitar autentificarse y/o cifrarse o si puede fluir fuera de peligro. Las políticas de seguridad aseguran que los datos de empresa puedan moverse por la red pública de forma tan segura, fiable y flexible como si estuvieran pasando por líneas privadas y con unos ahorros de coste significativos.

El Network Utility puede colocarse en el punto límite entre Internet y la intranet de una empresa para terminar un gran número de túneles de la Capa 2 o IPSEC. Estos túneles se convierten en una extensión de la red de empresa, potenciando la economía y ubicuidad de la Internet pública.

En este manual, hemos seleccionado un subconjunto clave de las funciones mencionadas más arriba para proporcionar amplias descripciones y configuraciones de ejemplo. Los capítulos que vienen a continuación incluyen:

- Servidor TN3270E, opcionalmente con Asignador de tareas de red delante de múltiples servidores
- Pasarela de canal, para tráfico SNA e IP
- Conmutación de enlace de datos, con terminación TCP y conversión DLC local
- Redes privadas virtuales

Para obtener ayuda en la interpretación y configuración de las funciones de Network Utility distintas de éstas, consulte las publicaciones de software esenciales:

- *MAS Consulta de configuración y supervisión de protocolos Volumen 1*
- *MAS Consulta de configuración y supervisión de protocolos Volumen 2*
- *MAS Utilización y configuración de las características*
- *MAS Guía del usuario de software*

También puede encontrar ayuda de configuración en los Redbooks de IBM siguientes. Aunque los escenarios de configuración son específicos del IBM 2216 Modelo 400, puede que se apliquen algunos de ellos.

- *IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios Volume 1* (SG24-4957)
- *IBM 2210 Nways Multiprotocol Router and IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios Volume 2* (SG24-4956)

Diseño y convenios de los capítulos

Los capítulos 12 a 20 de este manual están organizados del modo siguiente.

Diseño de los capítulos

Cada una de las cuatro funciones clave (Servidor TN3270E, Pasarela de canal, Conmutación de enlace de datos y VPN) está cubierta por dos capítulos:

- Un capítulo de introducción que:
  - Resume la función soportada
  - Describe configuraciones de red de ejemplo
  - Introduce el modo de gestionar la función
- Un capítulo de ″Detalles de configuración de ejemplo″ que contiene:
  - Diagramas con etiquetas de configuraciones clave de ejemplo
  - Tablas coincidentes con parámetros de configuración para usuarios del Programa de configuración y usuarios de la línea de mandatos

  Las configuraciones mostradas y descritas en los cuatro capítulos ″Configuración de ejemplo ″ son configuraciones de trabajo reales. Los archivos de configuración binarios que coinciden con estas configuraciones se pueden bajar de la World Wide Web. Para acceder a estos archivos, siga los enlaces `Support` y `Downloads` desde:

  `http://www.networking.ibm.com/networkutility`

Además, el “Capítulo 18. Definiciones de sistema principal de ejemplo” en la página 259 proporciona ejemplos detallados para configurar productos de software de sistema principal de IBM para que coincidan con las configuraciones de Network Utility.

Convenios de las tablas de configuración de ejemplo

Las tablas de parámetros de configuración utilizadas en los cuatro capítulos ″Configuración de ejemplo″ siguen todas el mismo formato. Los convenios y las columnas de tabla son los siguientes:

Navegación por el programa de configuración
: Secuencia de nombres de carpeta y panel a seguir hasta obtener el panel donde se entran valores de parámetros.

Valores del programa de configuración
: Nombres de parámetros y sus valores.

Si el panel del programa de configuración muestra parámetros no listados en la tabla, se han utilizado sus valores por omisión.***La configuración debe ser para un Network Utility y no un 2216-400 para tener los valores por omisión correctos.***

Mandatos de la línea de mandatos

Mandatos que se escriben para configurar los mismos parámetros utilizando la interfaz de la línea de mandatos, como se indica a continuación:

- Las secuencias de mandatos se inician desde el indicador de talk 6 `Config>`. Cuando es necesario, el mandato inicial muestra cómo llegar al lugar adecuado en el sistema de menús y el indicador de mandatos resultante.
- Los mandatos sin parámetros especificados solicitarán los valores de entrada o bien no tienen parámetros. Las solicitudes de parámetros del sistema se muestran en `este font`.
- En los lugares donde las solicitudes de valores y los valores que se escriben son autoexplicativos, no se muestran los detalles.
- ″Acepte otros valores por omisión″ significa que hay otras solicitudes de parámetros para las que debe aceptar los valores por omisión (pulsando **Intro**).

Notas Números que hacen referencia a comentarios en la parte inferior de cada tabla.

Capítulo 12. Servidor TN3270E

Visión general

Esta sección introduce el TN3270 y resume la función de servidor TN3270E implementada en el Network Utility.

¿Qué es el TN3270?

En la actualidad muchas compañías están considerando la posibilidad de consolidar el tráfico de WAN en una red troncal individual sólo IP. Al mismo tiempo, otras compañías están simplificando las configuraciones de estación de trabajo e intentando ejecutar sólo la pila de protocolos TCP/IP en el escritorio. Sin embargo, la mayoría de estas compañías aún necesitan acceso a sistemas principales de aplicación SNA.

El TN3270 cumple estos requisitos al permitirle ejecutar IP desde el escritorio a través de la red y conectarse al sistema principal SNA a través de un servidor TN3270. Los clientes se conectan al servidor utilizando una conexión TCP. El servidor proporciona una función de pasarela para los clientes TN3270 en sentido directo correlacionado las sesiones de cliente a sesiones LU-LU dependientes de SNA que el servidor mantiene con el sistema principal SNA. El servidor TN3270 maneja la conversión entre la corriente de datos TN3270 y una corriente de datos SNA 3270.

Para utilizar una solución TN3270, instale software de cliente TN3270 en estaciones de trabajo de escritorio[13] y software de servidor TN3270 en uno de los diversos lugares descritos más abajo. El software de cliente está disponible en IBM y muchos otros proveedores y se ejecuta sobre la pila TCP/IP en la estación de trabajo. Un determinado producto cliente proporciona uno de dos niveles posibles de soporte de estándares:

- Cliente TN3270 base

  Estos clientes cumplen con RFC 1576 (Prácticas actuales TN3270) y/o RFC 1646 (Extensiones TN3270 para nombre de LU y Selección de impresora).
- Cliente TN3270E

  Estos clientes cumplen con RFC 1647 (Mejoras TN3270) y RFC 2355 (Mejoras TN3270).

Una implementación de servidor que puede soportar clientes TN3270E se denomina servidor TN3270E.

Colocación de la función de servidor TN3270

La función de servidor TN3270 puede colocarse en diversos productos y posiciones dentro de una red, que incluyen:

- En el propio sistema principal SNA

  IBM y otros diversos proveedores proporcionan software de servidor TN3270 de sistema principal que se coloca sobre la pila TCP/IP de sistema principal y se conecta dentro del sistema principal con VTAM.
- En un direccionador o Network Utility de la red

13. También puede encontrar pequeños productos cliente TN3270 dedicados que representan impresoras.

IBM y otros proveedores proporcionan la función de servidor TN3270 en productos de hardware de red. Puede colocar dichos productos directamente adyacentes al sistema principal SNA o en cualquier posición de la red donde tenga conectividad SNA con el sistema principal. Si está utilizando direccionadores IBM (2210 ó 2216) o Network Utilities y el sistema principal está ejecutando APPN, puede utilizar la tecnología de Enterprise Extender para colocar el servidor en cualquier posición donde tenga conectividad IP con el sistema principal.

- En un producto de software de la red

  IBM y otros proveedores proporcionan productos de software de servidor TN3270 que se instala en servidores de gama media que utilizan sistemas operativos como, por ejemplo, AIX, OS/2 o Windows/NT. Puede colocar estos productos en cualquier posición de la red donde tenga conectividad SNA con el sistema principal de aplicación.

La elección de la posición de red y del producto servidor TN3270 es compleja e incluye factores como los siguientes:

- Capacidad del sistema principal e impacto de ciclo
- Precio para el rendimiento y la capacidad
- Disponibilidad
- Impacto de anomalía de servidor
- Escalabilidad

El Network Utility proporciona una implementación de servidor TN3270E de alto rendimiento que se ajusta proporcionalmente a redes grandes. Combinándola con la característica Asignador de tareas de red, puede implementar redundancia de servidor y compartimiento de carga en grandes instalaciones TN3270. También puede colocar un Network Utility en una red SNA o IP lejos del centro de datos y obtener las mismas ventajas de escalabilidad, adición incremental e impacto reducido por anomalía de servidor.

Función de servidor TN3270E de Network Utility

Cumplimiento de estándares

La implementación del servidor TN3270E de Network Utility soporta estos RFC:

RFC 1576 - Prácticas actuales de TN3270
RFC 1646 - Extensiones de TN3270 para nombres de LU e impresoras
RFC 1647 - Mejoras de TN3270
RFC 2355 - Mejoras de TN3270 (deja obsoleto el RFC 1647)

Puede manejar los clientes TN3270 base y TN3270E al mismo tiempo.

Conectividad al sistema principal

Como se ha mencionado anteriormente, la vía de acceso desde un cliente TN3270 al sistema principal SNA consta de dos partes:

- Una conexión TCP a través de IP del cliente al servidor
- Una sesión LU-LU SNA del servidor al sistema principal

La forma de la conexión SNA del servidor al sistema principal depende del modo en que el servidor representa las PU y las LU dependientes. Cuando utilice el Network Utility como servidor TN3270, puede configurar de uno de dos modos diferentes para establecer enlaces y representar las PU y las LU en VTAM:

- Mediante la utilización de enlaces de subárea SNA

Configure el Network Utility de este modo cuando no esté ejecutando APPN en el sistema principal. Puede configurar un enlace de capa DLC independiente con el sistema principal para cada PU (un máximo de 253 LU). Múltiples PU requieren múltiples enlaces paralelos con el sistema principal. Las tramas SNA que llegan al Network Utility en uno de estos enlaces fluyen directamente a la PU interna correspondiente.

Los enlaces con el sistema principal de subárea deben ser un solo salto de capa DLC al producto que proporciona la función de límite de subárea SNA. Normalmente este producto es NCP ejecutándose en un FEP o el propio VTAM en el sistema principal. El enlace de subárea del Network Utility puede atravesar puentes u otros mecanismos de reenvío de la capa DLC (por ejemplo conversores de protocolo o direccionadores DLSw externos). El Network Utility soporta los tipos de enlace siguientes para la conexión de sistema principal de subárea:

- Red en Anillo: física, emulación ATM de LAN o LSA de canal
- Ethernet: física, emulación ATM de LAN o LSA de canal
- FDDI: sólo física
- PVC de Frame relay: formatos RFC 1490/2427 en puentes o direccionados
- DLSw

- Mediante la utilización de un enlace DLUR (Dependent LU Requester) (Peticionario de LU dependiente) de APPN

  Configure el Network Utility de este modo cuando esté ejecutando APPN con su función DLUS (Dependent LU Server) (Servidor de LU dependiente) en el sistema principal. Configure un enlace de la capa DLC con el sistema principal para transportar el ″conducto″ DLUR-DLUS, aunque esté definiendo múltiples PU locales. Las tramas SNA que llegan al Network Utility en este enlace fluyen a la función DLUR, que las redirige a la PU interna correcta.

  Cuando esté utilizando DLUR, podrá direccionar a través de una red APPN utilizando el direccionamiento ISR o HPR para alcanzar el sistema principal. El Network Utility soporta los tipos de enlace siguientes como enlace APPN de ″primer salto″ con el sistema principal:

  - Red en Anillo: física, emulación ATM de LAN o LSA de canal
  - Ethernet: física, emulación ATM de LAN o LSA de canal
  - FDDI: sólo física
  - PVC de Frame relay: formatos RFC 1490/2427 en puentes o direccionados
  - ATM (nativo, no emulación de LAN): sólo HPR
  - MPC+ de canal: sólo HPR
  - PPP
  - SDLC: sólo ISR
  - X.25: sólo ISR
  - DLSw: sólo ISR
  - IP (Enterprise Extender): sólo HPR

  Observe especialmente que cuando se utiliza el direccionamiento DLUR y HPR, se puede colocar un servidor TN3270E de Network Utility a través de una red IP desde el sistema principal de aplicación SNA. Enterprise Extender mantiene la clase de servicio a nivel de sesión y la prioridad de transmisión a través de la red IP.

Configuración general de servidor TN3270E

Esta sección contiene información general acerca de la configuración del soporte de servidor TN3270 de Network Utility. Para ver configuraciones específicas de ejemplo, consulte la página 138.

Configuración de subárea TN3270 bajo el protocolo APPN

En la implementación del servidor TN3270 de Network Utility, todas las funciones SNA están empaquetadas dentro del protocolo APPN. Esto significa que *incluso cuando esté configurando la conexión de subárea SNA y el sistema principal SNA no esté ejecutando APPN*, deberá utilizar los servicios de configuración y consola del protocolo APPN. En concreto:

- Deberá pasar por el protocolo APPN en la línea de mandatos y el Programa de configuración para configurar puertos, enlaces y funciones de servidor TN3270
- Deberá pasar por el protocolo APPN en la línea de mandatos para utilizar los mandatos de supervisión de TN3270
- De todos modos deberá configurar APPN a nivel de nodo

Al configurar soporte de subárea SNA, de hecho el Network Utility aún funciona como un nodo de red APPN, pero sólo en enlaces con otros nodos APPN. Si los *únicos* puertos y enlaces que configura son los destinados a la conexión de sistema principal de subárea SNA, la función APPN no sirve para nada.

Configuración en el entorno APPN

APPN y el servidor TN3270 son totalmente configurables desde el Programa de configuración y desde la línea de mandatos. Desde el Programa de configuración, los parámetros de configuración de TN3270 están siempre disponibles. Si crea una configuración TN3270 y la baja a un Network Utility Modelo TX1, que no soporta la función de servidor TN3270, el Network Utility ignorará la parte TN3270 de la configuración. Si está trabajando desde la línea de mandatos en un Modelo TX1, los mandatos para configurar y supervisar TN3270 simplemente no aparecen en los menús de APPN.

Para cambiar una configuración APPN/TN3270 desde el Programa de configuración, efectúe el cambio, transfiera la configuración al Network Utility y rearranque para que el cambio entre en vigor.

Para cambiar una configuración APPN/TN3270 desde la línea de mandatos, vaya a talk 6, escriba **p appn** y, a continuación, emita los mandatos para efectuar el cambio. Tiene dos opciones para activar el cambio:

- Grabe la configuración en disco y rearranque el Network Utility para activarla.
- Emita el mandato APPN **activate** de talk 6 para activar dinámicamente la configuración APPN/TN3270 modificada.

  En función de los elementos de configuración que cambie, APPN efectuará el cambio inmediatamente o reiniciará APPN (pero no el Network Utility entero) para activar el cambio. En el último caso, si va a talk 5 y escribe **p appn** mientras se está reiniciando APPN, obtendrá el mensaje `APPN is not currently active` (APPN no está activo actualmente). Puede sondear con los mandatos de talk 5 para ver cuándo se ha completado el reinicio.

Denominación y correlación implícitas y explícitas de LU

Al configurar la función de servidor TN3270 del Network Utility, se crea un nombre de LU local para cada una de las sesiones de cliente simultáneas potenciales que el Network Utility está destinado a soportar. No es necesario que el nombre de LU definido en el Network Utility tenga ninguna relación con los nombres de LU en VTAM.

Cuando un cliente TN3270 se conecta a un servidor a través de TCP, puede solicitar un nombre de LU específico o puede realizar una petición genérica para cualquier LU de un tipo determinado. Si se está configurando un cliente para solicitar un nombre específico, se especifica uno de los nombres locales definidos en el servidor (Network Utility), no un nombre de LU VTAM.

Dado que un solo Network Utility puede soportar miles de LU con características similares, no es necesario configurar individualmente cada LU. En lugar de ello, se puede crear una gran agrupación de LU *implícitas* para satisfacer a los clientes que no solicitan un nombre de LU determinado. A continuación se añade un pequeño número de LU *explícitas* para satisfacer a los clientes que sí solicitan un nombre determinado[14].

Como podrá verá en las configuraciones de ejemplo, las LU implícitas se definen en grupos a medida que se define cada PU local. Especifique una máscara de nombre de LU, el número de LU y a qué agrupación pertenecen las LU. Para configurar una LU explícita, especifique un nombre de LU y una dirección NAU (2-254). Cuando el Network Utility activa la configuración, reserva las direcciones NAU para las LU explícitas y luego genera nombres para las LU implícitas utilizando la máscara de nombre de grupo y una de las direcciones NAU disponibles.

El PTF01 de MAS V3.2 introdujo diversas mejoras funcionales significativas en el área de definición de LU y correlación de cliente:

- Puede definir agrupaciones de LU con nombre.

  La agrupación de LU es una mejora en la función de servidor TN3270E que facilita la configuración de algunas redes TN3270E. Esta función le permite agrupar las LU SNA en “agrupaciones” con nombre. Entonces, los clientes TN3270E pueden solicitar una conexión utilizando el nombre de la agrupación como un nombre de LU. Entonces el servidor TN3270E elegirá una LU de la agrupación especificada para servir la petición del cliente.
- Puede configurar correlaciones entre direcciones IP de cliente y nombres de LU o de agrupación de LU.

  La función de Correlación de dirección IP de cliente con nombre de LU del servidor TN3270E proporciona un mecanismo para que los administradores controlen el acceso de cliente a las LU del servidor TN3270E.

  La correlación mejora la administración central al permitir al administrador configurar qué subredes o dirección IP de cliente de recursos SNA (LU o Agrupación) se correlacionarán y utilizarán sin modificar las configuraciones de cliente.
- El servidor puede enviar a VTAM una lista de direcciones de LU dependientes para cada PU, para que VTAM pueda crear dinámicamente sus propias definiciones de LU.

  La definición dinámica de LU dependientes (DDDLU) es un recurso de VTAM que permite que VTAM conozca las unidades lógicas cuando éstas se conectan a VTAM, en lugar de hacerlo durante la activación de nodo principal de la PU relacionada.

  Si VTAM lo solicita, la función de servidor TN3270E utilizará DDDLU para crear sus LU locales en VTAM. En lugar de enviar todas las peticiones de definición de LU cuando se recibe la ACTPU, el servidor esperará hasta que sea realmente

14. La distinción entre implícito y explícito está únicamente dentro del Network Utility. Un cliente puede solicitar un nombre de LU implícita y el Network Utility satisfará la petición si la LU está disponible. El punto clave es que la función de servidor no asignará nunca una LU explícita a un cliente a no ser que el cliente solicite específicamente dicho nombre de LU.

necesario definir la LU. La definición de LU se producirá cuando un cliente TN3270 se conecte y necesite una LU que no se ha definido en VTAM.

- Puede configurar múltiples puertos TCP locales para la función de servidor TN3270.

  Esta mejora le permite definir múltiples puertos TCP en los que el servidor TN3270E podrá “escuchar”. Este soporte permite a los clientes especificar el recurso SNA que desean utilizando un número de puerto.

- Puede inhabilitar la negociación de TN3270E.

  Esta mejora le permite especificar si el puerto añadido negociará para convertirse en servidor TN3270E, en lugar de conformarse con el soporte TN3270E base. Esto es necesario para algunos clientes TN3270 base, que no manejan correctamente la recepción de negociaciones iniciales de TN3270 Extended.

Consulte la publicación de MAS V3.2 o posterior *MAS Consulta de configuración y supervisión de protocolos Volumen 2* para obtener más información sobre cómo configurar estas funciones.

MAS V3.3 ha introducido Host Initiated DDLU:

- Host Initiated DDLU elimina la necesidad de definir redundantemente las LU en el servidor TN3270E, si las LU ya se han definido en VTAM. El servidor TN3270E definirá dinámicamente cada una de las LU a medida que se activen en VTAM.

Configuraciones de ejemplo

El Network Utility como servidor TN3270E puede usarse en varias configuraciones. Por ejemplo, puede colocarse en la bifurcación remota o en el centro de datos. Puede conectarse al sistema principal a través de una conexión de subárea SNA tradicional o puede utilizar APPN. En el centro de datos, puede colocarse en una configuración conectada a canal o puede ser un servidor autónomo que reside en la LAN del campus (o nube de ATM) utilizando la conexión a canal proporcionada por un Controlador de comunicaciones IBM 3745/46, un 2216-400, un Controlador de interconexión 3172, un adaptador OSA o una pasarela OEM existente.

Uno de los elementos más importantes de una implementación de TN3270 es la escalabilidad. La solución Network Utility puede ajustarse proporcionalmente a configuraciones muy grandes al mismo tiempo que proporciona alta disponibilidad y redundancia.

Los escenarios siguientes le muestran cómo utilizar de forma efectiva el Network Utility como servidor TN3270E.

TN3270 a través de una conexión de subárea a un NCP

Este escenario (mostrado en la Figura 6 en la página 139) muestra una red de subárea SNA tradicional con todo el acceso al sistema principal que se produce a través de un Controlador de comunicaciones IBM 3745/46 con el NCP (Network Control Program) de IBM. El Network Utility se instala para proporcionar soporte de servidor TN3270 para estaciones de trabajo en sentido directo en el campus local o en las ubicaciones remotas. El Network Utility se conecta al sistema principal mediante el FEP a través de una conexión de subárea normal.

Se pueden manejar hasta 20.000 sesiones TN3270 con un solo Network Utility instalado, como se muestra en la Figura 6 en la página 139. A medida que crece la

red, la solución puede ajustarse proporcionalmente simplemente añadiendo más capacidad de servidor TN3270E a través de Network Utilities adicionales. También puede definir el equilibrio de carga automático entre los servidores TN3270E instalando un direccionador de IBM o Network Utility independiente para que sirva de asignador de tareas de red (Network Dispatcher). (Consulte el apartado “TN3270E de alta escalabilidad y tolerancia de errores” en la página 143 para ver un ejemplo de cómo ajustar proporcionalmente la red).

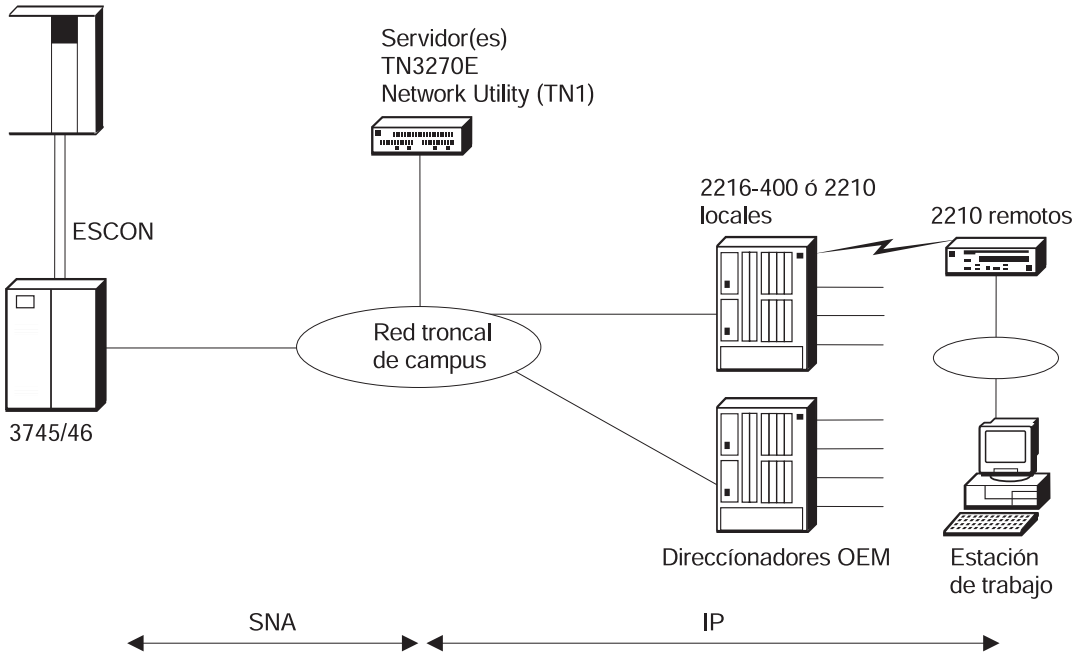


Figura 6. TN3270 a través de una conexión de subárea mediante un 37xx

Claves para la configuración

La configuración de la función de servidor TN3270E es muy directa en este escenario. Sin embargo, vale la pena mencionar los puntos siguientes:

- Existe una implementación de APPN y una de subárea del servidor TN3270E. Ambas necesitan soporte APPN para instalarse en el Network Utility y ambas se configuran dentro del proceso de configuración de APPN. Esto es cierto aunque una configuración de subárea pura no utilice la función APPN. Se trata de una declaración de implementación dado que la función de servidor TN3270E utiliza la pila SNA APPN para las conexiones de subárea y APPN con el sistema principal.

  Tenga en cuenta también estos puntos adicionales relacionados con la configuración de servidor TN3270E y APPN:

  – Se debe habilitar el soporte APPN.
  – Deberá definir un puerto y una o más estaciones de enlace para definir la conexión en VTAM.
  – Para configuraciones de subárea, al definir una estación de enlace y especificar que se solicite una sesión SSCP se define implícitamente una PU en el Network Utility. Esta PU soportará un máximo de 253 LU de sentido directo. Si necesita más de 253 LU, necesitará definir más de una estación de enlace. Cada estación de enlace necesita utilizar un punto de acceso de servicio (SAP) diferente y un ID de nodo local (IDNUM) diferente.
- Al configurar los parámetros para el servidor TN3270E, puede establecer la dirección IP del servidor en la dirección IP interna del sistema o en una de las

direcciones IP de interfaz. Tenga presente que la dirección que seleccione para TN3270 puede no estar disponible para utilizar Telnet IP normal para gestionar el sistema.[15]

- Las LU de sentido directo pueden definirse como explícitas o implícitas.
  - Utilice definiciones explícitas cuando necesite asegurarse de que el dispositivo utilizará siempre el mismo nombre de LU. (Por ejemplo, las impresoras utilizarán normalmente definiciones explícitas).
  - Utilice definiciones implícitas cuando tenga un gran grupo de dispositivos que pueden utilizar una agrupación común de LU disponibles y no necesitan utilizar el mismo nombre de LU cada vez.

Para obtener una visión completa de los parámetros de configuración necesarios para este escenario, consulte la Tabla 19 en la página 158.

TN3270 a través de una conexión de subárea mediante una pasarela de canal

Este escenario, que se muestra en la Figura 7 en la página 141, es similar al escenario anterior excepto en que, aquí, el Network Utility se conecta al sistema principal mediante una pasarela de canal de LAN, por ejemplo un IBM 3172, un IBM 2216, un IBM 3746 con el Multiaccess Enclosure (MAE) o un dispositivo OEM. Estas pasarelas utilizan el paso a través XCA (External Communications Adapter) y no proporcionan la función de límite de SNA proporcionada normalmente por un NCP. Con una pasarela, esta función la proporciona VTAM.

Si tiene una pasarela existente con un servidor TN3270 configurado, puede utilizar el Network Utility para descargar la carga de trabajo TN3270 existente o para proporcionar capacidad TN3270 adicional a medida que aumentan los requisitos de red.

Un 2216 existente o un 3746 le permite tener múltiples conexiones de canal al sistema principal mientras que puede incrementar las instalaciones de Network Utilities para los requisitos de servidor TN3270E. Se pueden utilizar las características de equilibrio de carga dinámica del asignador de tareas de red para optimizar la eficiencia.

15. Si necesita utilizar Telnet en esta misma dirección, puede configurar el servidor TN3270E para que utilice otro puerto (24, por ejemplo) para que telnet pueda utilizar el número de puerto 23. Para ello es necesario que las estaciones de trabajo cliente TN3270 estén configuradas para utilizar este mismo puerto.

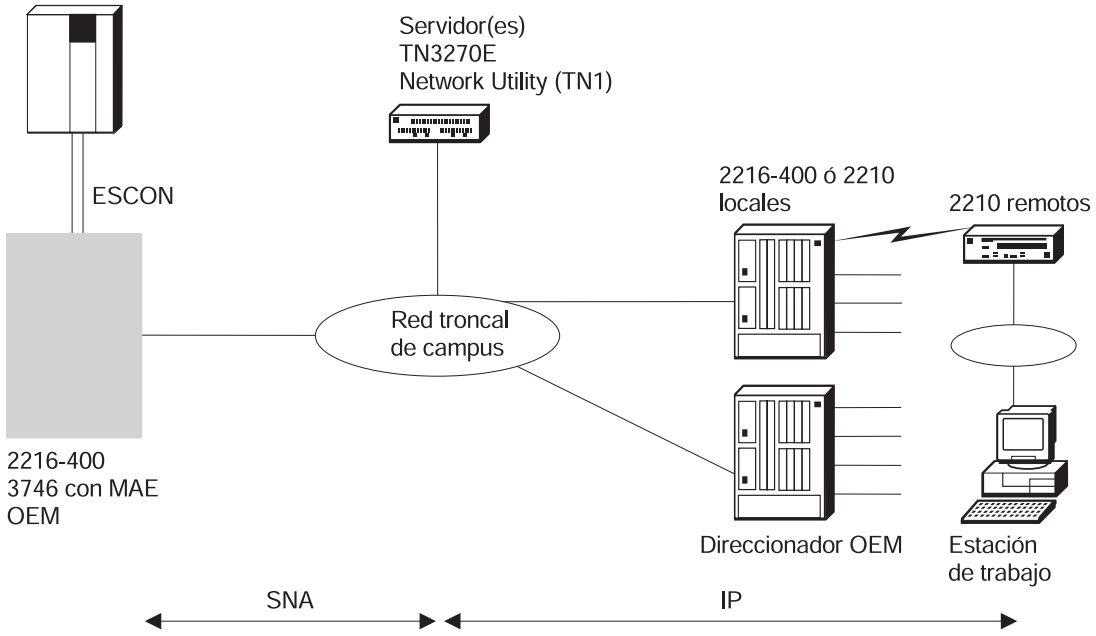


Figura 7. TN3270 a través de una conexión de subárea mediante una pasarela LAN

Claves para la configuración

Desde la perspectiva del Network Utility, la configuración de este escenario es idéntica a la del escenario anterior. Las definiciones de sistema principal también son idénticas. Para ambos escenarios, sólo tiene que definir los nodos principales conmutados para las PU en el servidor TN3270E.

TN3270 mediante un adaptador OSA

Este escenario se muestra en la Figura 8 en la página 142. Aquí, el Network Utility se conecta al sistema principal mediante el OSA (Open Systems Adapter) S/390. Igual que el escenario de pasarela anterior, la función de límite SNA está en el sistema principal.

Mientras que la función de servidor TN3270 puede residir en el propio sistema principal, muchos clientes prefieren descargar esta función externamente a otra plataforma. El Network Utility cumple bien este requisito al proporcionar la función escalable y efectiva de costes de servidor TN3270E sin cambiar el método de conexión al sistema principal. Esto le permite aprovechar las inversiones existentes.

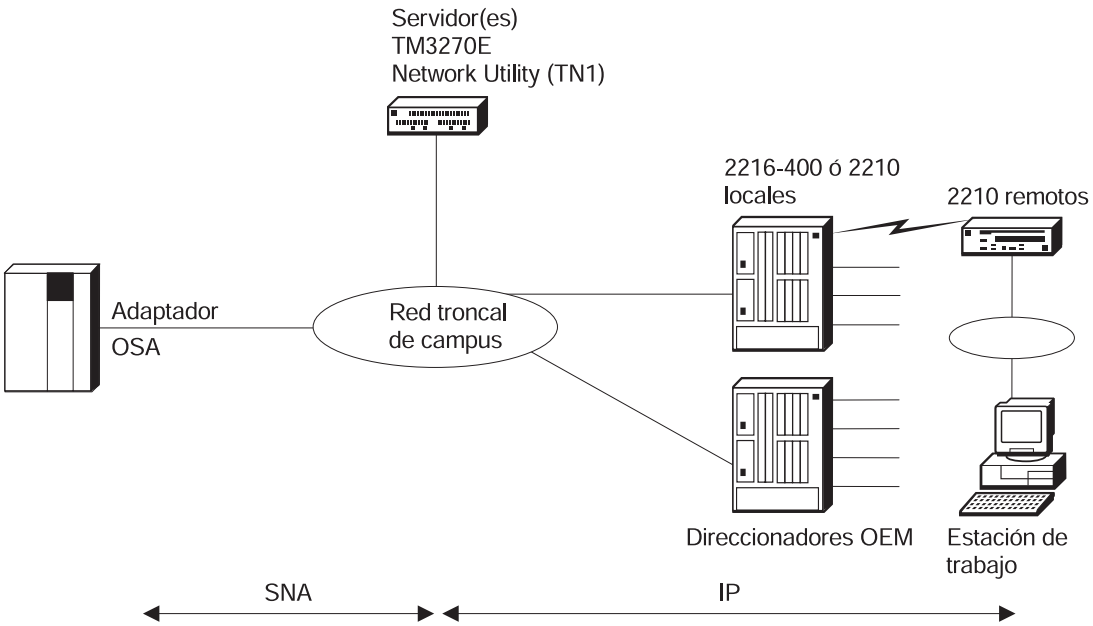


Figura 8. TN3270 a través de un adaptador OSA

Claves para la configuración

Desde la perspectiva del Network Utility, la configuración de este escenario es idéntica a la de los dos escenarios anteriores.

SNA de subárea de TN3270 a través de DLSw

Se utiliza la conexión TN3270E por SNA de subárea a través de DLSw para eliminar un segundo requisito de direccionador en las bifurcaciones o los nodos remotos. Sin esta función, necesitaría dos direccionadores en una bifurcación para poder ejecutar el Servidor TN3270E por IP, como se muestra en la Figura 9. Con el soporte de Servidor TN3270E en la Subárea DLSw, no se necesitan dos sistemas Network Utility puesto que los soportes de DLSw y TN3270E se fusionan en un solo Network Utility.

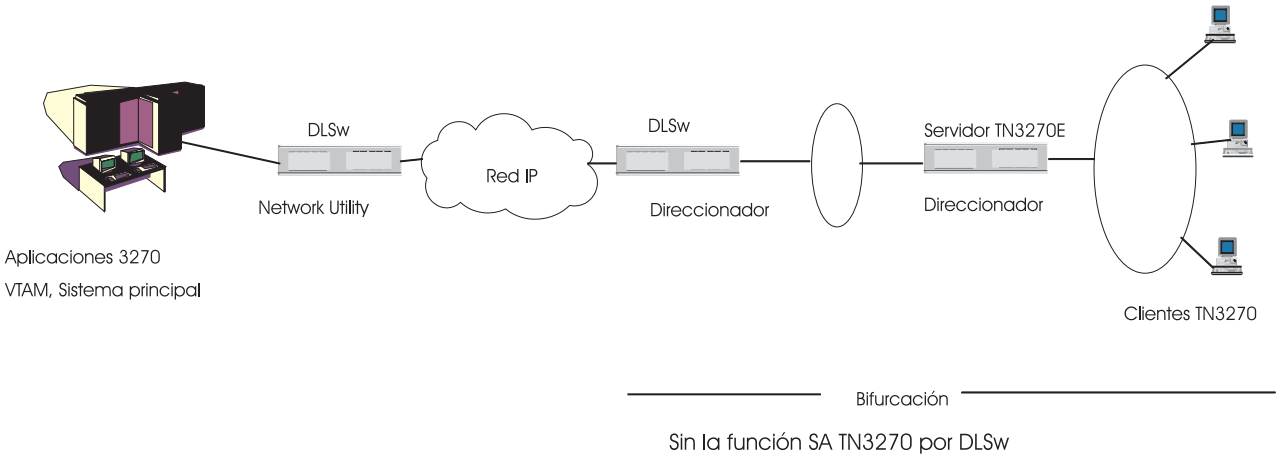


*Figura 9. Configuración de bifurcación típica **sin** soporte de subárea TN3270E a través de DLSw en Network Utility*

Tal como se muestra en la Figura 10, el Servidor TN3270E y DLSw se soportan en un solo Network Utility con la función de Subárea de múltiples PU. En esta función, hay una interfaz APPN/DLSw dentro de Network Utility. Es posible ejecutar 58 estaciones de enlace a través de esta interfaz — en otras palabras, puede ejecutar 58 PU SNA Tipo 2. La nueva función de subárea de múltiples PU puede ejecutarse a través DLSw local o remoto. La DLSw local soporta la conexión LSA ESCON, QLLC X.25 y los enlaces SDLC.

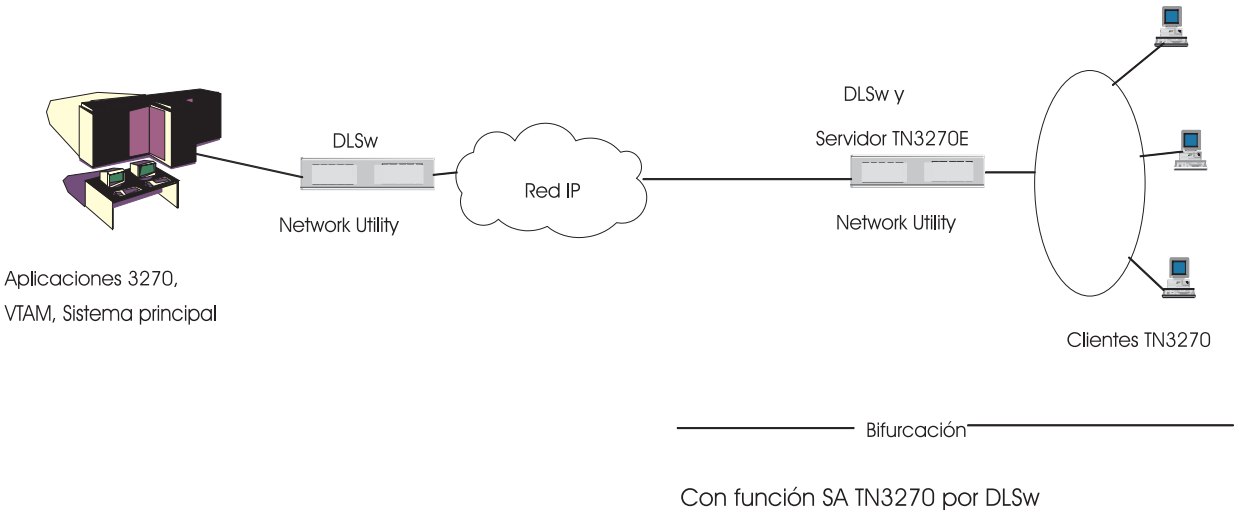


*Figura 10. Configuración de bifurcación típica **con** soporte de subárea TN3270E a través DLSw en Network Utility*

TN3270E de alta escalabilidad y tolerancia de errores

Este escenario, que se muestra en la Figura 11 en la página 144, es una ampliación del escenario descrito en el apartado “TN3270 a través de una conexión de subárea a un NCP” en la página 138. Aquí, la solución se ajusta proporcionalmente con múltiples dispositivos Network Utility para proporcionar soporte de servidor TN3270E para grandes entornos 3270. Asimismo, se configura un Network Utility independiente como asignador de tareas de red y se utiliza para proporcionar equilibrio de carga [16].El nuevo Asesor de Asignador de tareas de red para TN3270 permite al Asignador de tareas de red reunir estadísticas de carga de cada servidor TN3270E de Network Utility en tiempo real para lograr la mejor distribución posible entre los servidores TN3270.

La solución proporciona alta disponibilidad en el caso de una anomalía en uno de los servidores TN3270E. El servidor al que se despacha la sesión cliente es transparente para el usuario. Si se produce una anomalía, las sesiones a través de dicho servidor se pierden pero los usuarios simplemente vuelven a conectarse al sistema principal a través de otro Network Utility utilizando la misma dirección IP de destino para el servidor TN3270E.

La función Asignador de tareas de red también puede utilizar hardware redundante, con un segundo Network Utility configurado como Asignador de tareas de red y sirviendo de reserva al primario.

16. A partir de MAS V3.2, la función Asignador de tareas de red también puede despachar sesiones de cliente a la función de servidor TN3270 que se ejecuta en el mismo Network Utility.

Con esta configuración, puede ajustar proporcionalmente el soporte TN3270E a cualquier tamaño simplemente añadiendo capacidad adicional de servidor TN3270E. Esto puede llevarse a cabo sin disrupciones realizando incrementos de capacidad a medida que aumentan los requisitos de red.

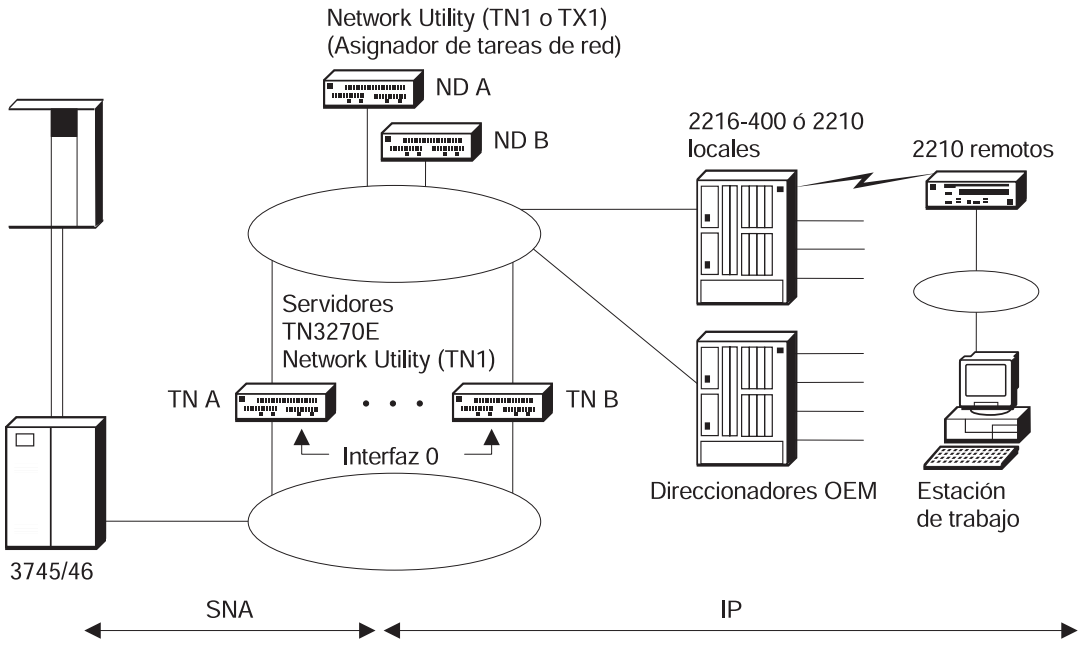


Figura 11. TN3270E de alta escalabilidad y tolerancia de errores

Claves para la configuración

En lo que se refiere al servidor TN3270E, la configuración es la misma tanto si tiene como si no un Asignador de tareas de red, De hecho, el servidor TN3270E no está al corriente del tráfico de los clientes a los que se está despachando mediante otra máquina. Consulte el apartado “TN3270 a través de una conexión de subárea a un NCP” en la página 138 para conocer los puntos básicos de configuración para un servidor TN3270E. Consulte la Tabla 20 en la página 162 para ver el conjunto completo de parámetros de configuración para los servidores TN3270E para este escenario.

Sin embargo, el direccionamiento IP necesita prestar especial atención a la alta disponibilidad en esta configuración. En el apartado “TN3270 a través de una conexión de subárea a un NCP” en la página 138, el servidor TN3270E se ha configurado con la misma dirección que el ID de direccionador (también la misma dirección que la interfaz de LAN). En un entorno de Asignador de tareas de red, el direccionamiento IP es algo diferente.

Un Asignador de tareas de red y uno o más servidores TN3270E forman lo que se denomina cluster. Se define una dirección IP para el cluster y las estaciones de trabajo envían sus paquetes TN3270 a esta dirección IP. El Asignador de tareas de red recibe estos paquetes y los reenvía a un servidor del cluster para su proceso.

Puesto que el Asignador de tareas de red no modifica la dirección IP de destino de estos paquetes, es necesario configurar también cada servidor TN3270E con esta misma dirección IP. Sin embargo, deberá asegurarse de que los servidores TN3270E no difunden esta dirección a través de OSPF o RIP a la red porque no

desea que estos servidores respondan a la dirección de cluster. Sólo el Asignador de tareas de red debe responder a la dirección de cluster[17].

El direccionador debe conocer la dirección IP del servidor TN3270E para reenviar paquetes a la función de servidor. Un modo para que el direccionador conozca esta dirección consiste en especificarla en una interfaz como una dirección secundaria. La Figura 12 muestra un ejemplo de este esquema de direccionamiento IP para la configuración altamente disponible y con tolerancia de errores TN3270 representada en la Figura 11 en la página 144.

```
Servidor TN3270E núm. 1 (TNA):
    Dirección interna      172.128.252.3
    Interfaz 0             172.128.2.3 (Segunda direcc.: 172.128.1.100)
    Interfaz 1             172.128.1.3
    ID direccionador OSPF  172.128.1.3
    Servidor TN3270E       172.128.1.100 (igual que direcc. de cluster)

Servidor TN3270E núm. 2 (TNB):
    Dirección interna      172.128.252.4
    Interfaz 0             172.128.2.4 (Segunda direcc.: 172.128.1.100)
    Interfaz 1             172.128.1.4
    ID direccionador OSPF  172.128.1.4
    Servidor TN3270E       172.128.1.100 (igual que direcc. de cluster)

Asignador de tareas de red núm. 1 (NDA):
    Dirección interna      172.128.252.1
    Direc. interfaz 0      172.128.1.1
    ID direccionador OSPF  172.128.1.1
    Dirección de cluster   172.128.1.100
       Puerto 23
         Servidor 1        172.128.1.3
         Servidor 2        172.128.1.4

Asignador de tareas de red núm. 2 (NDB):
    Dirección interna      172.128.252.2
    Direc. interfaz 0      172.128.1.2
    ID direccionador OSPF  172.128.1.2
    Dirección de cluster   172.128.1.100
       Puerto 23
         Servidor 1        172.128.1.3
         Servidor 2        172.128.1.4
```

Figura 12. Direccionamiento IP para el escenario altamente escalable y con tolerancia de errores de TN3270

Observe que la dirección de cluster está asignada como segunda dirección IP en la interfaz 0 de las máquinas Network Utility. En este escenario, el segmento de LAN al que se conecta la interfaz 0 no transporta tráfico IP – sólo el tráfico de subárea SNA del servidor TN3270E al sistema principal.

La configuración de los Asignadores de tareas de red es estándar. Para ver el conjunto completo de parámetros de configuración necesarios para este escenario, consulte la Tabla 21 en la página 166 para el asignador de tareas de red primario. Para conocer las diferencias de esta configuración para el asignador de tareas de red de reserva, consulte la Tabla 22 en la página 168.

17. No se puede hacer ping para la dirección de cluster. El Asignador de tareas de red no responde a los ping efectuados para la dirección de cluster. Sólo procesa paquetes UDP y TCP.

TN3270 a través de DLUR por APPN

Este escenario, que se muestra en la Figura 13, utiliza APPN para comunicarse con el sistema principal. El Network Utility utiliza el HPR (High Performance Routing) de APPN y establece una sesión RTP (Rapid Transport Protocol) con el sistema principal. El HPR se utiliza todo el tiempo desde el servidor TN3270E hasta VTAM. En caso de producirse una anomalía, esto asegura la conmutación de sesión sin disrupciones a una vía de acceso alternativa si se tienen pasarelas paralelas. Esto es especialmente importante en entornos de Parallel Sysplex.

Además, el HPR se soporta por IP a través de la característica Enterprise Extender del Network Utility. Esto es importante si desea colocar el servidor TN3270E en una ubicación remota y utilizar IP para transportar el tráfico APPN de vuelta al centro de datos.

La pasarela de canal es un nodo de red APPN que efectúa el Direccionamiento de red automático (ANR) de APPN para la sesión RTP entre el Network Utility y el sistema principal.

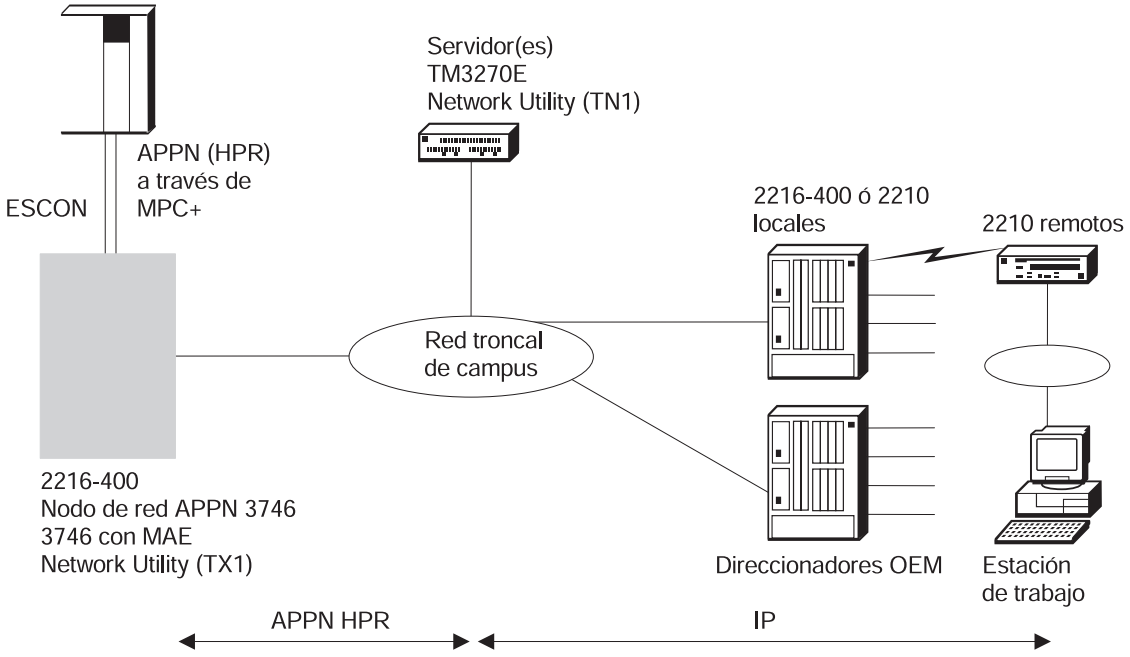


Figura 13. TN3270 a través de DLUR por APPN

Cuando se conecta un servidor TN3270E al sistema principal a través de APPN, se deberá configurar soporte DLUR en el Network Utility. La característica DLUR extiende hasta los nodos APPN el soporte de dispositivos T2.0 o T2.1 que contienen LU dependientes. La función DLUR en un nodo de red APPN funciona conjuntamente con DLUS. La función DLUS la proporciona normalmente VTAM, aunque puede residir en cualquier parte de una red mixta APPN/subárea.

Los flujos de LU dependiente (SSCP-PU y SSCP-LU) se encapsulan en un conducto LU 6.2 (CP-SVR) establecido entre el nodo DLUR APPN y el SSCP DLUS. El conducto CP-SVR está compuesto por un par de sesiones LU 6.2 que utilizan una modalidad CPSVRMGR nueva entre el DLUR y el DLUS. Este conducto lleva la función SSCP (en el DLUS) al nodo APPN DLUR donde puede quedar disponible para conectar nodos T2.0/T2.1 que contengan LU dependientes.

Claves para la configuración

Desde la perspectiva de una estación de trabajo de sentido directo, el servidor TN3270E parece el mismo tanto si dicho servidor está utilizando subárea SNA como si está utilizando APPN para comunicarse con el sistema principal en el enlace superior. En el Network Utility, los parámetros base de servidor TN3270 se configuran del mismo modo que en los escenarios de subárea SNA, pero las PU locales se configuran de modo diferente. En lugar de asociar cada PU con un enlace de subárea, configure las PU locales sin ninguna asociación de enlaces. La función DLUR es responsable de direccionar el tráfico en el conducto DLUS-DLUR hacia y desde estas PU locales.

APPN necesita soporte DLUR para configurarse en el Network Utility. DLUR es bastante simple de configurar dado que el único parámetro necesario es el nombre CP del DLUS, que es VTAM.

Deberá realizar algunas definiciones de sistema principal adicionales para el soporte DLUR y APPN. Consulte el “Capítulo 18. Definiciones de sistema principal de ejemplo” en la página 259 para ver un ejemplo de estos mandatos.

Para obtener una visión completa de los parámetros de configuración necesarios para este escenario, consulte la Tabla 23 en la página 170.

Servidor TN3270E distribuido

Las configuraciones anteriores mostraban cómo se puede utilizar el Network Utility en el centro de datos para centralizar la función de servidor TN3270E en la red. Esta configuración, que se muestra en la Figura 14 en la página 148, sólo muestra un ejemplo de cómo se puede colocar también el Network Utility en una ubicación remota para proporcionar posibilidad de servidor TN3270E distribuido.

En esta configuración, el Network Utility proporciona servicio de servidor TN3270E a estaciones de trabajo de la ubicación remota. Como sucede siempre con una configuración TN3270, las estaciones de trabajo utilizan IP para comunicarse con el servidor TN3270E. El servidor TN3270E utiliza DLUR a través de una conexión APPN al volver al sistema principal en el centro de datos.

En este ejemplo, la WAN corporativa es una red Frame Relay pública que sólo transporta tráfico IP. Por consiguiente, el Network Utility está configurado para utilizar la característica Enterprise Extender que permite que el tráfico HPR APPN se transporte a través de la WAN sólo IP.

El tráfico de Enterprise Extender termina en la pasarela de sistema principal, que desencapsula el tráfico HPR y luego pasa el tráfico APPN a través del nodo de red a la vía de acceso MPC+ hacia el sistema principal. Esta función de reenvío de paquetes de actividad general baja es muy rápida de modo que una sola pasarela puede manejar una gran cantidad de tráfico.

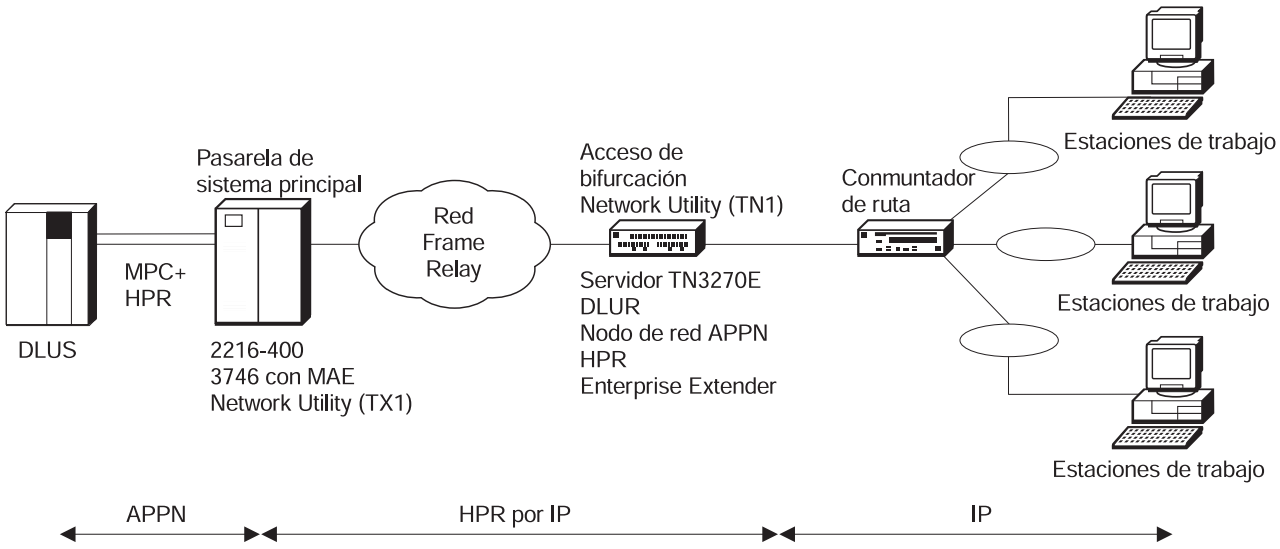


Figura 14. Servidor TN3270E distribuido

Claves para la configuración

Desde la perspectiva de una estación de trabajo de sentido directo, el servidor TN3270E parece el mismo tanto si está en la bifurcación remota como si está en el centro de datos independientemente de que la conexión en sentido inverso con el sistema principal esté utilizando la subárea SNA o APPN. Por consiguiente, la función de servidor TN3270E del Network Utility se configura exactamente igual que en los escenarios anteriores.

APPN y DLUR se configuran igual que en el apartado “TN3270 a través de DLUR por APPN” en la página 146 con una excepción, que es la definición de puerto para APPN a través del enlace IP frame relay. Cuando se configura APPN para utilizar HPR a través de IP (la característica Enterprise Extender), se especifica un tipo de puerto de IP. Entonces, al añadir la estación de enlace para este puerto, en lugar de especificar la dirección MAC del FEP adyacente como se hacía en en apartado “TN3270 a través de DLUR por APPN” en la página 146, se especifica la dirección IP del otro extremo de la red HPR a través de IP, que es la pasarela de sistema principal en este ejemplo[18]. La red IP es responsable de la entrega del tráfico a la pasarela de sistema principal a través de la mejor vía de acceso disponible. Se le asegura un transporte fiable porque la conexión entre el servidor TN3270E y el sistema principal utiliza una sesión RTP.

Gestión del servidor TN3270E

Esta sección presenta algunos de los modos en que puede supervisar y gestionar la función de servidor TN3270E.

Nota: Las funciones de supervisión descritas en esta sección suponen que está ejecutando el código de operación MAS V3.2 o posterior. MAS V3.2 ha introducido varios mandatos de supervisión de TN3270 nuevos así como un submenú TN3270E.

18. La pasarela de sistema principal también debe configurarse con un puerto HPR a través de IP del mismo modo que se describe aquí.

Supervisión de la línea de mandatos

Para ver el estado del servidor TN3270 que se está ejecutando actualmente desde la línea de mandatos, vaya primero a talk 5 y entre **p appn**. Si obtiene el mensaje `Protocol APPN is available but not configured` (El protocolo APPN está disponible pero no está configurado), necesitará completar la configuración APPN base y rearrancar el Network Utility para activar APPN. Tal como se ha indicado en el apartado “Configuración de subárea TN3270 bajo el protocolo APPN” en la página 136, necesita que APPN esté activo incluso aunque sólo esté utilizando la conectividad de subárea TN3270.

Una vez que haya obtenido el indicador de supervisión de APPN `APPN >`, escriba **tn** (abreviatura para ″TN3270E″) para obtener el submenú para supervisar el estado del servidor TN3270E.

Entonces están disponibles los mandatos siguientes en el indicador de supervisión `TN3270E >`:

list status

Si el sistema responde *TN3270E is not configured or not active* (TN3270E no está configurado o no está activo), no ha habilitado la función de servidor TN3270 adecuadamente en la configuración de APPN actualmente activa. Si obtiene este error y ha configurado la función, quizá la dirección IP del servidor TN3270 que ha elegido no está activa como una dirección de interfaz o como la dirección IP interna. Consulte los ejemplos de las configuraciones de TN3270 del Capítulo 13 para conocer otras posibles razones y, a continuación, cambie la configuración APPN/TN3270 y actívela como se describe en el apartado “Configuración en el entorno APPN” en la página 136.

Si la función de servidor está activa, este mandato proporciona la información siguiente:

- Información de configuración en uso actualmente

  TN3270E IP Address
  Dirección IP del servidor a la que pueden conectarse los clientes, también la dirección de cluster si está utilizando el Asignador de tareas de red

  NetDisp Advisor Port Number
  Puerto TCP al que se pueden conectar los Asignador de tareas de red para recibir información de carga

  Keepalive type
  Indica si el servidor sondea a los clientes para ver si están aún activos y cómo lo hace. Los valores posibles son:

  None El servidor no sondea los clientes y sólo descubrirá la ausencia de cliente cuando intente enviar datos.

  NOP El servidor sondea a los clientes a nivel de TCP, el software de cliente no necesita tener posibilidad de responder.

  Timing mark
  El servidor sondea a los clientes a nivel de TN3270 y el software de cliente debe responder dentro de un periodo de tiempo determinado.

  Automatic Logoff
  Indica si el servidor desconecta o no a los clientes después de un periodo de inactividad (no fluyen datos en ninguna dirección)

- Estadísticas de resumen

Number of connections
Número actual de conexiones TCP activas desde clientes TN3270

Number of available Logical Unit Application (LUA) LUs
Número de LU que se han activado desde VTAM o que son LU dinámicas y la PU se ha activado desde VTAM.

Number of defined LUs
Número de LU definidas en un servidor TN3270E.

Number of LUA LUs pending termination
Las LU que se han terminado desde el 3270 pero que no se han borrado enteramente de VTAM.

Number of connections in SSCP-LU state
Número de conexiones TCP de cliente activas actualmente que tienen una LU asociada en este estado (se ha recibido ACTLU pero aún no un BIND)

Number of connections in LU-LU state
Número de conexiones TCP de cliente actualmente activas que tienen una LU asociada en este estado (se ha recibido BIND, totalmente activo)

list connections

Puede escribir este mandato con o sin modificadores:

- **list connections**

  Visualiza todas las conexiones de cliente actualmente activas (aquéllas con una conexión TCP activa).

- **list connections** *dirección ip cliente*

  Visualiza todas las conexiones actualmente activas que se han originado desde la dirección IP especificada.

- **list connections** *nombre recurso*

  Visualiza todas las conexiones actualmente activas que están asociadas con el nombre de agrupación o LU especificado.

Para cada uno de los mandatos **list connection**, se visualiza la información siguiente para cada sesión:

Local LU
Nombre de LU, configurado en Network Utility, con el que la función de servidor ha correlacionado esta conexión TCP de cliente

Class Tipo de LU, como se indica a continuación:
- **IW** Estación de trabajo implícita
- **EW** Estación de trabajo explícita
- **IP** Impresora implícita
- **EP** Impresora explícita

Assoc LU
Para una LU de estación de trabajo, nombre de cualquier LU de impresora asociada

Client Addr
Dirección IP del cliente

Status
Indica si la conexión está en estado SSCP-LU o en estado LU-LU

Prim LU
Nombre de LU primaria como se conoce en VTAM

Sec LU
Nombre de LU secundaria como se conoce en VTAM

Idle Min
Número de minutos desde que esta conexión ha transportado datos de usuario

list port
Muestra los puertos TN3270 adicionales y los parámetros definidos.

list mapping
Lista todas las entradas de correlación de nombres LU.

list pools
Lista todas las agrupaciones implícitas de TN3270E.

Además de los mandatos de la lista anterior, un usuario de servidor TN3270 necesita poder consultar el estado de otros recursos APPN o SNA de los que depende la función. Los mandatos de supervisión APPN siguientes son de uso general:

aping - para probar la conectividad a una LU remota
li port - para mostrar el estado de interfaz
li link - para mostrar el estado de los enlaces lógicos

Si está utilizando DLUR para la conexión de sistema principal, los mandatos siguientes son especialmente útiles:

li appc - para comprobar el estado del conducto DLUS-DLUR
li local - para mostrar el estado de las PU internas utilizadas por la función de servidor TN3270
li dlur - para mostrar el estado de las PU DLUR

Para revisar la configuración APPN, vaya a talk 6 y escriba **list all**.

Soporte de anotación cronológica de sucesos

En general, los mensajes ELS APPN/TN3270 están destinados a capturar información de depuración y rastreo para el personal de soporte de IBM. Estas funciones tienen un amplio soporte de anotación cronológica y rastreo, pero los mensajes ELS propiamente dichos están empaquetados de forma compacta con información de bajo nivel.

Normalmente, activará el rastreo y la anotación cronológica de APPN/TN3270 bajo la dirección del personal de soporte de IBM. El procedimiento general consiste en habilitar algunos rastreos entre una larga lista de posibles rastreos como parte de la configuración APPN. Desde el Programa de configuración, consulte la carpeta APPN Node Services. Desde talk 6, utilice el mandato **set trace**. Después de activar este cambio de configuración, la salida de estos rastreos fluye en una tabla de rastreo en la memoria APPN y también en ELS si tiene activos los mensajes ELS APPN. Si tiene un problema que requiere la activación de rastreos, el soporte de IBM proporcionará procedimientos detallados para guiarle en la captura de información de depuración.

Soporte de gestión SNA

APPN genera alertas SNA para diversas condiciones de error y puede reenviar alertas desde otros dispositivos SNA. Este soporte se describe en el apartado “Soporte de alertas SNA” en la página 97. No hay alertas específicas de la función de servidor TN3270 pero las alertas que genera un Network Utility propiamente dicho pueden estar relacionadas con recursos SNA involucrados con TN3270.

Desde una consola de operador VTAM o NetView/390, puede controlar los enlaces, las PU y las LU involucrados con TN3270 como se describe en el apartado “NetView/390” en la página 102.

Soporte de trampas y MIB SNMP

El Network Utility soporta una versión Internet Draft de las próximas MIB estándares para la función de servidor TN3270:

MIB TN3270 base
MIB TN3270 de tiempo de respuesta

El soporte de Network Utility para estas MIB incluye la posibilidad de:

- Ver la configuración, el estado y las estadísticas del servidor
- Definir grupos de clientes para recogida de tiempos de respuesta
- Ver la correlación de los nombres LU de nombre VTAM con nombre local y con dirección IP de cliente
- Ver la correlación de direcciones IP de cliente con los nombres LU de VTAM
- Reunir datos de tiempo de respuesta para grupos de clientes actuales

Además, el Network Utility soporta las MIB IETF siguientes que están relacionadas con las funciones APPN y SNA:

RFC 2155, APPN
RFC 2051, APPC
RFC 2232, DLUR
RFC 2238, HPR
RFC 1666, SNA NAU
Internet Draft, Extended Border Node

El Network Utility soporta las siguientes MIB específicas de empresa de IBM que están relacionadas con las funciones APPN:

APPN Memory
APPN Accounting
APPN HPR NCL
APPN HPR Route Test
APPN Peripheral Access Node (Branch Extender)

Estas MIB proporcionan una amplia visión de los recursos APPN y SNA dentro del Network Utility, incluidos los que se están utilizando para TN3270.

Soporte de aplicación de gestión de red

Los productos Nways Manager descritos en el apartado “Productos IBM Nways Manager” en la página 98 proporcionan soporte estadístico especializado para la supervisión de tiempos de respuesta de TN3270 así como la posibilidad de ver recursos de servidor TN3270. Para iniciar la supervisión de tiempos de respuesta, seleccione un grupo de uno o más clientes utilizando una máscara y dirección IP. Para cada grupo definido, el gestor reúne estadísticas de tiempos de respuesta en cubetas de tiempo predefinidas (menos de 1 segundo, 1 a 2 segundos, etc.) Utilizando la información reunida, puede ver el tiempo de respuesta histórico agregado por grupo o crear informes personalizados que presentan los datos en diferentes formatos gráficos.

Para ver recursos TN3270 y su estado, se utilizan paneles específicos que combinan información de tablas diferentes dentro del TN3270 base. Para ver recursos APPN y SNA en general, se utilizan paneles específicos que acceden a la

información de las MIB APPN. También puede utilizar soporte de navegador integrado para ver la información en cualquiera de estas MIB.

Nways Manager para AIX proporciona una vista a nivel de APPN de la topología de la red. Puede descubrir recursos APPN participantes, verlos y ver su estado como iconos codificados en color. También se proporcionan sucesos de errores y de rendimiento de protocolo APPN (datos y gráficos). Esta aplicación no representa topologías Branch Extender o Extended Border Node.

Mejoras del servidor TN3270

Definición dinámica de LU dependientes

Puede utilizar la DDDLU (Dynamic Definition of Dependent LU) (Definición dinámica de LU dependientes) para evitar duplicar la definición de las LU en VTAM y el TN3270E. DDDLU permite definir las LU en un lugar solamente — el Network Utility. En VTAM, sólo necesita definir una o más PU en función del número de LU que necesite. La implementación de DDDLU también elimina los esfuerzos de definiciones y mantenimiento en VTAM para futuras necesidades de definición de LU.

Cuando un cliente TN3270E solicita una conexión utilizando una de las LU definidas en el direccionador, éste envía un mandato Reply/PSID NMVT a VTAM. En este mandato, la dirección local de la LU y la información de tipo de dispositivo (3270) se envía a VTAM utilizando la sesión SSCP-PU. Entonces VTAM ve en la definición de PU que no existe ninguna definición para la LU en cuestión. En este momento, VTAM crea una definición de LU utilizando la sentencia de modelo LUGROUP para los valores de parámetro y el valor LUSEED para la generación dinámica de nombre para la LU.

Las LU que necesitan nombres de LU específicos y las impresoras 3270 de puertos específicos también pueden definirse bajo el mismo nodo principal conmutado. Consulte el ejemplo a continuación.

Tabla 17. Ejemplo de DDDPU

```
DDDPU          VBUILD TYPE=SWNET
DDPU           PU  ADDR=02,      x
               IDBLK=077,          x
               IDNUM=22160,        x
                 PUTYPE=2,           x
                USSTAB=US327X,       x
                LUGROUP=GROUP1,      x
               LUSEED=DDLU###,         x
               DLOGMOD=D4C32XX3        x
SALE01       LU  LOCADDR=98,           x     1
                 DLOGMOD=D4C32XX3,       x
               LOGAPPL=CICSA
SALEPRT      LU   LOCADDR=99,           x      2
               LOGMODE=SAL3287,
               LOGAPPL=CICSA
```

1. En esta definición de ejemplo, se ha solicitado que la LU 'SALE01' estuviera en LOCADDR=98 debido a requisitos específicos. Por consiguiente, esta LU específica se define bajo esta 'DDDPU' para satisfacer los requisitos.
2. En esta definición, la impresora también debe estar en un puerto específico. Esto sucede especialmente en el caso de algunas aplicaciones SNA (p.ej.

aplicación CICS). La aplicación para el departamento de ventas necesita una impresora en el puerto 99, con LOGMODE=SAL3287, y necesita conectarse a la aplicación CICSA cuando se activa.

No es necesario que el nombre especificado para la LU en el Servidor TN3270E (LU local) coincida con el nombre generado por VTAM para la misma LU. Si el cliente desea tener una LU específica, deberá utilizar el nombre de LU especificado en TN3270E, en lugar de sólo seleccionar cualquier LU en una agrupación. Sin embargo, la aplicación de sistema principal funciona con el nombre de LU que genera VTAM dinámicamente. Estos dos nombres están unidos entre sí a través de la dirección local de la LU.

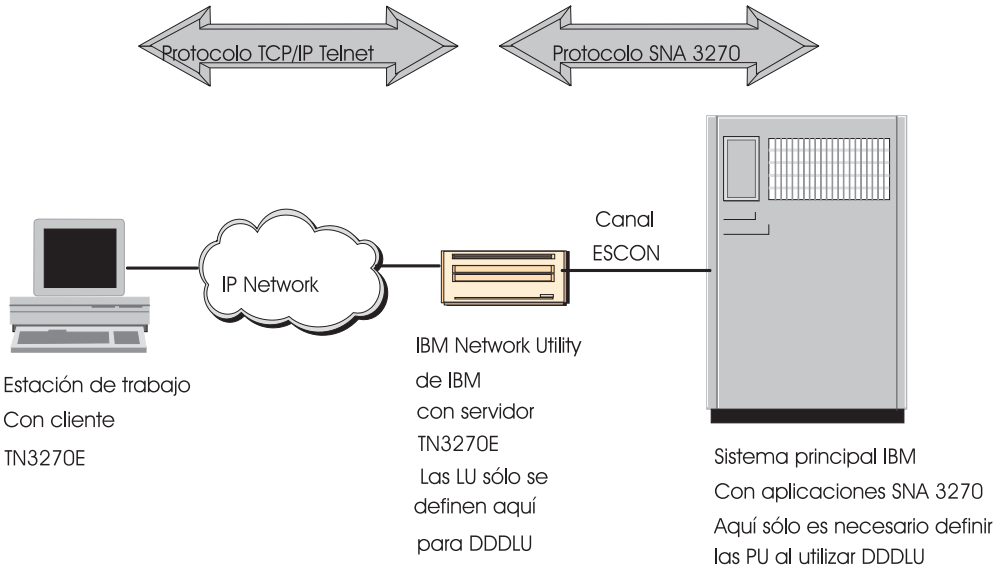


Figura 15. Servidor TN3270E en ejecución en Network Utility conectado a ESCON, utilizando DDDLU

La definición dinámica de las LU se realiza en la rutina de salida de VTAM SDDLU (Selection of Definitions for Dependent LUs) (Selección de definiciones para LU dependientes). Si utiliza el programa de salida SDDLU proporcionado por IBM, necesitará especificar el parámetro LUSEED para la creación de nombres en la definición de PU, además del nodo principal modelo LUGROUP. Si utiliza un programa de salida propio, deberá seguir la práctica del mismo.

Este concepto se describe detalladamente en la publicación SC31-8370, *VTAM Network Implementation Guide*, bajo la sección titulada “Defining Dependent LUs Dynamically”.

La LU puede ser explícita (como se define localmente en TN3270E), en cuyo caso el cliente debe especificar un nombre de LU exacto en la estación de trabajo. La LU solicitada por el usuario (cliente TN3270) también puede ser implícita, en cuyo caso pertenece a una agrupación de LU.

La correlación de dirección IP con nombre de LU también se soporta para las DDDLU. Además, puede tener otras LU explícitas, definidas de formas diferentes, bajo una PU diferente que se utilizará para la correlación de dirección IP con LU.

Definiciones de LU dinámicas iniciadas por el sistema principal TN3270

Además de DDDLU, otra forma de evitar definiciones de LU duplicadas es utilizando HIDLU (Host Initiated Dynamic LU) (LU dinámica iniciada por sistema principal). HIDLU permite definir las LU solamente en VTAM. En Network Utility (o 2216) sólo se define una PU o tantas PU como sean necesarias, pero no se definen LU para estas PU.

Cuando un cliente solicita utilizar una LU de este tipo, TN3270E envía a VTAM una petición para activar la PU y sus LU. Cuando se activen las LU definidas por VTAM, los nombres de LU se transferirán a Network Utility en los mandatos de ACTLU en el Vector de control 0E.

Las LU definidas de este modo tienen el mismo nombre en VTAM y en Network Utility.

Para utilizar HIDLU, tiene que usar el parámetro **INCLUD0E=YES** en la definición de PU en VTAM. Esta función necesita VTAM V4R4 con el APAR OW25501 y OW31805. Con HIDLU, sólo puede definir terminales de pantalla. No se soportan impresoras. Las definiciones de HIDLU pueden utilizarse al mismo tiempo con otras LU definidas localmente (en el Network Utility), que pueden ser implícitas, explícitas o LU definidas por DDDLU.

Almacenamiento en antememoria de cliente Host On-Demand de TN3270

Host On-Demand (HOD) permite a los clientes de navegador Web conectarse a aplicaciones de sistema principal SNA 3270 y 5250. La emulación de terminal (TN3270 o TN5250) se ejecuta como una applet Java en el navegador del cliente. La conexión a una aplicación de sistema principal se realiza a través de un servidor TN3270 (o TN5250).

Las applets Java se recuperan normalmente de un servidor HOD, que se ejecuta como un servidor Web.

El Almacenamiento en antememoria de cliente Host On-Demand permite a un IBM 2216, 2212 o Network Utility, que actúa como servidor TN3270, almacenar en antememoria las applets HOD y servirlas a los navegadores de cliente a petición.

El almacenamiento en antememoria de cliente HOD puede descargar el HOD Server y, si se coloca estratégicamente, puede cargar applets y páginas HOD más deprisa en las estaciones de trabajo clientes. Otra ventaja de utilizar la función de Almacenamiento en antememoria de cliente HOD es distribuir la carga en líneas/anchuras de banda específicas dentro de la red para eliminar la congestión. La función utiliza y se define bajo la característica Asignador de tareas de red, utilizando talk 6 o el programa de configuración. En primer lugar, se define una dirección de cluster en el Asignador de tareas de red y, a continuación, se definen el (los) número(s) de puerto y las direcciones de HOD Server bajo dicha dirección de cluster.

El principio de operación básico del Almacenamiento en antememoria de cliente HOD es el siguiente: los clientes utilizan la dirección de cluster ND en sus navegadores, en lugar de utilizar la dirección real del HOD Server. Cuando llega a la dirección de cluster la petición de HOD Server, el puerto 80 (número de puerto

HTTP), se transferirán desde la antememoria HOD las applets Java necesarias para establecer la sesión. Si las applets u otras páginas necesarias no están en la antememoria de Network Utility, el direccionador se conectará al HOD Server, bajará los elementos, los almacenará en la antememoria y los proporcionará al cliente. Ahora que las páginas y las applets están en la antememoria, el siguiente usuario las obtendrá directamente de la antememoria. Por consiguiente, esta función de Almacenamiento en antememoria de cliente HOD en Network Utility ayuda a utilizar mejor la red mediante la distribución de las applets Java en los Network Utilities de forma que los clientes no tengan que cargar estas applets del HOD Server. Cuando se utiliza esta función, tampoco se crea carga adicional en el HOD Server, dado que las peticiones de applets Java las entrega Network Utility.

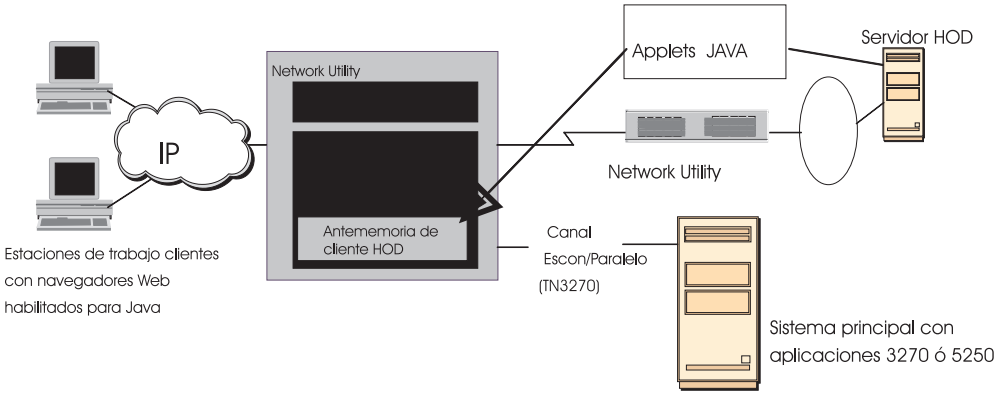


Figura 16. Escenario con servidor TN3270E y antememoria HOD

La función de Almacenamiento en antememoria de cliente HOD sólo está disponible junto con la función Servidor TN3270E.

Capítulo 13. Detalles de configuraciones de ejemplo de Servidor TN3270E

Este capítulo contiene diagramas y tablas de parámetros de configuración para varios de los ejemplos de las configuraciones de red de servidor TN3270E del "Capítulo 12. Servidor TN3270E" en la página 133. Los valores de parámetros mostrados proceden de configuraciones de prueba de trabajo reales.

Para obtener una explicación de las columnas y los convenios de las tablas de parámetros de configuración, consulte el apartado "Convenios de las tablas de configuración de ejemplo" en la página 131.

Las páginas World Wide Web de Network Utility contienen archivos de configuración binarios que coinciden con estas tablas de parámetros de configuración. Para acceder a estos archivos, siga el enlace `Download` desde:

`http://www.networking.ibm.com/networkutility`

Las configuraciones documentadas en este capítulo son:

Tabla 18. Referencia cruzada de información de configuraciones de ejemplo

Descripción de la configuración	Tabla de parámetros
"TN3270 a través de una conexión de subárea a un NCP" en la página 138	Tabla 19 en la página 158
"TN3270E de alta escalabilidad y tolerancia de errores" en la página 143, para el servidor TN3270 TN A	Tabla 20 en la página 162
"TN3270E de alta escalabilidad y tolerancia de errores" en la página 143, para el Asignador de tareas de red ND A	Tabla 21 en la página 166
"TN3270 a través de DLUR por APPN" en la página 146	Tabla 23 en la página 170
"Definición dinámica de LU dependientes" en la página 153	"Definición dinámica de LU dependientes" en la página 172
"Definiciones de LU dinámicas iniciadas por el sistema principal TN3270" en la página 155	"Definición de LU dinámica iniciada por el sistema principal" en la página 179
"Almacenamiento en antememoria de cliente Host On-Demand de TN3270" en la página 155	"Antememoria de cliente HOD (Host On-Demand) de TN3270E" en la página 185
"SNA de subárea de TN3270 a través de DLSw" en la página 142	"SNA de subárea de TN3270E a través de DLSw" en la página 192

TN3270 a través de subárea LAN, a través de DLUR utilizando el Asignador de tareas de red

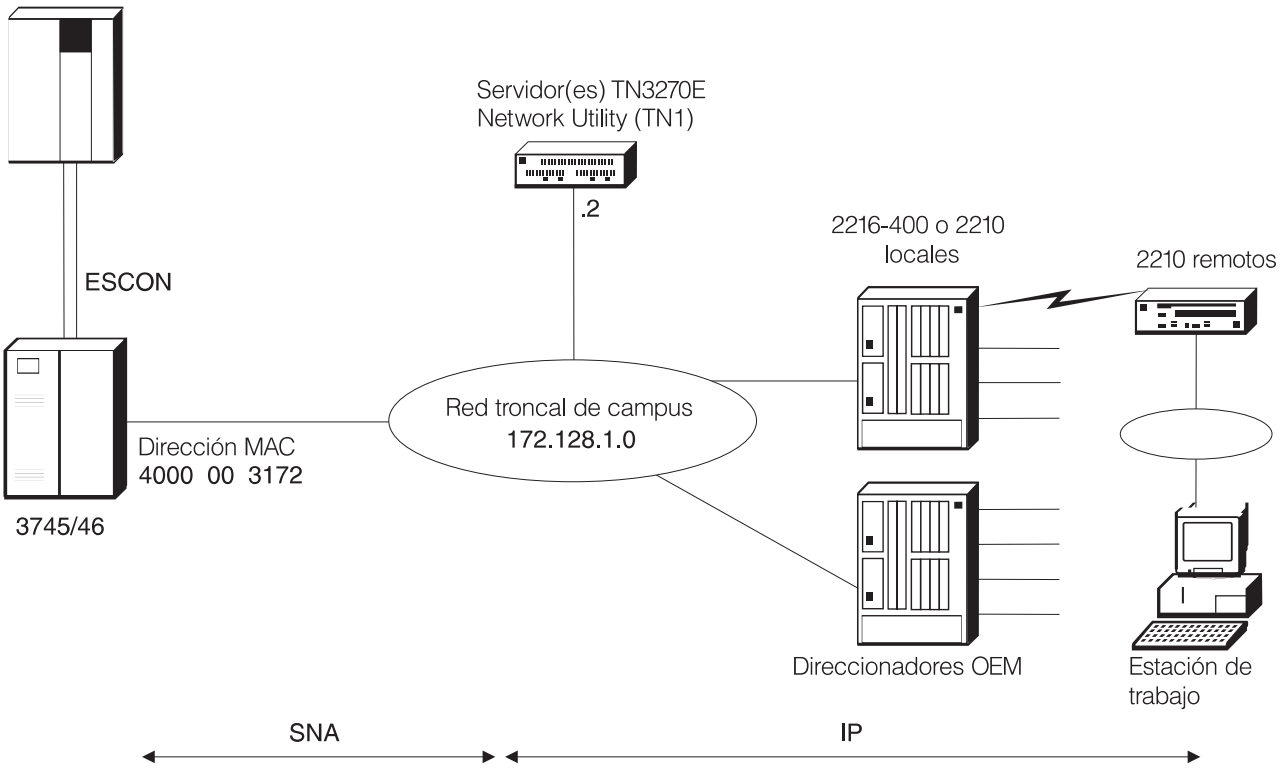


Figura 17. Subárea TN3270E

Tabla 19. Subárea TN3270E. Consulte la página 138 para obtener una descripción y la página 158 para ver un diagrama de esta configuración.

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Dispositivos Adaptadores Ranuras	Ranura1: TR de 2 puertos	Ver ″add dev″ en la fila siguiente	1
Dispositivos Adaptadores Puertos	Ranura 1/Puerto 1: Interfaz 0: TR	`Config>`**`add dev tok`**	2
Dispositivos Interfaces	Interfaz 0 Dirección MAC 400022AA0001	`Config>`**`net 0`** `TKR Config>`**`set phy 40:00:22:AA:00:01`**	
Sistema General	Nombre de sistema: NU_A Ubicación: XYZ Contacto: Administrador	`Config>`**`set host`** `Config>`**`set location`** `Config>`**`set contact`**	
Sistema SNMP Config General	SNMP (seleccionado)	`Config>`**`p snmp`** `SNMP Config>`**`enable snmp`**	
Sistema SNMP Config Comunidades General	Nombre de comunidad: admin Tipo acceso: Trampa lect.-grab. Vista de comunidad: Toda	`SNMP Config>`**`add community`** `SNMP Config>`**`set comm access write`**	3
Protocolos IP General	Dirección interna: 172.128.252.2 ID direccionador: 172.128.1.2	`Config>`**`p ip`** `IP Config>`**`set internal 172.128.252.2`** `IP Config>`**`set router-id 172.128.1.2`**	

Tabla 19. Subárea TN3270E (continuación). Consulte la página 138 para obtener una descripción y la página 158 para ver un diagrama de esta configuración.

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Protocolos IP Interfaces	Interf. 0 (TR ranura 1 puerto 1) Dirección IP: 172.128.1.2 Másc. subred: 255.255.255.0	`IP Config>`**`add address`**	
Protocolos IP OSPF General	OSPF (seleccionado)	`Config>`**`p ospf`** `OSPF Config>`**`enable ospf`** (Aceptar otros valores por omisión)	
Protocolos IP OSPF Config. de área General	Número de área: 0.0.0.0 Área apéndice (no seleccionada)	`OSPF Config>`**`set area`**	
Protocolos IP OSPF Interfaces	Interfaz 0 OSPF (seleccionado)	`OSPF Config>`**`set interface`** `Dirección IP interfaz:` **`172.128.1.2`** `Se conecta a área:` **`0.0.0.0`** (Aceptar otros valores por omisión)	
Protocolos APPN General	Nodo red APPN (para habilitar) ID de red: NUBNODE Nombre punto de control: CPNU	`Config>`**`p appn`** `APPN config>` **`set node`** `Enable APPN` `Network ID:` **`NUBNODE`** `Control point name:` **`CPNU`** (Aceptar otros valores por omisión)	4

Protocolos
APPN
Interfaces
	(resaltar Red en Anillo interfaz 0)
	(pulsar pestaña Configure)
	Def. puerto APPN (para habil.)
	Nombre de puerto: TR3270
	Direcc. alto rend. (HPR) sop.
	(no sel. para inhabilitar)
	Sop. múlt. PU (sel. para hab.)
		`APPN config>`**`add port`**
		`APPN Port Link Type:` **`TOKEN RING`**
		`Port name:` **`TR3270`**
		`Enable APPN`
		`Support multiple PUs`
		`High performance routing:` **`No`**
		(Aceptar otros valores por omisión)
			5

Tabla 19. Subárea TN3270E (continuación). Consulte la página 138 para obtener una descripción y la página 158 para ver un diagrama de esta configuración.

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Protocolos APPN Interfaces	(resaltar Red en Anillo interfaz 0) (pulsar pestaña Link stations) STAT001 (nueva definición) Pestaña General-1: Nombre est. enl.: STAT001 Solic. sesión SSCP (sel.) Func. APPN sop. de enl. (no seleccionado) Pestaña General-2: Direcc. MAC nodo adyac.: 400000003172 ID de nodo: 12244 Dirección SAP local: 04 (**Add** para crear Est. de enlace) STAT002 (nueva definición) Pestaña General-1: Nomb. estac. enl.: STAT002 Solic. sesión SSCP (sel.) Func. APPN sop. de enl. (no seleccionado) Pestaña General-2: Direcc. MAC nodo adyac.: 400000003172 ID de nodo: 12245 Dirección SAP local: 08 (**Add** para crear Est. de enlace)	APPN config>**add link** Port name for the link stat.: **TR3270** Station name: **STAT001** MAC add. of adj. node: **400000003172** Solicit SSCP Session: **Yes** Local Node ID: **12244** Local SAP address: **4** Does link support APPN function?: **No** (Aceptar otros valores por omisión) APPN config>**add link** Port name for the link stat.: **TR3270** Station name: **STAT002** MAC add. of adj. node: **400000003172** Solicit SSCP Session: **Yes** Local Node ID: **12245** Local SAP address: **8** Does link support APPN function?: **No** (Aceptar otros valores por omisión)	6
Protocolos APPN Servidor TN3270E General	TN3270E (selecc. para habilitar) Dirección IP: 172.128.1.2 Descon. autom. (sel. para hab.)	APPN config>**tn** TN3270E config>**set** Enable TN3270E Server TN3270E Server IP Add.: **172.128.1.2** Automatic logoff: **Yes** (Aceptar otros valores por omisión)	7
Protocolos APPN Servidor TN3270E LU	Nombre de PU local: STAT001 (pulsar en **Implicit Pool**) Másc. nombre LU: @LU1A Número de def. de estación de trabajo implícitas: 10 Nombre de PU local: STAT002 (pulsar en **Implicit Pool**) Másc. nombre LU: @LU2A Número de def. de estación de trabajo implícitas: 10 (**LUs** para def. LU explícitas) Nombre de LU: PC03A Dirección NAU: 5 (pulsar en **Add**)	TN3270E config>**add imp** Station Name: **STAT001** LU name mask: **@LU1A** Number of Implicit LUs in Pool: **10** TN3270E config>**add imp** Station Name: **STAT002** LU name mask: **@LU2A** Number of Implicit LUs in Pool: **10** TN3270E config>**add lu** Station Name: **STAT002** LU name: **PC03A** NAU address: **5**	8

Tabla 19. Subárea TN3270E (continuación). Consulte la página 138 para obtener una descripción y la página 158 para ver un diagrama de esta configuración.

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.

Notas:

1. **add dev** define un solo puerto, no un adaptador.
2. El programa de configuración asigna automáticamente un número de interfaz a todos los puertos de un adaptador y el usuario suprime los que no desea utilizar. Desde la línea de mandatos, escriba el mandato **add dev** para cada puerto que desee utilizar y el número de interfaz (también conocido como ″número de red″) es la salida del mandato.
3. Sólo necesita una comunidad SNMP con capacidad para grabación si desea bajar archivos de configuración directamente del programa de configuración al direccionador. SNMP no es necesario para enviar mediante TFTP un archivo de configuración al direccionador.
4. Si tiene una red de subárea SNA pura sin APPN, el ID de red puede ser cualquier valor. Si tiene APPN en la red, el ID de red debe adaptarse a los convenios de denominación de red APPN.
5. APPN debe habilitarse aunque este ejemplo utilice la subárea SNA para la conexión de servidor TN3270E al sistema principal. Esto se debe a que el código de servidor TN3270E utiliza la pila SNA APPN para las comunicaciones APPN y de subárea en el sistema principal.
6. Al crear las estaciones de enlace, también está creando implícitamente PU. A estas PU se les asigna aquí un ″ID de nodo local″. Éste debe coincidir con el ″IDNUM″ de la definición de nodo principal SW de VTAM. El bloque de ID es siempre 077 para un Network Utility. Si necesita definir múltiples estaciones de enlace (PU), cada estación de enlace tiene que tener una dirección SAP local diferente.

   Si se establece `Solicit SSCP session` en `yes`, se define el enlace como una conexión de subárea.
7. A partir de MAS V3.2, el Servidor TN3270E tiene su propio submenú de línea de mandatos.
8. Para las LU implícitas, sólo tiene que definir las agrupaciones. `@LU1A` es una plantilla que se utilizará para crear los nombres de LU reales en la agrupación. En este ejemplo, con 10 LU en la agrupación, los nombres de LU generados son `@LU1A2, @LU1A3, @LU1A4,...@LU1A11` que corresponden a las LOCADDR 2-11 para la PU definida en VTAM. Del mismo modo, `@LU2A` generará `@LU2A2, @LU2A3, @LU2A4`. Tenga en cuenta que el nombre de LU `@LU2A5` no se utiliza porque la dirección NAU de 5 se ha reservado para la definición explícita. Por consiguiente, las LU restantes de la agrupación son `@LU2A6` a `@LU2A12`.

   Para las LU explícitas, el nombre de LU proporcionado aquí debe coincidir con el nombre definido en la configuración de emulación 3270 de la estación de trabajo. La dirección NAU apunta a la LOCADDR de la definición de PU apropiada del Nodo principal conmutado de VTAM.

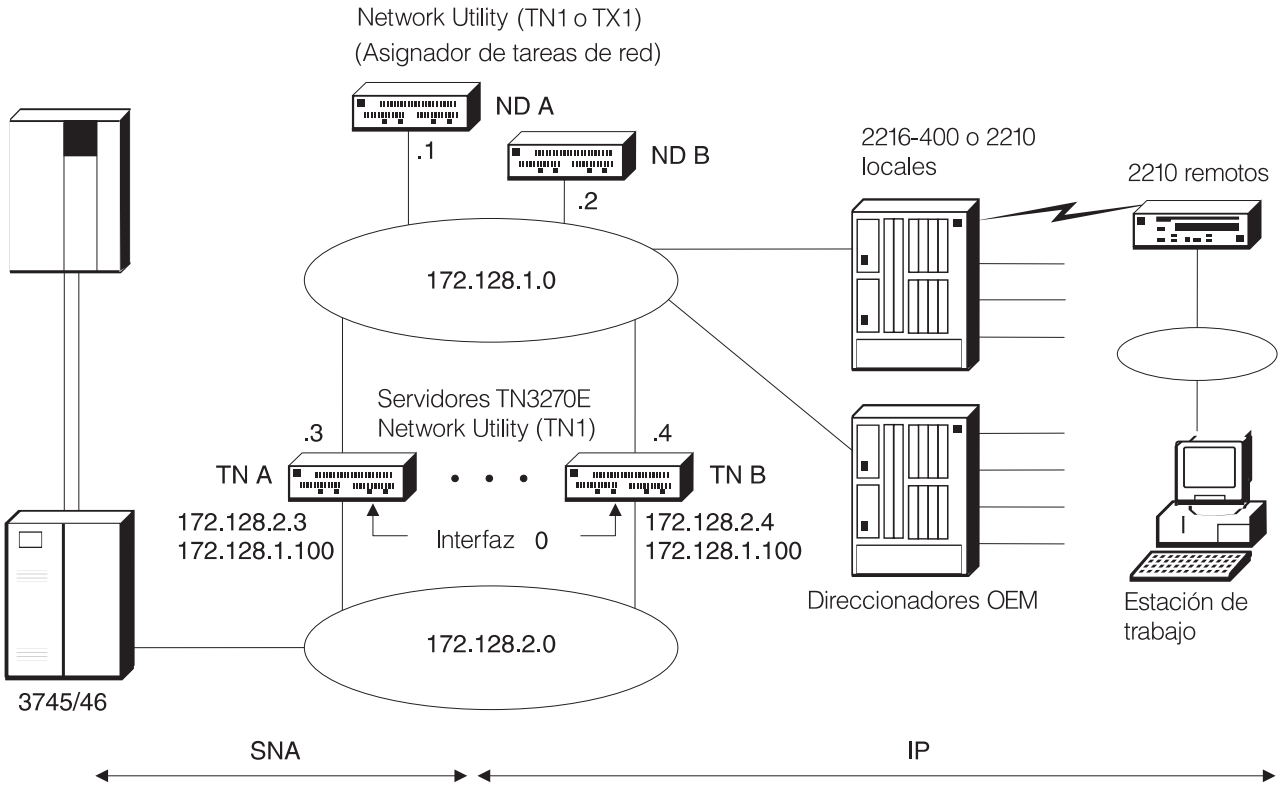


Figura 18. Config de servidor TN3270E -TN3270 altamente escalable y con tolerancia de errores

Tabla 20. Config de servidor TN3270E -TN3270 altamente escalable y con tolerancia de errores. Consulte la página 143 para obtener una descripción y la página 162 para ver un diagrama de esta configuración. **Esta tabla proporciona la configuración para el servidor TN A.***Consulte la Tabla 21 en la página 166 y la Tabla 22 en la página 168 para conocer la configuración de los Asignadores de tareas de red para este ejemplo.*

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Dispositivos Adaptadores Ranuras	Ranura1: TR de 2 puertos	Ver ″add dev″ en la fila siguiente	1
Dispositivos Adaptadores Puertos	Ranura 1/Puerto 1: Interfaz 0: TR Ranura 1/Puerto 2: Interfaz 1: TR	Config>**add dev tok** (una vez para cada interfaz)	2
Dispositivos Interfaces	Interfaz 0 Dirección Mac 400022AA0053 Interfaz 1 Dirección Mac 400022AA0003	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:53** TKR config>**exit** Config>**net 1** TKR config>**set phy 40:00:22:AA:00:03**	
Sistema General	Nombre de sistema: NU_A Ubicación: XYZ Contacto: Administrador	Config>**set host** Config>**set location** Config>**set contact**	
Sistema SNMP Config General	SNMP (seleccionado)	Config>**p snmp** SNMP Config>**enable snmp**	
Sistema SNMP Config Comunidades General	Nombre de comunidad: admin Tipo acceso: Trampa lect.-grab. Vista de comunidad: Toda	SNMP Config>**add community** SNMP Config>**set comm access write**	3

Tabla 20. Config de servidor TN3270E -TN3270 altamente escalable y con tolerancia de errores (continuación). Consulte la página 143 para obtener una descripción y la página 162 para ver un diagrama de esta configuración. **Esta tabla proporciona la configuración para el servidor TN A.***Consulte la Tabla 21 en la página 166 y la Tabla 22 en la página 168 para conocer la configuración de los Asignadores de tareas de red para este ejemplo.*

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Protocolos IP General	Dirección interna: 172.128.252.3 ID direccionador: 172.128.1.3 Misma subred (seleccionado)	Config>**p ip** IP config>**set internal 172.128.252.3** IP config>**set router-id 172.128.1.3** IP config>**enable same-subnet**	4
Protocolos IP Interfaces	Interf. 0 (TR ranura 1 puerto 1) Dirección IP: 172.128.2.3 Másc. subred: 255.255.255.0 Dirección IP: 172.128.1.100 Másc. subred: 255.255.255.0 Interfaz 1 (TR ranura 1 puerto 2) Dirección IP: 172.128.1.3 Másc. subred: 255.255.255.0	IP config>**add address 0 172.128.2.3 255.255.255.0** IP config>**add address 0 172.128.1.100 255.255.255.0** IP config>**add address 1 172.128.1.3 255.255.255.0**	5,6
Protocolos IP OSPF General	OSPF (seleccionado)	Config>**p ospf** OSPF Config>**enable ospf**	
Protocolos IP OSPF Config. de área General	Número de área: 0.0.0.0 Área apéndice (no seleccionada)	OSPF Config>**set area**	
Protocolos IP OSPF Interfaces	Interfaz 1 OSPF (seleccionado)	OSPF Config>**set interface** Interface IP address: **172.128.1.3** Attaches to area: **0.0.0.0** (Aceptar otros valores por omisión)	7
Protocolos APPN General	Nodo red APPN (sel. para hab.) ID de red: NUBNODE Nombre punto de control: CPNU	Config>**p appn** APPN config> **set node** Enable APPN Network ID: **NUBNODE** Control point name: **CPNU** (Aceptar otros valores por omisión)	8
Protocolos APPN Interfaces	(resaltar Red en Anillo interfaz 0) (pulsar en pestaña **configure**) Def. puerto APPN (sel. habil.) Nombre de puerto: TR3270 Direcc. alto rend. (HPR) sop. (no selecc. para inhabil.) Sop. múlt. PU (sel. para hab.)	APPN config>**add port** APPN Port Link Type: **TOKEN RING** Port name: **TR3270** Enable APPN Support multiple PUs High performance routing: **No** (Aceptar otros valores por omisión)	9

Tabla 20. Config de servidor TN3270E -TN3270 altamente escalable y con tolerancia de errores (continuación). Consulte la página 143 para obtener una descripción y la página 162 para ver un diagrama de esta configuración. **Esta tabla proporciona la configuración para el servidor TN A.***Consulte la Tabla 21 en la página 166 y la Tabla 22 en la página 168 para conocer la configuración de los Asignadores de tareas de red para este ejemplo.*

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Protocolos APPN Interfaces	(resaltar Red en Anillo interfaz 0) (pulsar pestaña **Link stations**) STAT001 (nueva definición) Pestaña General-1: Nomb. est. enlace: STAT001 Solic. sesión SSCP (sel.) Func. APPN sop. de enl. (no seleccionado) Pestaña General-2: Direcc. MAC nodo adyac.: 400000003172 ID de nodo: 12244 Dirección SAP local: 04 (**Add** para crear Estac. enlace) STAT002 (nueva definición) Pestaña General-1: Nomb. est. enlace: STAT002 Solic. sesión SSCP (sel.) Func. APPN sop. de enl. (no seleccionado) Pestaña General-2: Direcc. MAC nodo adyac.: 400000003172 ID de nodo: 12245 Dirección SAP local: 08 (**Add** para crear Estac. enlace)	APPN config>**add link** Port name for the link stat.: **TR3270** Station name: **STAT001** MAC add. of adj. node: **400000003172** Solicit SSCP Session: **Yes** Local Node ID: **12244** Local SAP address: **4** Does link support APPN function?: **No** (Aceptar otros valores por omisión) APPN config>**add link** Port name for the link stat.: **TR3270** Station name: **STAT002** MAC add. of adj. node:**400000003172** Solicit SSCP Session: **Yes** Local Node ID: **12245** Local SAP address: **8** Does link support APPN function?: **No** (Aceptar otros valores por omisión)	10
Protocolos APPN Servidor TN3270E General	TN3270E (selecc. para habilit.) Dirección IP: 172.128.1.100 Desc. autom. (sel. para habil.)	APPN config>**tn** TN3270E config>**set** Enable TN3270E Server TN3270E Server IP Add.:**172.128.1.100** Automatic logoff: **Yes** (Aceptar otros valores por omisión)	11
Protocolos APPN Servidor TN3270E LU	Nombre de PU local: STAT001 (pulsar en **Implicit Pool**) Másc. nombre LU: @LU1A Núm. de def. de estación de trabajo implícitas: 10 Nombre de PU local: STAT002 (pulsar en **Implicit Pool**) Másc. nombre LU: @LU2A Núm. de def. de estación de trabajo implícitas: 10	TN3270E config>**add imp** Station Name: **STAT001** LU name mask: **@LU1A** Number of Implicit LUs in Pool: **10** TN3270E config>**add imp** Station Name: **STAT002** LU name mask: **@LU2A** Number of Implicit LUs in Pool: **10**	12

Tabla 20. Config de servidor TN3270E -TN3270 altamente escalable y con tolerancia de errores (continuación). Consulte la página 143 para obtener una descripción y la página 162 para ver un diagrama de esta configuración. **Esta tabla proporciona la configuración para el servidor TN A.***Consulte la Tabla 21 en la página 166 y la Tabla 22 en la página 168 para conocer la configuración de los Asignadores de tareas de red para este ejemplo.*

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.

Notas:

1. **add dev** define un solo puerto, no un adaptador.
2. El programa de configuración asigna automáticamente un número de interfaz a todos los puertos de un adaptador y el usuario suprime los que no desea utilizar. Desde la línea de mandatos, escriba el mandato **add dev** para cada puerto que desee utilizar y el número de interfaz (también conocido como ″número de red″) es la salida del mandato.
3. Sólo necesita una comunidad SNMP con capacidad para grabación si desea bajar archivos de configuración directamente del programa de configuración al direccionador. SNMP no es necesario para enviar mediante TFTP un archivo de configuración al direccionador.
4. Debe habilitar la ″función de la misma subred″ porque está utilizando dos interfaces con una dirección IP dentro de la misma subred. (172.128.1.3 se asigna a TR 1 y 172.128.1.100 (dirección de cluster) se asigna como segunda dirección a TR 0).
5. Observe que a la Interfaz 0 se le han asignado dos direcciones IP, una de las cuales es la dirección de cluster utilizada por el Asignador de tareas de red. El Servidor TN3270E se configurará para la misma dirección en un paso subsiguiente. Todo el tráfico TN3270 se enviará a esta dirección a través del Asignador de tareas de red. Para que este tráfico alcance la cola IP interna Network Utility, es necesario asignar esta dirección a una dirección de interfaz o a la dirección interna. En este ejemplo, se ha asignado a una interfaz como la segunda dirección de dicha interfaz.
6. Observe que Interfaz 0 está en el segmento de LAN que está conectado a la pasarela SNA. Este segmento lleva el tráfico LLC del servidor TN3270 a la pasarela. En función del resto de la configuración del Network Utility, puede que este segmento no tenga ningún tráfico IP. Sin embargo, dado que todos los servidores TN3270E tendrán la misma dirección IP asignada a la interfaz de este segmento, se le ha asignado una dirección de subred (172.128.2) y todos los servidores TN3270E también tendrán una dirección en esta subred (en este caso 172.128.2.3) a fin de evitar un conflicto de direccionamiento IP.
7. Es muy importante ***no*** habilitar OSPF en la dirección de cluster del Asignador de tareas de red. Si se habilita, la dirección de cluster se difundirá en la red como si estuviera en el servidor TN3270E (además de la máquina del Asignador de tareas de red).
8. Si tiene una red de subárea SNA pura sin APPN, el ID de red puede ser cualquier valor. Si tiene APPN en la red, el ID de red debe adaptarse a los convenios de denominación de red APPN.
9. APPN debe habilitarse aunque el ejemplo utilice la subárea SNA para la conexión de servidor TN3270E al sistema principal. Esto se debe a que el código de servidor TN3270E utiliza la pila SNA APPN para las comunicaciones APPN y de subárea en el sistema principal.
10. Al crear las estaciones de enlace, también está creando implícitamente PU. A estas PU se les asigna aquí un ″ID de nodo local″. Éste debe coincidir con el ″IDNUM″ de la definición de nodo principal SW de VTAM. El bloque de ID es siempre 077 para un Network Utility. Si necesita definir múltiples estaciones de enlace (PU), cada estación de enlace tiene que tener una dirección SAP local diferente.
11. A partir de MAS V3.2, el Servidor TN3270E tiene su propio submenú de línea de mandatos.
12. Para las LU implícitas, sólo tiene que definir las agrupaciones. `@LU1A` es una plantilla que se utilizará para crear los nombres de LU reales en la agrupación. En este ejemplo, con 10 LU en la agrupación, los nombres de LU generados son `@LU1A2, @LU1A3,...@LU1A11` que corresponden a las LOCADDR 2-11 para la PU definida en VTAM. Del mismo modo, `@LU2A` generará `@LU2A2, @LU2A3, ... @LU2A11`.

Tabla 21. Config de Asignador de tareas de red - TN3270 altamente escalable y con tolerancia de errores. Consulte la página 143 para obtener una descripción y la página 162 para ver un diagrama de esta configuración. **Esta tabla proporciona la configuración para el Asignador de tareas de red primario, ND A.** *Consulte la Tabla 22 en la página 168 para conocer la configuración del Asignador de tareas de red de reserva. Consulte la Tabla 19 en la página 158 para conocer la configuración de los servidores TN3270E para este ejemplo.*

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Dispositivos Adaptadores Ranuras	Ranura 1: TR de 2 puertos	Ver ″add device″ en la fila siguiente	1
Dispositivos Adaptadores Puertos	Ranura 1/Puerto 1: Interf. 0: TR	`Config>`**`add dev tok`**	2
Dispositivos Interfaces	Interfaz 0 Dirección MAC: 400022AA0001	`Config>`**`net 0`** `TKR config>`**`set phy 40:00:22:AA:00:01`**	
Sistema General	Nombre de sistema: NU_A Ubicación: XYZ Contacto: Administrador	`Config>`**`set host`** `Config>`**`set location`** `Config>`**`set contact`**	
Sistema SNMP Config General	SNMP (seleccionado)	`Config>`**`p snmp`** `SNMP Config>`**`enable snmp`**	
Sistema SNMP Config Comunidades General	Nombre de comunidad: admin Tipo acceso: Trampa lect.-grab. Vista de comunidad: Toda	`SNMP Config>`**`add community`** `SNMP Config>`**`set comm access write`**	3
Protocolos IP General	Dirección interna: 172.128.252.1 ID direccionador: 172.128.1.1	`Config>`**`p ip`** `IP config>`**`set internal 172.128.252.1`** `IP config>`**`set router-id 172.128.1.1`**	4
Protocolos IP Interfaces	Interf. 0 (TR ranura 1 puerto 1) Dirección IP: 172.128.1.1 Másc. subred: 255.255.255.0	`IP config>`**`add address`**	
Protocolos IP OSPF General	OSPF (seleccionado)	`Config>`**`p ospf`** `OSPF Config>`**`enable ospf`**	
Protocolos IP OSPF Config. de área General	Número de área: 0.0.0.0 Área apéndice (no seleccionada)	`OSPF Config>`**`set area`**	
Protocolos IP OSPF Interfaces	Interfaz 0 OSPF (seleccionado)	`OSPF Config>`**`set interface`** `Interface IP address` **`172.128.1.1`** `Attaches to area` **`0.0.0.0`** (Aceptar otros valores por omisión)	
Características Asignador tareas de red Direccionador Ejecutor	Ejecutor (seleccionado)	`Config>`**`feat ndr`** `NDR Config>`**`enable executor`**	
Características Asignador tareas de red Direccionador Clusters Detalle	Dirección cluster: 172.128.1.100	`NDR Config>`**`add cluster`** `Cluster Address:` **`172.128.1.100`** (Aceptar otros valores por omisión)	

Tabla 21. Config de Asignador de tareas de red - TN3270 altamente escalable y con tolerancia de errores (continuación). Consulte la página 143 para obtener una descripción y la página 162 para ver un diagrama de esta configuración. **Esta tabla proporciona la configuración para el Asignador de tareas de red primario, ND A.** *Consulte la Tabla 22 en la página 168 para conocer la configuración del Asignador de tareas de red de reserva. Consulte la Tabla 19 en la página 158 para conocer la configuración de los servidores TN3270E para este ejemplo.*

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Características Asignador tareas de red Direccionador Clusters Puertos	Número de puerto 23	NDR Config>**add port** Cluster Address **172.128.1.100** Port number **23** (Aceptar otros valores por omisión)	
Características Asignador tareas de red Direccionador Clusters Servidores	Dirección de servidor: 172.128.1.3 172.128.1.4	NDR Config>**add server** Cluster Address**: 172.128.1.100** Port number**: 23** Server Address**: 172.128.1.3** (Aceptar otros valores por omisión) (Repetir para 172.128.1.4)	
Características Asignador tareas de red Direccionador Gestor	Gestor (seleccionado) Proporción Activa: 10 Nueva: 10 Asesor: 80 Sistema: 0	NDR Config>**enable manager** NDR Config>**set manager propor** Active**: 10** New**: 10** Advisor**: 80** System**: 0** (Aceptar otros valores por omisión)	5
Características Asignador tareas de red Direccionador Asesores	Asesor (seleccionado) Nombre de asesor: TN3270 Puerto de asesor: 23 Tiempo de espera: 10	NDR Config>**add advisor** Advisor name**: 3** (for TN3270) Timeout**: 10** (Aceptar otros valores por omisión) NDR Config>**enable advisor** Advisor name**: 3** (for TN3270) Port number**: 23**	6
Características Asignador tareas de red Direccionador Reserva	Reserva (selecc. para habilitar) Función de reserva: PRIMARY Estrat. conmut. atrás: MANUAL	NDR Config>**add backup** Role**: 0**=PRIMARY Switch back strategy**: 1**=MANUAL	7
Características Asignador tareas de red Direccionador Alcances	Dirección de alcance: (Entrar dirección y pulsar **Add**) 172.128.1.3 172.128.1.4	NDR Config>**add reach** Address to reach**: 172.128.1.3** (Repetir para 172.128.1.4)	8
Características Asignador tareas de red Direccionador Latidos	Dirección de origen: 172.128.1.1 Dirección de destino: 172.128.1.2 (Entrar direcc. y pulsar **Add**)	NDR Config>**add heartbeat** Source Heartbeat Addr.**: 172.128.1.1** Target Heartbeat Addr.**: 172.128.1.2**	8

Tabla 21. Config de Asignador de tareas de red - TN3270 altamente escalable y con tolerancia de errores (continuación). Consulte la página 143 para obtener una descripción y la página 162 para ver un diagrama de esta configuración. **Esta tabla proporciona la configuración para el Asignador de tareas de red primario, ND A.** *Consulte la Tabla 22 para conocer la configuración del Asignador de tareas de red de reserva. Consulte la Tabla 19 en la página 158 para conocer la configuración de los servidores TN3270E para este ejemplo.*

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.

Notas:

1. **add dev** define un solo puerto, no un adaptador.
2. El programa de configuración asigna automáticamente un número de interfaz a todos los puertos de un adaptador y el usuario suprime los que no desea utilizar. Desde la línea de mandatos, escriba el mandato **add dev** para cada puerto que desee utilizar y el número de interfaz (también conocido como ″número de red″) es la salida del mandato.
3. Sólo necesita una comunidad SNMP con capacidad para grabación si desea bajar archivos de configuración directamente del programa de configuración al direccionador. SNMP no es necesario para enviar mediante TFTP un archivo de configuración al direccionador.
4. Debe establecerse la dirección interna para que las funciones del asesor y del gestor se comuniquen con el componente ejecutor de asignador de tareas de red.
5. Los valores para Activa, Nueva, Asesor y Sistema deben sumar un máximo 100. La proporción de Asesor toma por omisión 0. Necesitará cambiar este valor para que se pueda utilizar la entrada de Asesor para equilibrar la carga de tráfico de TN3270. En este caso, se ha establecido en `80` para proporcionarle un peso mucho mayor que los de las conexiones activas y nuevas.
6. El número de puerto de comunicaciones (toma por omisión 10008) debe coincidir con el ″Puerto de asesor de Asignador de tareas de red″.
7. La estrategia de conmutación hacia atrás debe ser la misma para los asignadores de tareas de red primario y de reserva. IBM recomienda un valor manual para que pueda planificar la conmutación hacia atrás en un momento en que tenga la menor probabilidad de interrumpir las sesiones SNA.
8. Las direcciones de alcance son las direcciones que el Asignador de tareas de red debe poder alcanzar con el fin de determinar que está funcionado correctamente. El asignador de tareas de red primario envía esta información al asignador de tareas de red de reserva. Si el asignador de tareas de red de reserva determina que tiene mejores posibilidades de alcance que el primario, efectuará una conmutación y tomará el papel principal. Elija como mínimo un sistema principal en cada subred que utiliza el Asignador de tareas de red. Asimismo, añada las direcciones para cada servidor del cluster. En este ejemplo, el Asignador de tareas de red utiliza solamente una interfaz y ambos servidores están en la misma subred que esta interfaz.
9. Aquí, está configurando la conexión que el Asignador de tareas de red primario utilizará para enviar los latidos al Asignador de tareas de red de reserva. Puede definir varias vías si tiene múltiples conexiones entre los asignadores de tareas de red primario y de reserva. Los latidos se enviarán a través de la primera vía que esté disponible. La solución más segura es configurar una segunda vía entre el asignador de tareas de red primario y el asignador de tareas de red de reserva utilizando la segunda ranura que esté disponible en cada Network Utility.

Tabla 22. Config de Asignador de tareas de red - TN3270 altamente escalable y con tolerancia de errores. Consulte la página 143 para obtener una descripción y la página 162 para ver un diagrama de esta configuración. **Esta tabla proporciona las diferencias de configuración para el Asignador de tareas de red de reserva ND B basado en la Tabla 21 en la página 166, que proporciona la configuración para el Asignador de tareas de red primario.** *La definición para el Asignador de tareas de red de reserva es la misma que para el Primario excepto en las diferencias que se muestran en esta tabla. Estas diferencias corresponden a las direcciones de interfaz y a las funciones de reserva del Asignador de tareas de red. Los parámetros relacionados con el Asignador de tareas de red que no se muestran aquí deben ser idénticos a los valores configurados en el primario. También se recomienda que la configuración de hardware sea igual para ambos Asignadores de tareas de red primario y de reserva. Consulte la Tabla 20 en la página 162 para conocer la configuración de los servidores TN3270E para este ejemplo.*

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Dispositivos Interfaces	Interfaz 0 Dirección MAC 400022AA0002	`Config>`**`net 0`** `TKR config>`**`set phy 40:00:22:AA:00:02`**	

Tabla 22. Config de Asignador de tareas de red - TN3270 altamente escalable y con tolerancia de errores (continuación). Consulte la página 143 para obtener una descripción y la página 162 para ver un diagrama de esta configuración. **Esta tabla proporciona las diferencias de configuración para el Asignador de tareas de red de reserva ND B basado en la Tabla 21 en la página 166, que proporciona la configuración para el Asignador de tareas de red primario.** *La definición para el Asignador de tareas de red de reserva es la misma que para el Primario excepto en las diferencias que se muestran en esta tabla. Estas diferencias corresponden a las direcciones de interfaz y a las funciones de reserva del Asignador de tareas de red. Los parámetros relacionados con el Asignador de tareas de red que no se muestran aquí deben ser idénticos a los valores configurados en el primario. También se recomienda que la configuración de hardware sea igual para ambos Asignadores de tareas de red primario y de reserva. Consulte la Tabla 20 en la página 162 para conocer la configuración de los servidores TN3270E para este ejemplo.*

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Sistema General	Nombre de sistema: NU_ND2	`Config>`**`set host`**	
Protocolos IP General	Dirección interna: 172.128.252.2 ID direccionador: 172.128.1.2	`Config>`**`p ip`** `IP config>` **`set internal 172.128.252.2`** **`set router-id 172.128.1.2`**	1
Protocolos IP Interfaces	Interfaz 0 (TR ranura 1 puerto 1) Dirección IP: 172.128.1.2 Másc. subred: 255.255.255.0	`Config>`**`p ip`** `IP config>`**`add address`**	
Protocolos IP OSPF Interfaces	Interfaz 0 OSPF (seleccionado)	`Config>`**`p ospf`** `OSPF Config>`**`set interface`** `Interface IP address:` **`172.128.1.2`** `Attaches to area:` **`0.0.0.0`** (aceptar otros valores por omisión)	

Características
Asignador tareas de red
Direccionador
Reserva
	Reserva (selecc. para habilitar)
	Función de reserva: BACKUP
	Estrat. conmut. atrás: MANUAL
		`Config>`**`feat NDR`**
		`NDR Config>`**`add backup`**
		`Role:` **`1`**`=BACKUP`
		`Switch back strategy:` **`1`**`=MANUAL`	

Características Asignador tareas de red Direccionador Latidos	Dirección de origen: 172.128.1.2 Dirección de destino: 172.128.1.1 (Entrar direcc. y pulsar en **Add**)	`NDR Config>`**`add heartbeat`** `Source Heartbeat Addr.:` **`172.128.1.2`** `Target Heartbeat Addr.:` **`172.128.1.1`**	2

Notas:

1. Debe establecerse la dirección interna para que las funciones del asesor y del gestor se comuniquen con el componente ejecutor de asignador de tareas de red.
2. El asignador de tareas de red de reserva debe configurarse con la misma información que el asignador de tareas de red primario de forma que si el primario falla, el de reserva pueda asumir las funciones completas del primario incluyendo el envío de los latidos y de la información de alcance al primario cuando éste vuelva a estar en línea.

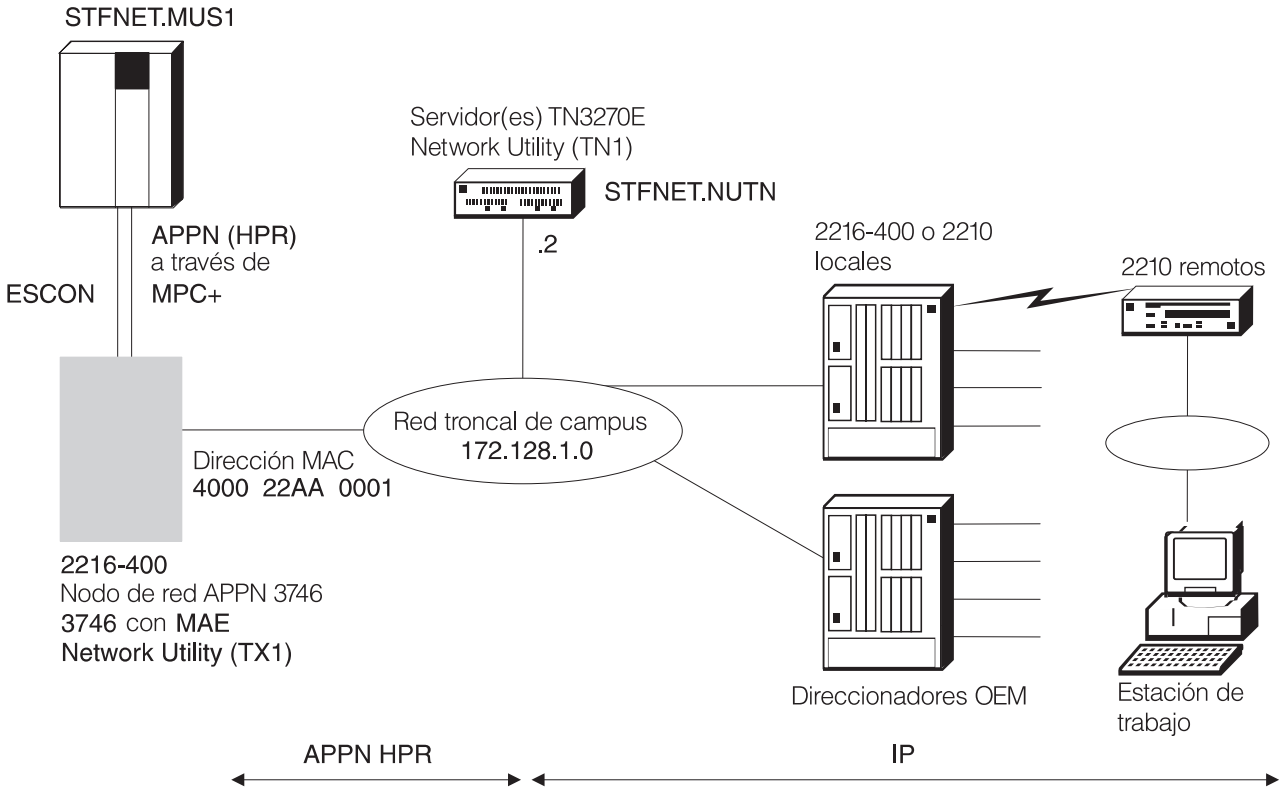


Figura 19. TN3270 a través de DLUR por APPN

Tabla 23. TN3270 a través de DLUR por APPN. Consulte la página 146 para obtener una descripción y la página 170 para ver un diagrama de esta configuración.

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Dispositivos Adaptadores Ranuras	Ranura1: TR de 2 puertos	Ver ″add dev″ en la fila siguiente	1
Dispositivos Adaptadores Puertos	Ranura 1/Puerto 1: Interfaz 0: TR	Config>**add dev tok**	2
Dispositivos Interfaces	Interfaz 0 Dirección Mac 400022AA0011	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:11**	
Sistema General	Nombre de sistema: NU_A Ubicación: XYZ Contacto: Administrador	Config>**set host** onfig>**set location** Config>**set contact**	
Sistema SNMP Config General	SNMP (seleccionado)	Config>**p snmp** SNMP Config>**enable snmp**	
Sistema SNMP Config Comunidades General	Nombre de comunidad: admin Tipo acceso: Trampa lect.-grab. Vista de comunidad: Toda	SNMP Config>**add community** SNMP Config>**set comm access write**	3
Protocolos IP General	Dirección interna: 172.128.252.2 ID direccionador: 172.128.1.2	Config>**p ip** IP config>**set internal 172.128.252.2** IP config>**set router-id 172.128.1.2**	

Tabla 23. TN3270 a través de DLUR por APPN (continuación). Consulte la página 146 para obtener una descripción y la página 170 para ver un diagrama de esta configuración.

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Protocolos IP Interfaces	Interf. 0 (TR ranura 1 puerto 1) Dirección IP: 172.128.1.2 Másc. subred: 255.255.255.0	IP config>**add address**	
Protocolos IP OSPF General	OSPF (seleccionado)	Config>**p ospf** OSPF Config>**enable ospf**	
Protocolos IP OSPF Configuración de área General	Número de área: 0.0.0.0 Área apéndice (no seleccionada)	OSPF Config>**set area**	
Protocolos IP OSPF Interfaces	Interfaz 0 OSPF (seleccionado)	OSPF Config>**set interface** Interface IP address: **172.128.1.2** Attaches to area: **0.0.0.0** (Aceptar otros valores por omisión)	
Protocolos APPN General	Nodo red APPN (sel. para hab.) ID de red: STFNET Nombre punto de control: NUTN	Config>**p appn** APPN config> **set node** Enable APPN Network ID: **STFNET** Control point name: **NUTN** (Aceptar otros valores por omisión)	
Protocolos APPN Interfaces	(resaltar Red en Anillo interfaz 0) (pulsar pestaña Configure) Def. puerto APPN (sel. habil.) Nombre de puerto: TR001	APPN config>**add port** APPN Port Link Type: **TOKEN RING** Port name: **TR001** Enable APPN (Aceptar otros valores por omisión)	4
Protocolos APPN Interfaces	(resaltar Red en Anillo interfaz 0) (pulsar pestaña Link stations) TRTG001 (nueva definición) Pestaña General-1: Nomb. est. enlace: TRTG001 Pestaña General-2: Direcc. MAC nodo adyac.: 400022AA0001 Tipo de nodo adyacente: Nodo de red APPN (**Add** para crear Est. de enlace)	APPN config>**add link** Port name for the link stat.: **TR001** Station name: **TRTG001** MAC addr. of adj. node: **400022AA0001** (Aceptar otros valores por omisión)	5
Protocolos APPN DLUR	DLUR (selecc. para habilitar) Nombre CP totalmente calif. de DLUS primario: STFNET.MVS1	APPN config>**set dlur** Enable DLUR Fully-qualified CP name of primary DLUS: **STFNET.MVS1** (Aceptar otros valores por omisión)	6
Protocolos APPN Servidor TN3270E General	TN3270E (selecc. para hab.) Dirección IP: 172.128.1.2 Desc. autom. (sel. para habil.)	APPN config>**tn** TN3270E config>**set** Enable TN3270E Server TN3270E Server IP Addr.: **172.128.1.2** Automatic logoff: **Yes** (Aceptar otros valores por omisión)	7

Tabla 23. TN3270 a través de DLUR por APPN (continuación). Consulte la página 146 para obtener una descripción y la página 170 para ver un diagrama de esta configuración.

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Protocolos APPN Servidor TN3270E PU locales	Nombre est. de enlace: PUPS08T ID de nodo: 12244 Nombre est. de enlace: PUPS18T ID de nodo: 12245	TN3270E config>**exit** APPN config>**add loc** Station Name: **PUPS08T** Local Node ID: **12244** (Aceptar otros valores por omisión) APPN config>**add loc** Station Name: **PUPS18T** Local Node ID: **12245** (Aceptar otros valores por omisión)	8
Protocolos APPN Servidor TN3270E LU	Nombre de PU local: PUPS08T (pulsar en **Implicit Pool**) Másc. nombre LU: @LU1A Número de def. de estación de trabajo implícitas: 5 Nombre de PU local: PUPS18T (pulsar en **Implicit Pool**) Másc. nombre LU: @LU2A Número de def. de estación de trabajo implícitas: 5	APPN config>**tn** TN3270E config>**add imp** Station Name: **PUPS08T** LU name mask: **@LU1A** Number of Implicit LUs in Pool: **5** TN3270E config>**add imp** Station Name: **PUPS18T** LU name mask: **@LU2A** Number of Implicit LUs in Pool: **5**	9

Notas:

1.

add dev define un solo puerto, no un adaptador.

El programa de configuración asigna automáticamente un número de interfaz a todos los puertos de un adaptador y el usuario suprime los que no desea utilizar. Desde la línea de mandatos, escriba el mandato **add dev** para cada puerto que desee utilizar y el número de interfaz (también conocido como ″número de red″) es la salida del mandato.

Sólo necesita una comunidad SNMP con capacidad para grabación si desea bajar archivos de configuración directamente del programa de configuración al direccionador. SNMP no es necesario para enviar mediante TFTP un archivo de configuración al direccionador.

Al utilizar APPN, puede usar el Direccionamiento de alto rendimiento (HPR) o el Direccionamiento de sesión intermedio (ISR). HPR es el valor por omisión y es lo que se utiliza en este escenario.

La dirección MAC especificada es la dirección MAC de la pasarela de sistema principal APPN.

El nombre de CP de DLUS es el VTAM de sistema principal.

Los ID de nodo local entrados para estas PU necesitan coincidir con los campos IDNUM de las definiciones de PU del VTAM de sistema principal.

A partir de MAS V3.2, el Servidor TN3270E tiene su propio submenú de línea de mandatos.

Para las LU implícitas, sólo tiene que definir las agrupaciones. `@LU1A` es una plantilla que se utilizará para crear los nombres de LU reales en la agrupación. En este ejemplo, con 5 LU en la agrupación, los nombres de LU generados son `@LU1A2`, `@LU1A3`, `@LU1A4`, `@LU1A5` y `@LU1A6` que corresponden a las LOCADDR 2-6 para la PU definida en VTAM. Del mismo modo, @LU2A generará `@LU2A2` a `@LU2A6`.

Definición dinámica de LU dependientes

Este escenario se ha creado con un MVS ejecutando VTAM V4R4 y un IBM 2216 que se ha conectado mediante ESCON al sistema principal. El Network Utility tenía un adaptador de Red en Anillo de dos puertos en la ranura 1 y un adaptador ESCON en la ranura 2. Se ha utilizado el protocolo de bucle de retorno LSA para la comunicación a través del canal ESCON. El Network Utility se ha definido como un Nodo de red y ha utilizado APPN/ISR para comunicarse con VTAM. Las PU y LU de TN3270E se han conectado a VTAM utilizando DLUR/DLUS.

La función DDDLU se ha probado utilizando las definiciones VTAM siguientes:

- X5303—Un nodo principal XCA, necesario para la conexión ESCON utilizando LSA
- SW5303N—Un nodo principal conmutado VTAM para la PU NN de Network Utility
- DDDPU—Un nodo principal conmutado VTAM para las LU definidas dinámicamente que sólo contiene una sentencia PU con referencia a un LUGROUP y con el parámetro LUSEED
- DDGROUP—El nodo principal LUGROUP de VTAM, con definición de modelo para las LU 3270

El archivo de configuración 2216 para este escenario era DDD.

La Figura 20 muestra las relaciones de diferentes parámetros en VTAM y en el 2216 para este escenario.

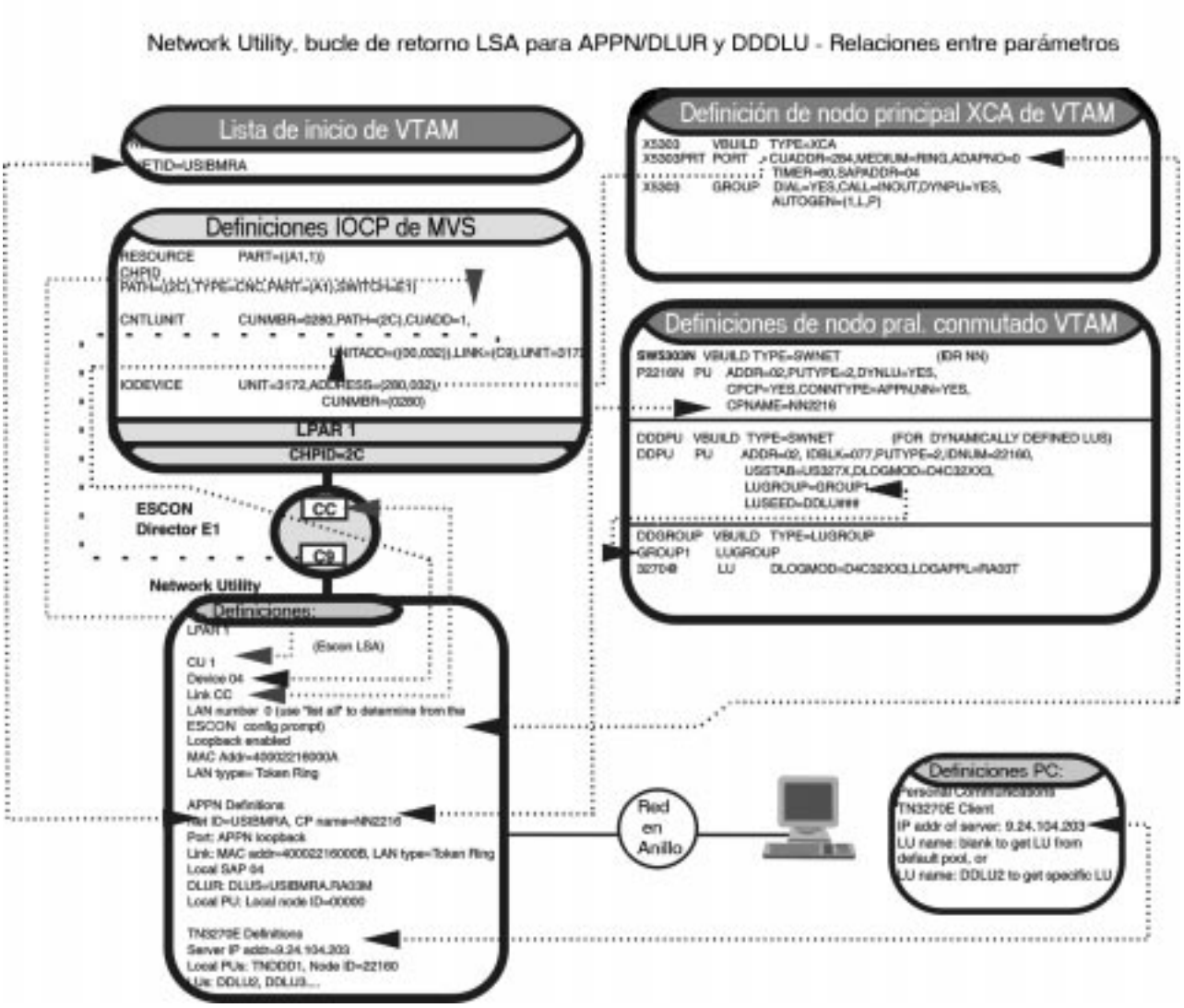


Figura 20. Relaciones de parámetros, el Network Utility/2216 ejecuta TN3270E con DDDLU y APPN/DLUR utilizando el bucle de retorno LSA a través del canal ESCON

La Tabla 24 lista el nodo principal real XCA VTAM utilizado.

Tabla 24. Nodo principal de XCA X5303 para conexión de canal ESCON

```
*************************Top of Data ***********************
X5303    VBUILD TYPE=XCA
X5303    VBUILD TYPE=XCA
X5303PRT PORT  ADAPNO=0,
X5303PRT PORT  ADAPNO=0,                                    *
               CUADDR=284,                                  *
               SAPADDR=4,                                   *
               MEDIUM=RING
X5303GRP GROUP DIAL=YES,CALL=INOUT,DYNPU=YES,               *
               AUTOGEN=(1,L,P)
*********************** Bottom of Data ******************
```

La Tabla 25 contiene el nodo principal conmutado real SW5303N de VTAM para el Nodo de red en 2216.

Tabla 25. Nodo principal conmutado SW5303N para nodo de red 2216

```
***************************** Top of Data ******************************
SW5303N  VBUILD TYPE=SWNET
P2216N   PU    ADDR=02,         X
               PUTYPE=2,        X
               CPCP=YES,        X
               CONNTYPE=APPN,   X
               USSTAB=US327X,   X
               NN=YES,          X
               DYNLU=YES,       X
               CPNAME=NN2216
***************************** Bottom of Data ***************************
```

Para las PU de Punto de control APPN, por ejemplo el Nodo de red mostrado en la Tabla 25, no necesita números de Bloque ID ni de Núm. ID. Los Nodos de red se pueden reconocer unos a otros mediante los nombres de red totalmente calificados.

Tabla 26. Nodo principal DDGROUP de LUGROUP, Modelo para definiciones de LU

```
***************************** Top of Data ******************************
DDGROUP  VBUILD TYPE=LUGROUP
GROUP1   LUGROUP
3270@    LU    DLOGMOD=D4C32XX3,LOGAPPL=RA03T       1
***************************** Bottom of Data ***************************
```

1. El nombre 3270@ especifica el tipo de dispositivo 3270. La utilización de @ como último carácter especifica que coincide con cualquier número de modelo del producto, 3270. De los parámetros de sentencia LU, sólo se muestran DLOGMOD y LOAGAPPL. Sin embargo, puede especificar cualquier parámetro de LU adicional que pueda serle necesario.

Tabla 27. Nodo principal conmutado DDDPU para las LU definidas dinámicamente

```
***************************** Top of Data ******************************
DDDPU    VBUILD TYPE=SWNET
DDPU     PU    ADDR=02,                                          X
               IDBLK=077,         1                              X
               IDNUM=22160,                                      X
               PUTYPE=2,                                         X
               USSTAB=US327X,                                    X
               LUGROUP=GROUP1,    2                              X
               LUSEED=DDLU###,    3                              X
               DLOGMOD=D4C32XX3
***************************** Bottom of Data ***************************
```

1. El Network Utility de IBM utiliza 077 como valor de IDBLK.

2. Este parámetro apunta a la sentencia LUGROUP con el nombre GROUP1 de un nodo principal LUGROUP. Consulte la tabla 26.
3. Con este valor LUSEED, las LU creadas dinámicamente tendrán nombres que empiezan por DDLU, seguidos del número de dirección local de LU en formato de tres dígitos decimales.

Tabla 28. Configuración DDD realizada con el programa de configuración de MAS 3.3 (Parte 1 de 2)

Navegación por programa de configuración	**Valores de programa de configuración**
Dispositivos Ranuras	Ranura 1: TR de 2 puertos Ranura 2: ESCON
Dispositivos Adaptadores de canal Interfaces ESCON Interfaces ESCON	Tipo de protocolo: LSA Tipo de LAN: Red en Anillo Dirección MAC (LAN virtual LSA, lado de VTAM): p.ej. 40002216000A Pulsar en **Loopback** Pulsar en **Add**
Dispositivos Adaptadores de canal Interfaces ESCON Subcanales ESCON	Direcciones de dispositivo: 4 Tipo de subcanal: lectura/grabación LPAR: 1 Dirección de enlace: CC CU: 1 Pulsar en **Add**
Dispositivos Adaptadores de canal Red de bucle de retorno APPN	Tipo de LAN: Red en Anillo Dirección MAC: 40002216000B Pulsar en **Add**
Sistema General	Nombre de sistema: DDD Ubicación: Sala de máquinas Contacto: su nombre
Sistema Usuarios	Nombre: ID de usuario Permiso: Administrativo Contraseña: contraseña Repetir contraseña: contraseña Pulsar en **Add**
Sistema SNMP Config Comunidades General	Nombre: público Tipo de acceso: Trampa de lectura-grabación Pulsar en **Add**
Protocolos IP Detalles	Dirección interna: 9.24.104.203
Protocolos IP Interfaces	Interfaz 1 (TR ranura 1 puerto 2) Dirección IP: 9.24.106.9 Máscara de subred: 255.255.255.0 Pulsar en **Add** Dirección IP: 9.24.104.203 Máscara de subred: 255.255.255.0 Pulsar en **Add**
Protocolos APPN General	Pulsar en **APPN network node** ID de red: USIBMRA Nombre de punto de control: NN2216
Protocolos APPN DLUR	Pulsar en **DLUR** Nombre totalmente calificado de DLUS primario: USIBMRA.RA03M

Tabla 29. Configuración DDD, realizada con el programa de configuración de MAS 3.3 (Parte 2 de 2)

Navegación por programa de configuración	**Valores de programa de configuración**
Protocolos APPN Interfaces	Pulsar elemento de línea **APPN Net—Token Ring** Pulsar cabecera **Configure** (Sel. pestaña General) Pulsar en **Define APPN Port** Pulsar en **Service Any Node** Pulsar ***off*** **High Performance Routing (HPR)** Soportados Pulsar en **Support Multiple PUs** Seleccionar pestaña **Port Definition** Especificar dirección SAP local: 04
Protocolos Servidor TN3270E General	Pulsar en **TN3270E** Dirección IP: 9.24.104.203
Protocolos Servidor TN3270E PU locales	Nombre de estación de enlace: TNDDD1 ID de nodo: 22160 DLUS primario: USIBMRA.RA03M Pulsar en **Add**
Protocolos Servidor TN3270E LU	Seleccionar **TNDDD1** Pulsar en cabecera **LUs** Nombre de LU: DDLU2 Clase: Implícita Dirección NAU: 2 Pulsar en **Add** Repetir Nombre de LU, Clase, Dirección NAU Añadir secuencia para cada LU

Supervisión de la configuración

Por lo general, en los Network Utility se puede supervisar -entre otros- el estado de las conexiones en uso, las agrupaciones, las correlaciones mediante **talk 5/appn/tn3270e**.

Para obtener una lista de todos los recursos definidos localmente, por ejemplo las LU, las PU y las agrupaciones, puede utilizar **talk 6/appn/tn3270e**. Consulte la Tabla 30 en la página 177 para conocer la configuración de TN3270E.

Tabla 30. Listado de configuración de TN3270E bajo talk 6/p app/tn3270e

```
DDD TN3270E config>LIST ALL
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 9.24.104.203
TN3270E Port Number: 23
Default Pool Name : PUBLIC
NetDisp Advisor Port Number: 10008
Client IP Address Mapping : N
Keepalive type: NONE
Automatic Logoff: N        Timeout: 30
        Enable IP Precedence: N

DLUS Link Station: TNDDD1
        Fully-qualified CP name of primary DLUS: USIBMRA.RA03M
        Fully-qualified CP name of backup DLUS:
        Local Node ID: 22160
        Auto activate : YES
        Host Initiated Dynamic LU Definition : NO
        LU Name   NAU addr     Class             Assoc LU Name   Assoc NAU
addr
        ------------------------------------------------------------------------
        DDLU2        2     Implicit Workstation
        DDLU3        3     Implicit Workstation
        DDLU4        4     Implicit Workstation
--More--
        DDLU5        5     Implicit Workstation
        DDLU6        6     Explicit Workstation
        DDLU7        7     Explicit Workstation


Client IP Address mapping
-------------------------
Client IP Address   Address Mask       Resource Name
-----------------------------------------------------


Multiple Port
-----------------------------
Port Number    Enable TN3270E    Resource Name
-----------------------------------------------
DDD TN3270E config>
```

Los mandatos de la Tabla 31 en la página 178 le llevan primero a **talk 5/appn/tn3270e**.

Podrá ver entonces el estado actual de los recursos TN3270E. En este momento no hay sesiones de usuario final activas, pero una PU con 6 LU está activa en la sesión SSCP-LU.

Tabla 31. Traslado a talk 5/appn/tn3270 para estado de TN3270E

```
DDD *TALK 5

DDD +PROTOCOL APPN
APPN GWCON
DDD APPN >TN3270E
TN3270E GWCON
DDD TN3270E >LIST STATUS
TN3270E Server Status Summary

TN3270E IP Address: 9.24.104.203
NetDisp Advisor Port Number: 10008
  Keepalive type: None
  Automatic Logoff: N
  Client IP Address mapping : N
  Number of connections                   : 1
  Number of available LUA LU's            : 5
  Number of LUA LU's pending termination  : 0
  Number of defined LU's                  : 6
  Number of connections in SSCP-LU state  : 0
  Number of connections in LU-LU state    : 1     1
 DDD TN3270E >
```

Este número aumenta según las sesiones LU-LU establecidas entre las LU definidas bajo Network Utilities y las aplicaciones VTAM.

Después de que el primer usuario haya establecido una sesión y haya dejado el campo de nombre de LU en blanco en el cliente, LIST CONNECTIONS bajo **talk 5/appn/tn3270e** tiene el aspecto que se muestra en la Tabla 32:

Tabla 32. Primera sesión establecida, LU seleccionada de agrupación por omisión

```
DDD TN3270E >LIST CONNECTIONS
Connection information for all the LUs

Local LU  Class  Assoc LU   Client Addr     Status   Prim LU  Sec LU  Idle
Min
------------------------------------------------------------------------------
DDLU5      IW              9.24.106.217      LU-LU  RA03T07   DDLU005   0
DDD TN3270E >
```

Después de que un segundo usuario abra su sesión, de nuevo sin nombre específico de LU o agrupación, la lista de conexiones tiene el aspecto mostrado en la Tabla 33:

Tabla 33. Dos sesiones que utilizan la agrupación por omisión

```
DDD TN3270E >LIST CONNECTIONS
Connection information for all the LUs

Local LU  Class  Assoc LU   Client Addr     Status   Prim LU  Sec LU  Idle
Min
------------------------------------------------------------------------------
DDLU2      IW              9.24.106.127      LU-LU  RA03T08   DDLU002   0
DDLU5      IW              9.24.106.217      LU-LU  RA03T07   DDLU005   4
DDD TN3270E >
```

La Tabla 34 en la página 179 es un ejemplo del aspecto que tiene la lista de conexiones cuando se conecta un tercer usuario, que solicita la LU DDLU7 explícita.

Tabla 34. Lista de conexiones con dos usuarios LU implícita y un usuario de LU explícita

```
DDD TN3270E >LIST CONNECTIONS
Connection information for all the LUs

Local LU  Class  Assoc LU   Client Addr     Status   Prim LU  Sec LU  Idle
Min
------------------------------------------------------------------------------
DDLU7      EW              9.24.106.146      LU-LU  RA03T09   DDLU007   0
DDLU2      IW              9.24.106.127      LU-LU  RA03T08   DDLU002   6
DDLU5      IW              9.24.106.217      LU-LU  RA03T07   DDLU005   6
DDD TN3270E >
```

Definición de LU dinámica iniciada por el sistema principal

Este escenario se ha establecido con un MVS ejecutando VTAM V4R4 y un Network Utility de IBM, conectado mediante ESCON al sistema principal. En el Network Utility, hay un adaptador de Red en Anillo de dos puertos en la ranura 1 y un adaptador ESCON en la ranura 3. Se ha utilizado el protocolo de bucle de retorno LSA para la comunicación a través del canal ESCON. El Network Utility se ha definido como un Nodo de red que utiliza APPN/ISR para comunicarse con VTAM. Las PU y las LU de TN3270E se han conectado a VTAM utilizando DLUR/DLUS.

La función de Definición de HIDLU (Host Initiated Dynamic LU) (LU dinámica iniciada por sistema principal) se ha comprobado mediante las definiciones de VTAM siguientes:

- X5303 — nodo principal XCA para Network Utility conectado a ESCON por bucle de retorno LSA. De igual modo que en el escenario anterior para DDDLU.
- SW5303N — nodo principal conmutado para Nodo de red APPN de Network Utility. De igual modo que en el escenario anterior para DDDLU.
- SWHID — nodo principal conmutado que contiene definiciones de LU que crearán definiciones de LU explícitas en Network Utility.
- SWIMP — nodo principal conmutado cuyas definiciones de LU crearán LU implícitas en el Network Utility. Las LU implícitas van a la(s) agrupación (agrupaciones).

  Nota: En VTAM, todas las LU — implícitas o explícitas — se definen igual. Una LU se convierte en explícita o implícita en función de las definiciones de agrupación del Network Utility.

Las relaciones de parámetros entre la configuración de VTAM y del Network Utility se muestran en la Figura 21 en la página 180.

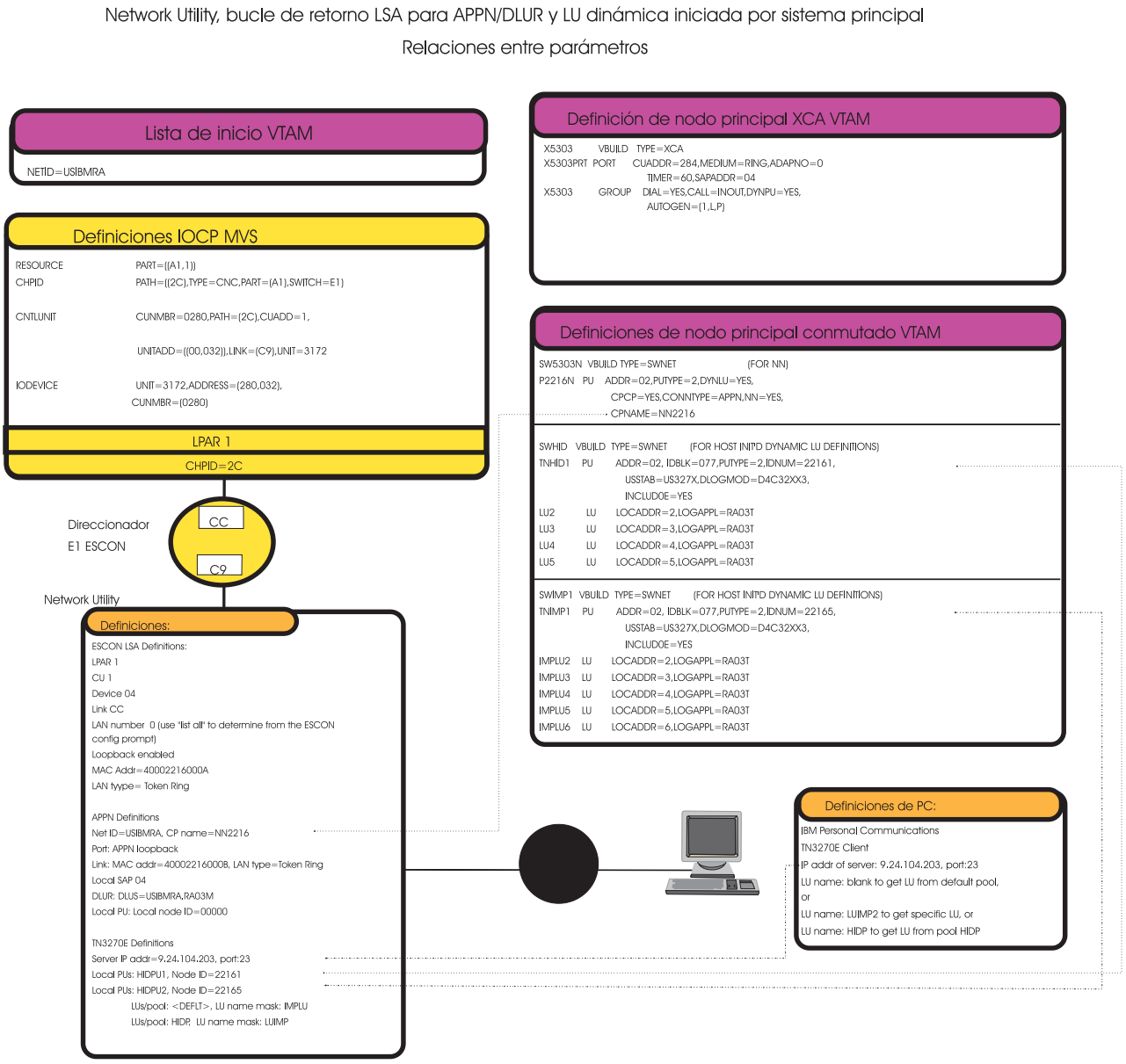


Figura 21. Relación de los parámetros de configuración para la definición de HIDLU

El nodo principal conmutado real SWHID se muestra en la Tabla 35.

Tabla 35. Definición de nodo principal conmutado SWHID1 en VTAM

```
****************************** Top of Data ******************************
SWHID1   VBUILD TYPE=SWNET
TNHID1   PU    ADDR=02,                                              X
               IDBLK=077,       1                                    X
               IDNUM=22161,                                          X
               PUTYPE=2,                                             X
               USSTAB=US327X,                                        X
               INCLUD0E=YES,    2                                    X
               DLOGMOD=D4C32XX3
LU2      LU    LOCADDR=02,LOGAPPL=RA03T
LU3      LU    LOCADDR=03,LOGAPPL=RA03T
LU4      LU    LOCADDR=04,LOGAPPL=RA03T
LU5      LU    LOCADDR=05,LOGAPPL=RA03T
****************************** Bottom of Data ***************************
```

1. Network Utility utiliza el valor IDBLK de 077.
2. Este parámetro es nuevo y necesario para la definición de HIDLU.

La Tabla 35 en la página 180 es una definición de Nodo principal conmutado para las LU de Network Utility definidas en agrupaciones.

Estas LU quedarán definidas en Network Utility con los nombres mostrados aquí (LU2 a LU5). Dado que las LU que representan estas NAU de red de VTAM aún no están definidas en el servidor TN3270E, las LU se convertirán en LU explícitas.

Para un cliente TN3270, se deberá definir el nombre de LU en el campo de nombre de LU del cliente para obtener una de estas LU.

También puede definir que las LU dinámicas iniciadas por el sistema principal vayan a una agrupación del Network Utility. Esto se realiza en el programa de configuración de MAS (o talk 6) definiendo una o más agrupaciones en el Network Utility y especificando el número de LU o los rangos de LU, así como una máscara de nombre para las LU que entran en una agrupación. Las LU siguientes bajo PU TNIMP1 se han definido de este modo.

Tabla 36. Definición de nodo principal conmutado SWIMP1 en VTAM

```
***************************** Top of Data ******************************
SWIMP1   VBUILD TYPE=SWNET
TNIMP1   PU    ADDR=02,                                              X
               IDBLK=077,      1                                     X
               IDNUM=22165,                                          X
               PUTYPE=2,                                             X
               USSTAB=US327X,                                        X
               INCLUD0E=YES,   2                                     X
               DLOGMOD=D4C32XX3
IMPLU2   LU    LOCADDR=02,LOGAPPL=RA03T
IMPLU3   LU    LOCADDR=03,LOGAPPL=RA03T
IMPLU4   LU    LOCADDR=04,LOGAPPL=RA03T
IMPLU5   LU    LOCADDR=05,LOGAPPL=RA03T
IMPLU6   LU    LOCADDR=06,LOGAPPL=RA03T
************************** Bottom of Data ***************************
```

1. Network Utility utiliza el valor IDBLK de 077.
2. Este parámetro es nuevo y necesario para la definición de HIDLU.

Las LU definidas en el nodo principal conmutado SWIMP se convertirán en LU implícitas y explícitas en el Network Utility debido a las definiciones de la configuración de MAS, como se muestra en la Tabla 38 en la página 183.

Las tres primeras LU — IMPLU2, IMPLU3 e IMPLU4 — van a la agrupación HIDP. Un usuario de TN3270E puede acceder a una de estas LU dejando vacío el campo de nombre de LU en el cliente TN3270E.

La siguiente LU, IMPLU5, se ha definido en el programa de configuración de MAS para que vaya a la agrupación por omisión, <DEFLT>. Un usuario puede obtener esta LU dejando vacío el campo de nombre de LU en el cliente TN3270E.

Para la última LU, IMPLU6, no se ha definido ninguna agrupación en el Network Utility. Se convierte por tanto en una LU explícita, llamada IMPLU6.

Nota: Al definir una agrupación en el servidor TN3270E, deberá proporcionar también una máscara de nombre de LU. Esta máscara en realidad altera temporalmente el nombre de LU de VTAM y las LU implícitas que pertenecen a una agrupación tendrán nombres basados en la máscara de

nombre de LU. Sólo al definir LU explícitas (que no van a una agrupación), obtendrá los nombres de LU directamente de VTAM.

Tabla 37. Configuración de HIDLU, realizada con el programa de configuración de MAS 3.3 (Parte 1 de 2)

Navegación por programa de configuración	**Valores de programa de configuración**
Dispositivos Ranuras	Ranura 1: TR de 2 puertos Ranura 2: ESCON
Dispositivos Adaptadores de canal Interfaces ESCON Interfaces ESCON	Tipo de protocolo: LSA Tipo de LAN: Red en Anillo Dirección MAC: (LAN virtual LSA, lado de VTAM): p.ej. 40002216000A Pulsar en **Loopback** Pulsar en **Add**
Dispositivos Adaptadores de canal Interfaces ESCON Subcanales ESCON	Dirección de dispositivo: 4 Tipo de subcanal: lectura/grabación LPAR: 1 Dirección de enlace: CC CU: 1 Pulsar en **Add**
Dispositivos Adaptadores de canal Red de bucle de retorno APPN	Tipo de LAN: Red en Anillo Dirección MAC: 40002216000B Pulsar en **Add**
Sistema General	Nombre de sistema: HID Ubicación: Sala de máquinas Contacto: su nombre
Sistema Usuarios	Nombre: ID de usuario Permiso: Administrativo Contraseña: contraseña Contraseña de repetición: contraseña Pulsar en **Add**
Sistema SNMP Config Comunidades General	Nombre: público Tipo de acceso: Trampa de lectura-grabación Pulsar en **Add**
Protocolos IP Detalles	Dirección interna: 9.24.104.203
Protocolos IP Interfaces	Interfaz 1 (TR ranura 1 puerto 2) Dirección IP: 9.24.106.9 Máscara de subred: 255.255.255.0 Pulsar en **Add** Dirección IP: 9.24.104.203 Máscara de subred: 255.255.255.0 Pulsar en **Add**
Protocolos APPN General	Pulsar en **APPN network node** ID de red: USIBMRA Nombre de punto de control: NN2216
Protocolos APPN DLUR	Pulsar en **DLUR** Nombre totalmente calificado de DLUS primario: USIBMRA.RA03M

Tabla 38. Configuración de HIDLU, realizada con el programa de configuración de MAS 3.3 (Parte 2 de 2)

Navegación por programa de configuración	**Valores de programa de configuración**
Protocolos APPN Interfaces	Pulsa en elemento de línea **APPN Net—token ring** Pulsar en cabecera **Configure** (Seleccionada pestaña General) Pulsar en **Define APPN Port** Pulsar en **Service Any Node** Pulsar en ***off* High Performance Routing (HPR) Supported** Pulsar en **Support Multiple PUs** Seleccionar pestaña **Port Definition** Especificar dirección SAP local: 04
Protocolos Servidor TN3270E General	Pulsar en **TN3270E** Dirección IP: 9.24.104.203
Protocolos Servidor TN3270E Agrupaciones	Nombre de agrupación: HIDP Pulsar en **Add**
Protocolos Servidor TN3270E PU locales	Nombre de estación de enlace: HIDPU1 ID de nodo: 22161 Pulsar en **Host-Initiated Dynamic LUs allowed for PU** DLUS primario: USIMBRA.RA03M Pulsar en **Add** Nombre de estación de enlace: HIDPU2 Pulsar en **Host-Initiated Dynamic LUs allowed for PU** ID de nodo: 22165 DLUS primario: USIBMRA.RA03M Pulsar en **Add**
Protocolos Servidor TN3270E LU	Seleccionar línea HIDPU2 Pulsar en cabecera Implicit pools Seleccionar nombre de agrupación: <DEFLT> Máscara de nombre de LU: IMPLU Pulsar en **Specify Address Ranges** Rangos de direcciones: 5 Pulsar en **Add** Seleccionar nombre de agrupación: HIDP Máscara de nombre de LU: LUIMP Pulsar en **Specify Address Ranges** Rangos de direcciones: 2-4 Pulsar en **Add**

Supervisión de la configuración

La configuración de HIDLU puede supervisarse en talk 5 bajo **protocol appn** y **tn3270e**.

Bajo talk 5, puede supervisar todas las interfaces como se muestra en la Tabla 39 en la página 184:

Tabla 39. Mandato de listado de interfaces bajo Talk 5

```
HID +INTERFACE
                                                 Self-Test  Self-Test Maintenance
Net   Net'   Interface   Slot-Port                  Passed     Failed      Failed
0     0      TKR/0       Slot: 1   Port: 1           1          0         0
1     1      TKR/1       Slot: 1   Port: 2           1          0         0
2     2      ESCON/0     Slot: 3   Port: 1           1          0         0
3     2      LSA/0       Slot: 0   Port: 0           1          3         0
4     4      TKR/2       Slot: 0   Port: 0           1          0         0
```

Tabla 40. Estadísticas bajo talk 5

```
HID +STATISTICS
Net   Interface      Unicast  Multicast      Bytes    Packets      Bytes
                   Pkts Rcv   Pkts Rcv   Received      Trans      Trans
0     TKR/0           22521      25742    1399673      22522     472997
1     TKR/1           24301    1476136   97150812      23588     582533
2     ESCON/0         11453          0    2976076       9930    1481020
3     LSA/0           11452          0    2976060       9929    1480999
4     TKR/2               0          0          0          0          0
```

Mediante la emisión del mandato **p app** (protocol appn) a nivel de talk 5, puede supervisar las funciones relacionadas con APPN, por ejemplo verificar las conexiones CP-CP como en la Tabla 41.

Tabla 41. Verificación de la conexión NN-NN a VTAM

```
HID +PROTOCOL APPN
HID APPN >LIST CP-CP_SESSIONS
          CP Name Type     Status    ConWinner ConLoser ConWinner ConLoser
                                        ID        ID    Sense     Sense
=============================================================================
    USIBMRA.RA03M  NN     Active     3710C590  3710C592 00000000  00000000
```

Las funciones de TN3270E están bajo APPN y se pueden obtener emitiendo el mandato, **TN3270E**, como en la Tabla 43. En el nivel de TN3270E, sólo puede emitir el mandato **LIST** con las terminaciones mostradas en la Tabla 42:

Tabla 42. Opciones de LIST bajo TN3270E

```
HID TN3270E >LIST ?

Possible completions:
        CONNECTIONS
        MAPPING
        POOLS
        PORTS
        STATUS
(you may cycle through these commands by pressing the TAB key)
HID TN3270E >LIST
```

Tabla 43. Supervisión de sesiones de TN3270E

```
HID APPN >TN3270E
TN3270E GWCON
HID TN3270E >LIST CONNECTIONS
Connection information for all the LUs

Local LU  Class  Assoc LU   Client Addr     Status   Prim LU  Sec LU  Idle
Min
------------------------------------------------------------------------------
IMPLU5     IW              9.24.106.127      LU-LU  RA03T01   IMPLU5    38
```

La Tabla 43 en la página 184 muestra las conexiones de TN3270E después de haber establecido la primera sesión. El cliente TN3270E no había definido ningún nombre de LU, de modo que se ha seleccionado una LU de la agrupación por omisión.

A continuación, otro usuario efectúa una conexión TN3270E, especificando en el cliente el nombre de agrupación HIDP como el nombre de LU. La Tabla 44 es un ejemplo de lo que puede ser la lista:

Tabla 44. LIST CONNECTIONS tras la conexión de un segundo usuario

```
HID TN3270E >LIST CONNECTIONS
Connection information for all the LUs

Local LU  Class  Assoc LU   Client Addr     Status   Prim LU  Sec LU  Idle
Min
------------------------------------------------------------------------------
LUIMP4     IW              9.24.106.217      LU-LU  RA03T07   IMPLU4    1
IMPLU5     IW              9.24.106.127      LU-LU  RA03T01   IMPLU5    45
```

Si un tercer usuario establece una sesión, definiendo IMPLU6 en el cliente, la lista de conexiones será parecida a la de la Tabla 45:

Tabla 45. LIST CONNECTIONS después de la conexión de un tercer usuario

```
HID TN3270E >LIST CONNECTIONS
Connection information for all the LUs

Local LU  Class  Assoc LU   Client Addr     Status   Prim LU  Sec LU  Idle
Min
------------------------------------------------------------------------------
IMPLU6     EW              9.24.106.146      LU-LU  RA03T09   IMPLU6    0
LUIMP4     IW              9.24.106.217      LU-LU  RA03T07   IMPLU4    4
IMPLU5     IW              9.24.106.127      LU-LU  RA03T01   IMPLU5    48
```

Antememoria de cliente HOD (Host On-Demand) de TN3270E

Para la función de Antememoria de cliente HOD, deberá configurar el servidor TN3270E y la función HOD bajo el asignador de tareas de red (Network Dispatcher). Para esta configuración, puede mantener exactamente la misma configuración que para el servidor TN3270E, que se lleva a cabo en la Tabla 28 en la página 175 para DDDLU y en la Tabla 37 en la página 182 para HIDLU. En este escenario, se han utilizado las definiciones de HIDLU para el servidor TN3270E.

Para la parte de Antememoria de cliente HOD del entorno, deberán definirse el ejecutor (’Executor’) del asignador de tareas de red (Network Dispatcher) y la antememoria de cliente HOD (HOD Client Cache), además de las otras definiciones ya realizadas en HIDLU o DDDLU (en secciones anteriores de este capítulo).

Para la instalación del HOD Server en este escenario, se han instalado los productos siguientes: NT Server, NT Service Pack 3, Web Server y HOD Server.

La dirección de bucle de retorno del recuadro HOD Server debe definirse para que apunte a la dirección IP de Cluster del asignador de tareas de red. No se puede hacer en la dirección IP del Cluster del Asignador de tareas de red.

En el escenario siguiente, se ha definido el adaptador de bucle de retorno en MS NT Server del modo siguiente:

1. Pulse en **Inicio** y luego en **Configuración**.
2. Pulse en **Panel de control**, efectúe una doble pulsación en **Red**.
3. Añada el controlador de adaptador de bucle de retorno MS (MS Loopback Adapter Driver).
4. En la ventana Red, pulse en **Adaptadores**.
5. Seleccione el adaptador de bucle de retorno MS (MS Loopback Adapter) y pulse en **Aceptar**.
6. Cuando se le solicite, inserte el CD o los disquetes de instalación.
7. En la ventana Red, pulse en **Protocolos**.
8. Seleccione los protocolos TCP/IP y, a continuación, pulse en **Propiedades**.
9. Seleccione el adaptador de bucle de retorno (Loopback Adapter) y pulse en **Aceptar**.
10. Establezca la dirección del adaptador de bucle de retorno en la dirección de Cluster del asignador de tareas de red y acepte la máscara de subred (255.0.0.0). No entre ninguna dirección de pasarela.

Al definir el HOD Server, no se olvide de realizar también la acción siguiente. En el escenario para el Windows NT Server, la dirección IP de cluster (9.24.104.207) se encuentra en la columna de pasarela después de emitirse el mandato **netstat -r**. Suprima de esta columna, las rutas ajenas si ve más de una entrada con la dirección IP de cluster. Suprima la que empieza con la misma dirección de red que la dirección IP de cluster seguida de sólo ceros. En este caso, la entrada a suprimir es la línea con la dirección IP 9.0.0.0.

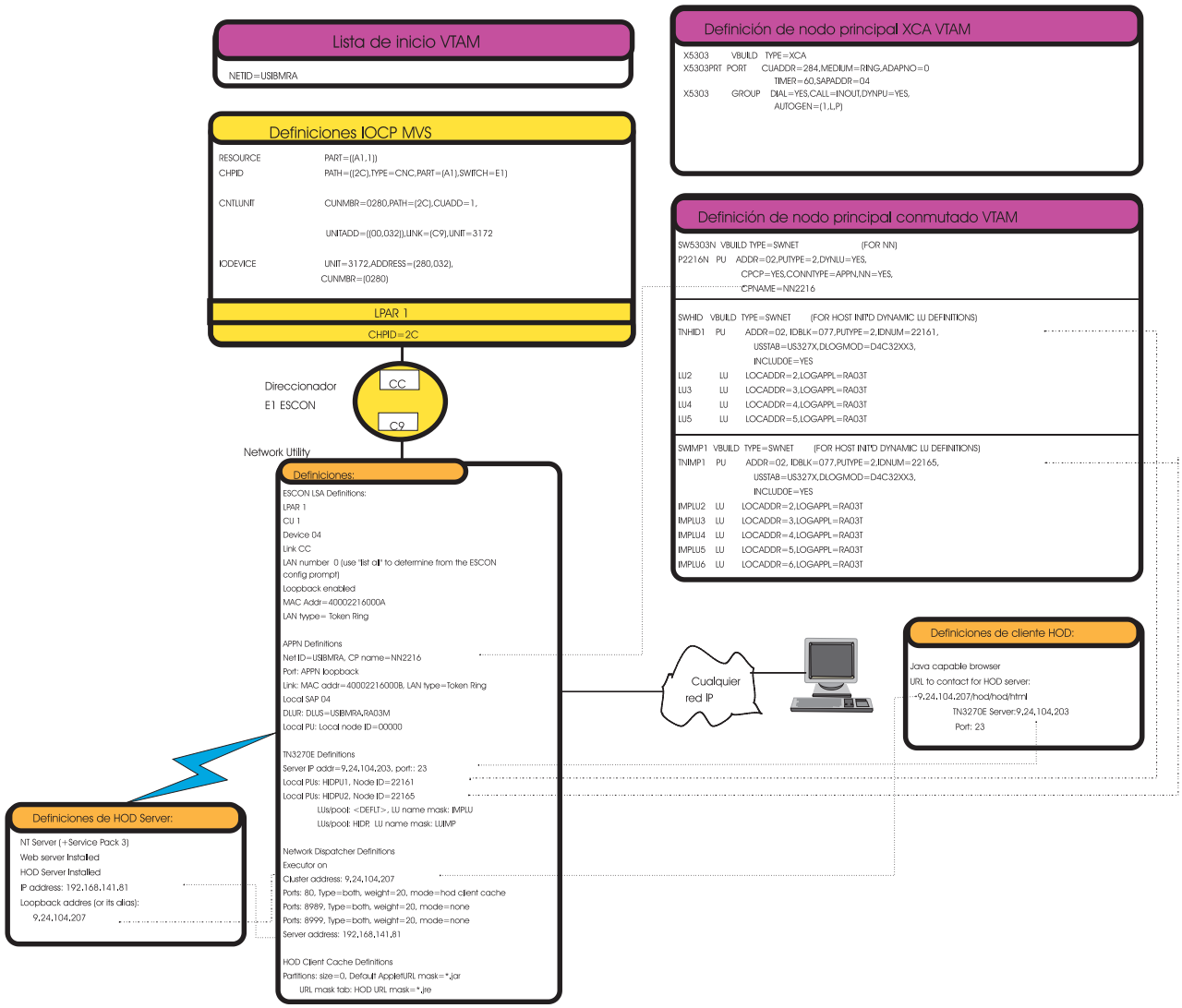


Figura 22. Relaciones entre parámetros de antememoria de cliente HOD

Para la configuración de Antememoria de cliente Host On-Demand, el HOD sólo se añade sobre la configuración DDDLU o HIDLU, como se ha realizado anteriormente en la Tabla 28 en la página 175 o en la Tabla 37 en la página 182, dado que éstas ya contienen las configuraciones de TN3270E.

Tabla 46. Configuración de antememoria de cliente HOD

Navegación por programa de configuración	**Valores de programa de configuración**
Dispositivos Interfaces	Interfaz 0: Ranura/Puerto=1/1 Pulsar en **Interfaz**
Protocolos IP Interfaces Direcciones	Pulsar en **Interface 0** Dirección IP: 192.168.141.82 Máscara 255.255.255.240 en nuestro escenario Pulsar en **ADD**

Tabla 46. Configuración de antememoria de cliente HOD (continuación)

Navegación por programa de configuración	**Valores de programa de configuración**			
Protocolos IP OSPF Interfaces	Pulsar en **address 192.168.141.82** Seleccionar recuadro OSPF			
Características Asignador de tareas de red Ejecutor	Pulsar **Executor** (ejecutor 'activado')			
Características Asignador de tareas de red Clusters Detalles	Dirección de cluster: 9.24.104.207 El resto son valores por omisión. Pulsar en **ADD**			
Características Asignador de tareas de red Clusters Puertos	*Número* 80 8989 8999	*Tipo* Ambos Ambos Ambos	*Modalidad* Cliente HOD Ninguna Ninguna	*Peso* 20 20 20
Características Asignador de tareas de red Clusters Servidores	Para los tres puertos: Dirección: 192.168.141.81 (NT Server) Peso: 20 Estado de servidor: activo Pulsar en **ADD**			
Características Asignador de tareas de red Clusters Antememoria de cliente HOD Proxies	Excluidos valores por omisión			
Características Asignador de tareas de red Clusters Antememoria de cliente HOD Particiones	Particiones: Applet por omisión: *.jar Los demás paráms. se dejan en el valor por omisión Máscara URL: Máscara URL: *jre Tipo de máscara URL: Incluir Pulsar en **ADD**			

En este ejemplo, con el navegador Netscape se ha seleccionado la dirección **http://9.24.104.207/hod/hod.html** y ha aparecido la pantalla que se ve en la Figura 23 en la página 189. Pulse el botón derecho del ratón en el icono 3270 para obtener la pantalla mostrada en la Figura 24 en la página 189. En dicha Figura 24 en la página 189, los parámetros del servidor TN3270E se definen del mismo modo que en el Network Utility.

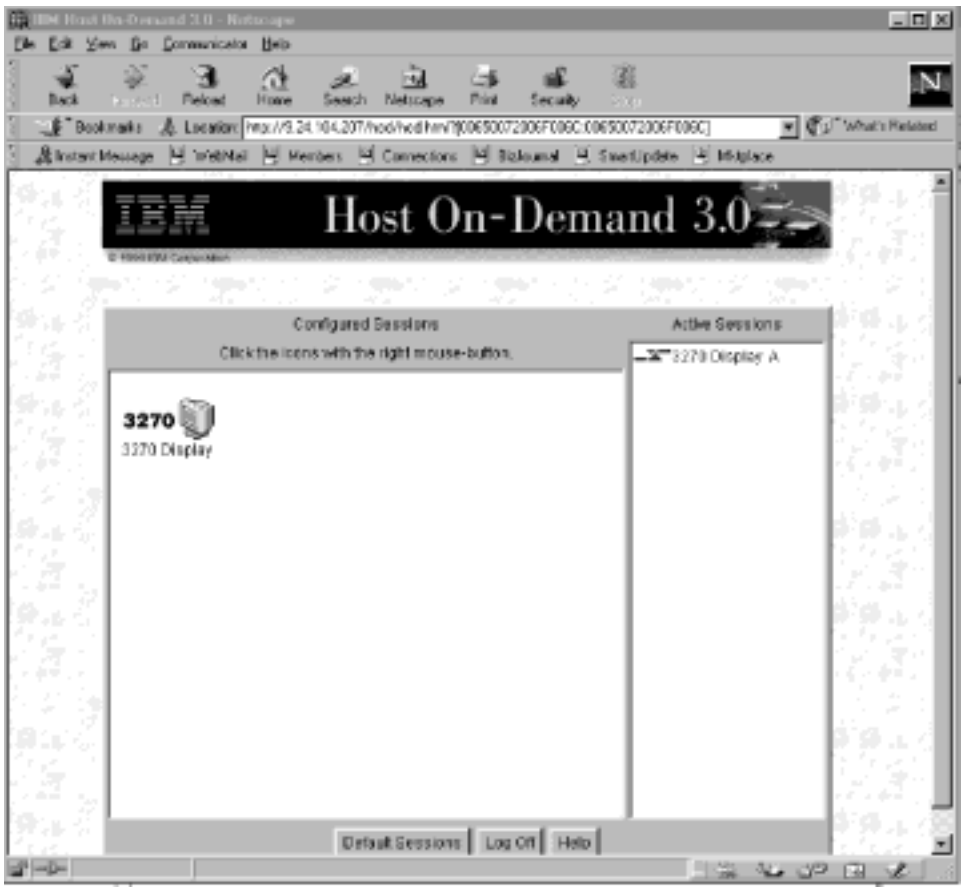


Figura 23. Pantalla del cliente HOD en el navegador (Netscape) de Internet

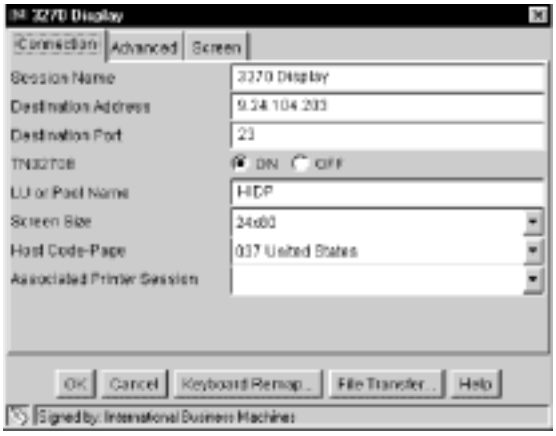


Figura 24. Definición de servidor TN3270E en cliente HOD

Después de esta definición, si efectúa una doble pulsación (con el botón izquierdo del ratón) en el icono 3270, aparecerá la pantalla siguiente (Figura 25 en la página 190).

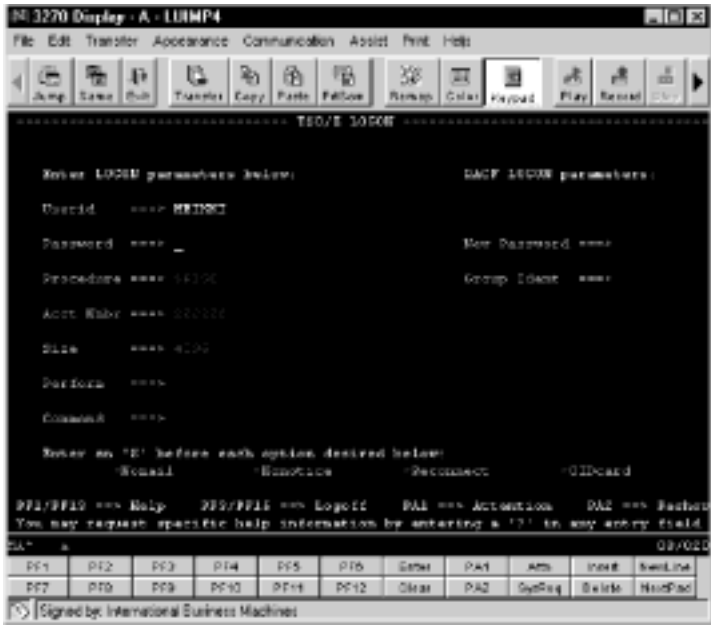


Figura 25. Pantalla de cliente HOD después de establecer la conexión

Supervisión de la configuración

Se emiten los mandatos siguientes para supervisar la configuración de HOD.

Tabla 47. Inicio de supervisión de antememoria en T5/ELS

```
HODCAC0 *TALK 5
HODCAC0 +EVENT
HODCAC0 ELS>NODISPLAY SUBSYSTEM ALL ALL
Complete
HODCAC0 ELS>DISPLAY SUBSYSTEM WEBH ALL
HODCAC0 ELS>    ..(Ctrl-P)
HODCAC0 *TALK 2
:
00:00:01  DOLOG: Server 192.168.141.81 has been set up.
:
00:20:01 WEBH.017: Client connection 31AE11C accepted as Socket 31BF564
00:20:01 WEBH.015: Conn (31AE11C) HTTP Proxy(cluster 9.24.104.207 port 80)
partition (0) opened
00:20:01 WEBH.009: HTTP Proxy(cluster 9.24.104.207 port 80) conn (31AE11C)
new req being parsed
00:20:01 WEBH.012: HTTP Proxy(cluster 9.24.104.207 port 80) partition (0)
conn (31AE11C) not using cache because object not found in cache     1
 :
 :
 :
```

1. Por primera vez, el cliente ha emitido una petición de applets Java desde la Dirección de cluster. Por consiguiente, este mensaje explica que no se ha encontrado en la antememoria del Network Utility.

Tabla 48. Supervisión de la definición de antememoria del cliente HOD

```
HODAC0 +FEATURE
Feature name or number [WAN Restoral System] ? hod
Host On-Demand Client Cache Console
HODCAC0 HOD Client Cache>LIst All
HOD Client Cache Partition 0    Status: Enabled
     Cluster address: 9.24.104.207  Port 80
1 partition(s) active.
External Cache Manager: Disabled
```

Tabla 49. Listado de antememoria de cliente HOD

```
HODCAC0 HOD Client Cache>LIst PArtition
HOD Client Cache Partition 0      Status: Enabled
        Cluster address: 9.24.104.207   Port 80
Partition size: Current - 1030296 bytes  Highest - 1030296 bytes  Max. - Unlimited
Number of objects: Current - 37  Highest - 37  Max. - Unlimited
Maximum object size: Unlimited
HOD Client Cache purge interval : 600 minute(s)
Hit ratio: 61%
Total number of hits:  59      1
Total number of misses:  37
Object Excluded (Object too large):          0
                (Object expired)             0
                (DONT CACHE header):         0
                (URL Mask excluded):         0
                (Image excluded):            0
                (Static object excluded):    0
                (Dynamic object excluded):   0
                (Cache disabled):            0
Objects explicitly Included: 0
Total number of purged objects: 0
Purged objects (Cache full):     0
               (Object stale):   0
               (Purged by user): 0
               (Invalidation):   0
```

1. Número de peticiones a la antememoria del Network Utility. Cuando los Clientes HOD son atendidos por la antememoria, las applets Java se entregan/bajan del Network Utility y en el NT Server no se instalará carga o tráfico de HOD Server.

Tabla 50. Visualización de la pantalla cuando otro cliente HOD solicita applets Java

```
HODCAC0 HOD Client Cache>LIst PArtition
HOD Client Cache Partition 0      Status: Enabled
         Cluster address: 9.24.104.207   Port 80
Partition size: Current - 1030296 bytes  Highest - 1030296 bytes  Max. - Unlimited
Number of objects: Current - 37  Highest - 37  Max. - Unlimited
Maximum object size: Unlimited
HOD Client Cache purge interval : 600 minute(s)
Hit ratio: 61%               1
Total number of hits:  59    2
Total number of misses:  37
Object Excluded (Object too large):          0
                (Object expired)             0  .....
:
:
```

1. La proporción de peticiones atendidas por la antememoria aumenta cuanto mayor es el número de peticiones de clientes HOD.
2. El número total de peticiones atendidas por la antememoria también aumenta con otras peticiones de clientes HOD. Éstos prueban que las applets Java se entregan de la antememoria del cliente HOD del Network Utility.

Ahora, las conexiones TN3270E pueden supervisarse del mismo modo que en las secciones de DDDLU y HIDLU tratadas anteriormente en este capítulo.

SNA de subárea de TN3270E a través de DLSw

Para el escenario de la función SNA de subárea de TN3270E a través de DLSw, consulte la Figura 26 en la página 195. El Network Utility A está conectado al canal ESCON y también al Network Utility B a través de un enlace PPP. Como puede verse en las pantallas de configuración siguientes, no hay ninguna función APPN en el Network Utility A puesto que la conexión a VTAM-Sistema principal es la Subárea. En el sistema principal, es necesario definir un Nodo principal conmutado VTAM (con el parámetro IDNUM) que apunte al ID de nodo local de Network Utility (que es '221B1' en nuestro escenario de ejemplo). Aunque ésta es una conexión SNA de subárea pura, la definición se realiza bajo APPN en el Network Utility B.

Tabla 51. Configuración de DLSw en Network Utility A

```
dlsa-ok DLSw config>ENABLE DLSW
Data Link Switching is now enabled
dlsa-ok DLSw config>ADD TCP
Enter the DLSw neighbor IP Address [0.0.0.0]? 172.16.220.253
Connectivity Setup Type (a/p) [a]? p
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
TCP Keepalive (E/D) [D]?
NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
TCP Neighbor has been changed
dlsa-ok DLSw config>OPEN-SAP
Enter Interface number [0]? 1
Enter the SAP in hex (range 0-FE), 'SNA', 'NB', or 'LNM'  [4]? sna
```

Ésta es la definición necesaria para el Network Utility A, como puede verse en la Tabla 51 de más arriba y en la Figura 26 en la página 195.

Cuando se configura el Network Utility B, es necesario configurar DLSw y el Servidor TN3270E bajo el indicador APPN.

Tabla 52. Configuración de DLSw en Network Utility B

```
dlsb-ok DLSw config>ENABLE DLSW
Data Link Switching is now enabled
dlsb-ok DLSw config>ADD TCP
Enter the DLSw neighbor IP Address [0.0.0.0]? 9.24.104.203
Record already exists, can be changed
Connectivity Setup Type (a/p) [a]? a
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
TCP Keepalive (E/D) [D]?
NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
TCP Neighbor has been changed
dlsb-ok DLSW config>OPEN-SAP
Enter Interface number [0]? 1
Enter SAP in hex (range 0-FE), 'SNA', 'NB', or 'LNM'  [4]? sna
dlsb-ok DLSw config>EXIT
```

Tabla 53. Carga de paquetes APPN y TN3270E si aún no se han cargado

```
2216 Config>load add package appn
appn package configured successfully
This change requires a reload.

2216 Config>load add package tn3270e
tn3270e package configured successfully
This change requires a reload.
```

Si los paquetes APPN y/o TN3270E no están cargados, deberá cargarlos del código de operación a la memoria para poder trabajar con ellos. Para cargar los paquetes APPN y TN3270E, consulte la Tabla 53 anterior.

Tabla 54. Adición de estación de enlace bajo APPN

```
dlsb-ok Config>PROTOCOL APPN
dlsb-ok APPN config>ADD/UPDATE LINK-STATION
APPN Station
Port name for the link station [ ]? dls65
Station name (Max 8 characters) [ ]? tnpub1
WARNING!! You are changing an existing record.
        Activate link automatically (Y)es (N)o  [Y]
        MAC address of adjacent node [40002216000A]?
        SAP address of adjacent node (04-EC) [4]?
        Solicit SSCP Session: (Y)es (N)o  [Y]?
                Local Node ID (5 hex digits)  [221B1]?
                Enable Host Initiated Dynamic LU Definition : (Y)es (N)o  [N]?
        Local SAP address (04-EC)  [4]?
        Does link support APPN function: (Y)es (N)o  [N]?  N
Edit TG Characteristics: (Y)es (N)o  [N}?
Write this record? [Y]?  y
The record has been written.
```

Tabla 55. Adición de puerto bajo APPN

```
dlsb-ok APPN config>ADD/UPDATE PORT
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P, [ ]? d
Port Name (Max 8 characters) [D65534]? dls65

WARNING!! You are changing an existing record.
Enable APPN on this port (Y)es (N)o? y
Port Definition
     Support multiple PU (Y)es (N)o [Y] y
All active port names will be of the form <port name sap>
     Service any node: (Y)es (N)o [N] n
     Maximum BTU size (768-4096) [2048]?
     Maximum number of link stations (1-65535) [65535]?
     Percent of link stations reserved for incoming calls (0-100) [0]?
     Percent of link stations reserved for outgoing calls (0-100) [0]?
     Local SAP address (04-EC) [4]?
     Locally administered MAC address (hex) [40002216B00B]?
Edit TG characteristics (Y)es (N)o [N]?
Write this record? [Y]? y
The record has been written.
```

Tabla 56. Definición de servidor TN3270E bajo APPN

```
dlsb-ok APPN config>TN3270E
lsadirect TN3270E config>SET
TN3270E Server Parameters
        Enable TN3270E Server (Y/N) [Y]?
        TN3270E Server IP Address [9.24.104.203]? 172.16.220.2
        Port Number [23]?
        Enable Client Address Mapping (Y/N) [N]?
        Default Pool name (Max 8 characters) [PUBLIC]?
        NetDisp Advisor Port Number [10008]?
        Keepalive type:
         0 = none,
         1 = Timing Mark,
         2 = NOP [0]?
        Automatic Logoff (Y/N) [N]?
        Enable IP Precedence (Y/N) [N]?
Write this record? [Y]?
dlsb-ok TN3270E config>ADD/UPDATE IMPLICIT-POOL
TN3270E Server Implicit Definitions
        Pool Name (Max 8 characters)  [<DEFLT>]?
        Station Name (Max 8 characters)  []? tnpub1
WARNING!! You are changing an existing record.
        LU Name Mask (Max 5 characters)  [@01LU]?
        LU Type  ( 1 - 3270 mod 2 display
                   2 - 3270 mod 3 display
                   3 - 3270 mod 4 display
                   4 - 3270 mod 5 display) [1]? 1
        Specify LU Address Ranges (s) (y/n)  [N]?
        Number of Implicit LUs in Pool(1-253)  [5]?
Write this record? [Y]? y
The record has been written.
```

Estas pantallas completan la definición del servidor TN3270E en el Network Utility B.

La definición correspondiente en VTAM se realiza como se muestra en la Tabla 57 siguiente:

Tabla 57. Definición de nodo principal conmutado de VTAM

```
SWB1              VBUILD     TYPE=SWNET
TNPUB1            PU    ADDR=02,                          X
                        IDBLK=077,                       X
                        IDNUM=221B1,                        X
                        PUTYPE=2,                           X
                        USSTAB=US327X,                      X
                        DLOGMOD=D4C32XX3
LUB2              LU    LOCADDR=02,LOGAPPL=RA03T
LUB3              LU    LOCADDR=03,LOGAPPL=RA03T
LUB4              LU    LOCADDR=04,LOGAPPL=RA03T
LUB5              LU    LOCADDR=05,LOGAPPL=RA03T
LUB6              LU    LOCADDR=06,LOGAPPL=RA03T
```

Cuando estas definiciones están en su sitio, la función queda lista para funcionar en los sistemas Network Utility.

Consulte la Figura 26 en la página 195 para ver una imagen general de la configuración.

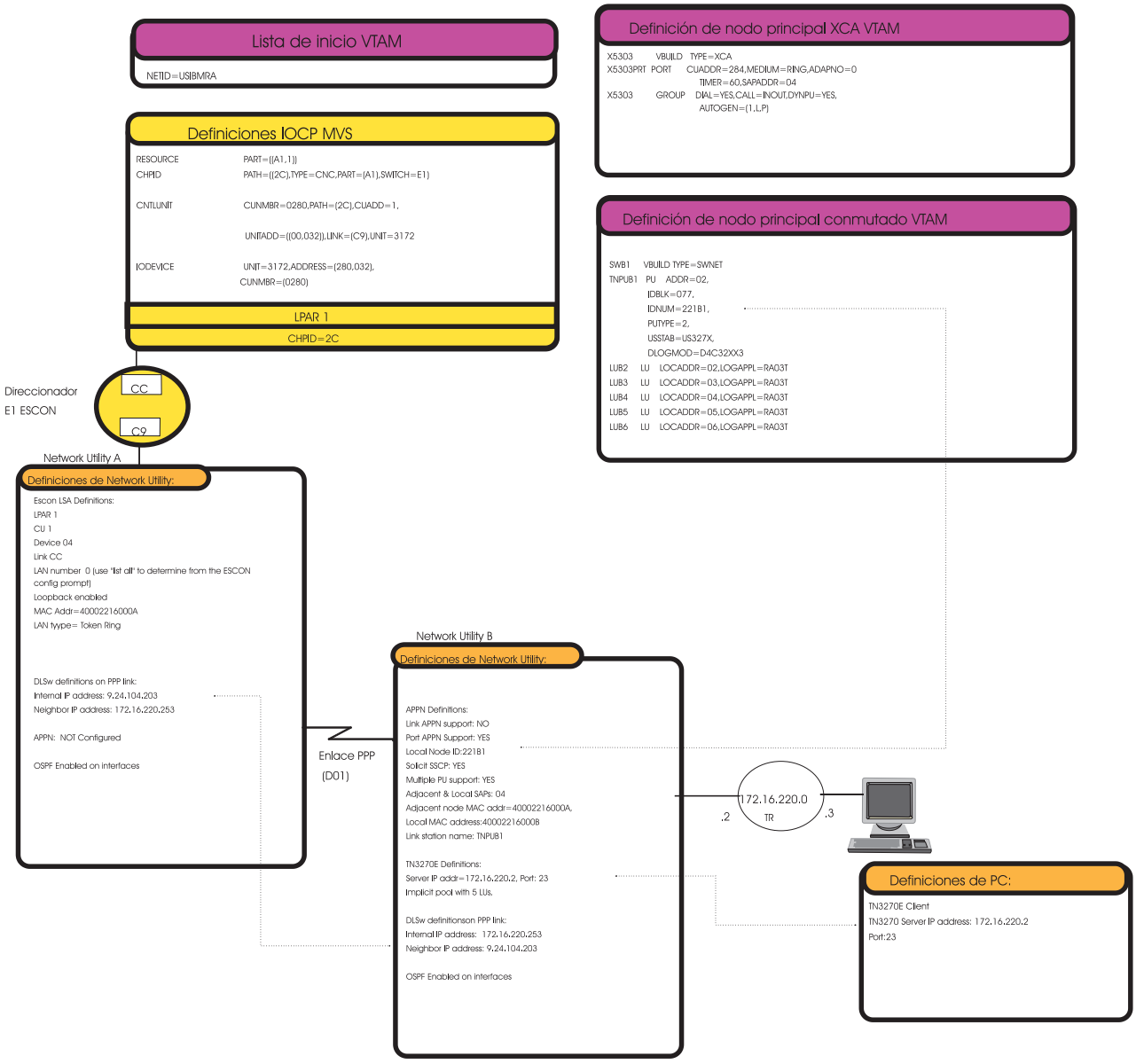


Figura 26. Relaciones entre parámetros de conexión de subárea TN3270E a través de DLSw

Supervisión de la configuración de subárea SNA de TN3270E a través de DLSw

Después de efectuar las definiciones anteriores, se deberá supervisar la configuración y su estado en el lado del Network Utility y el de VTAM.

Tabla 58. Visualización de pantalla de VTAM para las LU que hemos definido en Network Utility B

```
D NET,ID=SWB1,E
IST097I DISPLAY ACCEPTED
IST075I NAME=SWB1, TYPE=SW SNA MAJ NODE 774
IST486I STATUS=ACTIV, DESIRED STATE-ACTIV
IST1656I VTAMTOPO=REPORT, NODE REPORTED - YES
IST084I NETWORK RESOURCES:
IST089I TNPUB1     TYPE=PU_T2.1        , ACTIV
IST089I LUB2       TYPE=LOGICAL UNIT   , ACTIV
IST089I LUB3       TYPE=LOGICAL UNIT   , ACTIV
IST089I LUB4       TYPE=LOGICAL UNIT   , ACTIV
IST089I LUB5       TYPE=LOGICAL UNIT   , ACTIV
IST089I LUB6       TYPE=LOGICAL UNIT   , ACTIV
IST314I END
```

La configuración del Network Utility B puede supervisarse del modo siguiente.

Tabla 59. Pantalla de servidor TN3270E bajo 'T 6'

```
dlsb-ok *TALK 6
Gateway user configuration
dlsb-ok Config>PROTOCOL APPN
dlsb-ok APPN config>TN3270E
dlsb-ok TN3270E config>LIST ALL
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 172.16.220.2
TN3270E Port Number: 23
Default Pool Name: PUBLIC
NetDisp Advisor Port Number: 10008
Client IP Address Mapping: N
Keepalive type: NONE
Automatic Logoff: N    Timeout: 30
        Enable IP Precedence: N

Link Station: TNPUB1
        Local Node ID: 221B1
        Auto Activate: YES
        Host Initiated Dynamic LU Definition: NO
        Implicit Pool Information
        Pool Name: <DEFLT>
               Number of LUs: 5
               LU Mask: @01LU
        LU Name    NAU Addr     Class     Assoc LU Name  Assoc NAU addr
------------------------------------------------------------------------
        LUB2          2       Explicit Workstation

Client IP Address Mapping
-------------------------
Client IP Address              Address Mask      Resource Name
-------------------------------------------------------------

Multiple Port
-------------------------------------------------------------
PORT NUMBER   ENABLE TN3270E     RESOURCE NAME  DISABLE FILTERING
----------   --------------     -------------  -----------------
dlsb-ok TNE3270E config>
```

Tabla 60. Supervisión de las sesiones y conexiones DLSw

```
(control-p)
dlsb-ok *TALK 5

CGW Operator Console

dlsb-ok +PROTOCOL DLSW
Data Link Switching Console

dlsb-ok DLSw>LIST TCP SESSIONS
Group/Mcast@     IP Address  Conn State  CST Version ACTSes SesCreates
-------------------------------------------------------------------------
     1          9.24.104.203  ESTABLISHED  A  AIW V2RO    1        1

dlsb-ok DLSw>LIST DLSW SESSIONS ALL
Source     Destination   State   Flags   Dest IP Addr    Id
-----------------------------------------------------------
 1 APPN  04 40002216000a04 Connected     9.24.104.203     0
```

Tabla 61. Supervisión del enlace APPN

```
dlsb-ok APPN >LIST LINK_INFORMATION
   Name    Port Name  Intf   Adj CP Name   Type    HPR  State
=================================================================
TNPUB1     DLS65     65534 USIBMRA.RA03M   NN   INACTIVE ACT_LS 1
```

1. Esto significa que APPN está activo y en sesión.

Tabla 62. Pantalla de conexión LU-LU bajo TN3270E

```
dlsb-ok APPN >TN3270E
TN3270E GWCON
dlsb-ok TN3270E >LIST CONNECTIONS
Connection information for all the LUs
Local LU  Class  Assoc LU  Client Addr  Status  Prim LU  SEC LU  Idle Min
-------------------------------------------------------------------------
@01LU6     IW              9.24.106.44  LU-LU   RA03T03  LUB6       1
```

Tabla 63. Estado de servidor TN3270E

```
dlsb-ok TN3270E >LIST STATUS
TN3270E Server Status Summary

TN3270E IP Address: 172.16.220.2
NetDisp Advisor Port Number: 10008
   Keepalive type: None
   Automatic Logoff: N
   Client IP Address mapping: N
   Number of Connections                   :1
   Number of Available LUA LU's            :5
   Number of LUA LU's pending termination  :0
   Number of defined LU's                  :6
   Number of connections in SSCP-LU state  :0
   Number of connections in LU-LU state    :1
```

Conexión de subárea SNA LSA de TN3270E

Al transportar SNA, puede configurar el Servidor TN3270E utilizando enlaces de subárea SNA en el mismo 2216. Con esta configuración, necesitará las definiciones siguientes en el sistema principal:

- Una definición de nodo principal XCA

Tabla 64. Definición de nodo principal conmutado XCA de VTAM

```
X5303    VBUILD TYPE=XCA
X5303PRT PORT  ADAPNO=0,                                        *
               CUADDR=284,                                      *
               SAPADDR=4,                                       *
               MEDIUM=RING
X5303GRP GROUP DIAL=YES,CALL=INOUT,DYNPU=YES,                   *
               AUTOGEN=(1,L,P)
```

- Una definición de nodo principal conmutado

Tabla 65. Nodo principal conmutado de VTAM: SWB1

```
SWB1     VBUILD TYPE=SWNET
TNPUB1   PU    ADDR=02,              X
               IDBLK=077,            X
               IDNUM=221B1,          X
               PUTYPE=2,             X
               USSTAB=US327X,        X
               DLOGMOD=D4C32XX3
LUB2     LU    LOCADDR=02,LOGAPPL=RA03T
LUB3     LU    LOCADDR=03,LOGAPPL=RA03T
LUB4     LU    LOCADDR=04,LOGAPPL=RA03T
LUB5     LU    LOCADDR=05,LOGAPPL=RA03T
LUB6     LU    LOCADDR=06,LOGAPPL=RA03T
```

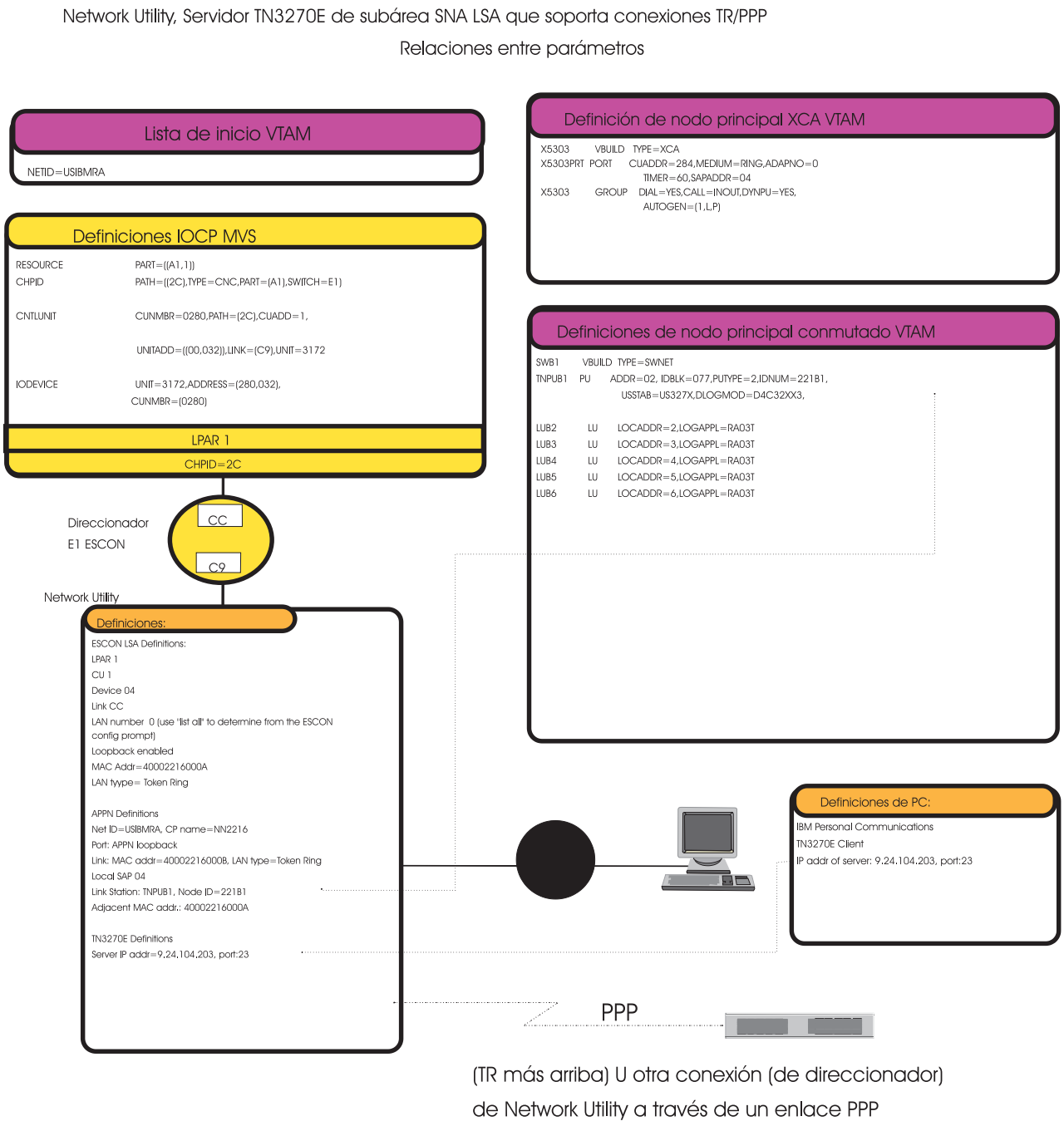


Figura 27. Subárea SNA de LSA para TN3270E que soporta conexiones TR/PPP

Las definiciones de nodo principal conmutado para las PU del Servidor TN3270E se han realizado como se indica a continuación.

Tabla 66. Lista de configuración Escon

```
lsadirect ESCON Config>LIst
Net:  4   Protocol: APPN Loopback   LAN type: Token-Ring/802.5   1
          APPN loopback MAC address: 40002216000B
Net:  3   Protocol: LSA    LAN type: Token Ring      LAN number:  0
          Maxdata: 2052
          Loopback is enabled.
          MAC address: 40002216000A
          Block Timer:   10 ms   ACK length:   10 bytes
```

1. Éste es el número de red de bucle de retorno APPN (4). Este número se utilizará posteriormente en la definición: **APPN config>add port** como puede verse en la Tabla 68 en la página 201.

Ahora podemos añadir las definiciones de puerto APPN, enlace APPN y servidor TN3270E como puede verse en las pantallas siguientes. Si no se han cargado los paquetes APPN y/o TN3270E, consulte la Tabla 53 en la página 193.

Tabla 67. Definición básica de nombre de CP de APPN

```
2216 Config>protocol appn
2216 APPN config>set node
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [  ]? usibmra
Control point name (Max 8 characters) [  ]? NN2216
Enable branch extender or border node
        (0=Neither, 1=Branch Extender, 2=Border Node) [0]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
2216 APPN config>ex
2216 Config>write
Config Save: Using bank A and config number 1
2216 Config>
2216 *reload y
```

Tabla 68. Adición de puerto y estación de enlace APPN

```
lsadirect APPN config>ADD/UPDATE PORT
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? t
Interface number(Default 0): [0]? 4          1
Port name (Max 8 characters) [T00004]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Support multiple PU (Y)es (N)o [N]?
        Service any node: (Y)es (N)o [Y]?
        High performance routing: (Y)es (N)o [N]?
        Maximum BTU size (768-17745) [2048]?
        Maximum number of link stations (1-65535) [65535]?
        Percent of link stations reserved for incoming calls (0-100) [0]?
        Percent of link stations reserved for outgoing calls (0-100) [0]?
        Local SAP address (04-EC) [4]?
        Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
lsadirect APPN config>
lsadirect APPN config>
lsadirect APPN config>
lsadirect APPN config>
lsadirect APPN config>ADD/UPDATE LINK-STATION
APPN Station
Port name for the link station [ ]? T00004
Station name (Max 8 characters) [ ]? tnpub1
        Activate link automatically (Y)es (N)o [Y]?
        MAC address of adjacent node [000000000000]? 40002216000A
        Solicit SSCP Session: (Y)es (N)o [N]? y
                Local Node ID (5 hex digits) [00000]? 221B1
                Enable Host Initiated Dynamic LU Definition : (Y)es (N)o [N]?
        Does link support APPN function: (Y)es (N)o [Y]? n
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
 The record has been written.
```

1. Éste es el número de interfaz de Bucle de retorno LSA que se muestra en la Tabla 66 en la página 200.

Tabla 69. Definición de TN3270E

```
lsadirect APPN config>TN3270E
lsadirect TN3270E config>SET
TN3270E Server Parameters
        Enable TN3270E Server (Y/N) [Y]?
        TN3270E Server IP Address [9.24.104.203]?
        Port Number [23]?
        Enable Client Address Mapping (Y/N) [N]?
        Default Pool name (Max 8 characters) [PUBLIC]?
        NetDisp Advisor Port Number [10008]?
        Keepalive type:
         0 = none,
         1 = Timing Mark,
         2 = NOP [0]?
        Automatic Logoff (Y/N) [N]?
        Enable IP Precedence (Y/N) [N]?
Write this record? [Y]?
The record has been written.
lsadirect TN3270E config>ADD/UPDATE IMPLICIT-POOL
TN3270E Server Implicit Definitions
        Pool name (Max 8 characters) []?
        Station name (Max 8 characters) []?
Invalid name please re-enter
        Station name (Max 8 characters) []? tnpub1
        LU Name Mask (Max 5 characters) [@01LU]?
        LU Type  ( 1 - 3270 mod 2 display
                   2 - 3270 mod 3 display
                   3 - 3270 mod 4 display
                   4 - 3270 mod 5 display) [1]?
        Specify LU Address Ranges(s) (y/n) [N]?
        Number of Implicit LUs in Pool(1-253) [1]? 5
Write this record? [Y]?
```

Supervisión de la configuración

Esta configuración puede supervisarse con mandatos similares como puede verse en el apartado “Supervisión de la configuración de subárea SNA de TN3270E a través de DLSw” en la página 195. Los resultados visualizados también serán similares.

Capítulo 14. Pasarela de canal

Visión general

El Network Utility proporciona conectividad de sistema principal a través de un canal ESCON o canal paralelo. Permite al Network Utility funcionar como una pasarela desde el sistema principal a otras redes.

Configuraciones soportadas

Existen tres interfaces de software de sistema principal que permiten habilitar el Network Utility como pasarela.

La primera interfaz es el soporte compatible con 8232, llamado LCS (LAN Channel Station) (Estación de canal LAN). Esta interfaz define diversos mandatos para la conexión a LAN directa y una estructura de creación y eliminación de bloques. Las tramas preparadas para la LAN se transmiten del sistema principal a los adaptadores de LAN virtuales y a la inversa. Esta interfaz la utiliza TCP/IP para VM, MVS y AIX/370.

La segunda interfaz es el soporte LSA (Link Services Architecture) (Arquitectura de servicios de enlace), a la que se accede en el sistema principal a través de VTAM.

El soporte LSA es una interfaz de control que permite a VTAM utilizar la parte LLC (Logical Link Control) (Control de enlace lógico) de la capa DLC (Data Link Control) (Control de enlace de datos) de la pila SNA. Se incluyen el acceso al transporte de datos LLC Tipo 1 (sin conexión) y LLC Tipo 2 (orientado a conexión). Esta interfaz la utiliza VTAM para la subárea SNA y el transporte de datos HPR y APPN ISR.

La tercera interfaz es el soporte de MPC+ (Multi-Path Channel) (Canal de múltiples vías), al que se accede en el sistema principal a través de VTAM. El soporte MPC+ es una capa de protocolo que permite tratar múltiples subcanales de lectura y grabación como un solo grupo de transmisión entre el sistema principal y los dispositivos conectados a canal. Esta interfaz la utiliza OS/390 para el transporte de datos HPDT UDP, TCP/IP y APPN HPR. Tenga en cuenta que el Canal no soporta grupos de subcanales MPC+ que se compartan entre más de una interfaz de canal física.

El Network Utility puede soportar 64 subcanales ESCON, en cualquier combinación de parejas de subcanales LCS, subcanales LSA y grupos MPC+. Esto permite un máximo de 32 adaptadores de LAN virtuales LCS, 32 adaptadores de LAN virtuales LSA o 32 grupos MPC+ (un grupo MPC+ debe incluir al menos un subcanal de lectura y un subcanal de grabación).

Los adaptadores de LAN virtuales LSA y LCS emulan una interfaz de Red en Anillo, FDDI o Ethernet para comunicaciones con el sistema principal. Esto no restringe el formato de la interfaz de red remota. Sólo está destinado a mantener las interfaces de sistema principal existentes del 3172 Interconnect Controller, para eliminar cambios de soporte de sistema principal.

Cada adaptador de LAN virtual o grupo MPC+ sólo puede soportar un tipo de conexión a sistema principal (LCS/LSA/MPC+). Los subcanales LSA y LCS pueden soportar múltiples adaptadores de LAN virtuales, por ejemplo, una interfaz de Red en Anillo y una interfaz Ethernet. No se ha observado ninguna ventaja en el hecho

de soportar múltiples adaptadores de LAN virtuales del mismo tipo en un solo subcanal o pareja, pero la configuración no lo impedirá.

Función de pasarela de LAN de sistema principal

La función de pasarela de LAN de sistema principal permite que las aplicaciones de sistema principal se comuniquen con estaciones de trabajo basadas en LAN. Las dos principales aplicaciones de sistema principal soportadas por la función de pasarela de LAN de sistema principal son TCP/IP y VTAM. Estas aplicaciones encapsulan tramas de LAN en palabras de control de canal (CCW) para el transporte a través del canal. Esto también se denomina ″bloque″, porque una CCW consta de un bloque de tramas de LAN enviadas como una sola unidad lógica. Entonces el receptor ″desempaqueta″ la CCW convirtiéndolo en tramas individuales.

Una gran parte de la función de pasarela de LAN del Network Utility se basa en el 3172 Interconnect Controller Program (ICP). Aunque existen diferencias en la función de pasarela del 3172 ICP y la función de Canal del Network Utility, las interfaces de hardware y software entre el sistema principal y el Canal de Network Utility son las mismas que las interfaces entre el sistema principal y el 3172 ICP (a excepción del soporte de direccionamiento de IP proporcionado en el Network Utility). Para conservar la interfaz de software, es necesario que el Network Utility cree el aspecto de un adaptador de LAN para que la aplicación de sistema principal siga creyendo que se está comunicando con una LAN real.

Conceptos sobre el canal ESCON

Subcanales

La interfaz de canal ESCON se divide en 256 direcciones lógicas (que, de forma incorrecta pero coherente, se denominan ″subcanales″ por razones históricas). Cada interfaz de aplicación de sistema principal utiliza uno o más subcanales para conectar la aplicación de sistema principal al Network Utility. Mediante la configuración, se asigna a cada subcanal un índice relativo exclusivo, que puede coincidir o no con su dirección lógica real. Varias aplicaciones de varios sistemas principales pueden compartir el canal ESCON, pero cada aplicación de sistema principal tendrá un uso dedicado de sus subcanales. (Esto no es estrictamente válido para MPC+, como se explica posteriormente, pero la sentencia se aplica a nivel de MPC+; los subcanales MPC+ no se pueden compartir con aplicaciones no MPC+). El Network Utility soporta hasta 64 subcanales a la vez.

Protocolos de canal

El Network Utility soporta tres protocolos de canal, correspondientes a las tres interfaces de software de sistema principal descritas más arriba. Cada protocolo utiliza los subcanales de forma diferente y un subcanal sólo puede soportar un protocolo cada vez. Los protocolos de canal soportados son LAN Channel Station (LCS), Link Services Architecture (LSA) y Multi-Path Channel (MPC+).

LAN Channel Station (LCS): LCS es un protocolo de canal soportado por aplicaciones TCP/IP en el sistema principal. Cada aplicación define una pareja consecutiva de subcanales, uno para que TCP/IP lea del canal y otro para que TCP/IP grabe en el canal. La interfaz LCS permite transportar tramas MAC de LAN a través del canal y proporcionar una interfaz de mandatos para activar, desactivar y consultar las interfaces de LAN. Cada trama MAC tiene una cabecera que identifica el adaptador de LAN virtual al que va destinada la trama.

Link Services Architecture (LSA): LSA es una interfaz para soportar tráfico SNA a través del canal. Cada vía LSA es un subcanal bidireccional entre la aplicación del sistema principal y el Network Utility. El software de sistema principal (VTAM) emite un mandato de lectura inmediatamente a continuación de cada mandato de grabación para recoger datos del canal. El Network Utility también emite un mandato de Atención cuando tiene algo que la aplicación de sistema principal debe leer. LSA tiene una interfaz de mandato que permite a VTAM abrir Puntos de acceso de servicio (Service Access Points - SAP) para comunicarse con estaciones de trabajo de sentido directo utilizando la interfaz de control de enlace lógico (LLC) IEEE 802.2. El mecanismo de creación/eliminación de bloques de canal para los subcanales LSA es el mismo que para las parejas de subcanales LCS.

Multi-Path Channel (MPC+): MPC+ es una interfaz de control de enlace de datos (DLC) para el canal. Cada vía MPC+ consta de uno o más subcanales de lectura y uno o más subcanales de grabación, unidos para formar un grupo de transmisión. Los grupos de transmisión MPC+ que abarcan más de un canal ESCON físico no se soportan en este release. VTAM y el Network Utility intercambian los XID para identificar el número y la dirección de los subcanales en la inicialización y entonces cada trama tiene una cabecera para indicar las aplicaciones de envío y recepción.

Bloques: La interfaz de canal de sistema principal empaqueta las tramas de control y datos en bloques de hasta 32 KB (36 KB para MPC+). El formato de los bloques de datos es diferente para aplicaciones de sistema principal MPC+ y no MPC+. Los bloques LSA y LCS constan de una o más tramas contiguas, cada una con una cabecera que identifica el dispositivo de destino por el tipo de LAN y el número de LAN. Los bloques MPC+ contienen una o más tramas ″no contiguas″, con los 4 primeros KB del bloque que contienen cabeceras PDU MPC+ y desplazamientos de datos de aplicación, que se almacenan en los últimos 32 KB del bloque. Los grupos MPC+ se identifican por un ″tipo de LAN″ y un ″número de LAN″ así como por la coherencia de implementación.

Un bloque de datos se transmite cuando está lleno o cuando caduca el temporizador de retardo de bloque (que determina cuánto tiempo espera el adaptador a que se llene el bloque antes de transmitirlo). El proceso de recepción de un bloque de datos y de reenvío de tramas individuales al controlador de dispositivo se denomina ″desempaquetado″.

Adaptadores de LAN virtuales: En primer lugar, unos datos históricos: el 3172 Interconnect Control Program (en el que se basa parcialmente el Network Utility) transfería tramas desde un canal de sistema principal a una o más LAN. En su configuración, cada subcanal estaba conectado a uno o más controladores de dispositivo de LAN. Los datos del sistema principal los recibía un desempaquetador, que distribuía las tramas a uno de los adaptadores de LAN basándose en el Tipo y el Número de LAN contenidos en la cabecera de la trama. Si una aplicación de sistema principal necesitaba acceder a múltiples adaptadores de LAN, el archivo de configuración contenía una entrada para cada adaptador de LAN.

En el Network Utility, en lugar de que cada subcanal esté conectado a uno o más adaptadores de LAN reales, todos los subcanales están conectados al Manejador de red base (Base Net Handler), que a su vez está conectado a uno o más manejadores de red virtuales. Cada manejador de red virtual soporta uno de los tres protocolos de canal (LSA/LCS/MPC+) y envía y recibe tramas con una de las aplicaciones de protocolo (LLC/IP/APPN), que envía los datos a otro manejador de red que representa una conexión de red. Pueden haber o no adaptadores de LAN reales conectados al Network Utility.

Para conservar las interfaces de sistema principal existentes, el Network Utility adopta el aspecto de múltiples adaptadores de LAN para las conexiones LSA y LCS. Basándose en los parámetros de configuración, los Manejadores de red virtuales se registran en los protocolos adecuados como adaptadores de Red en Anillo, Ethernet o FDDI. El Manejador de red base permite al sistema principal activar y desactivar este ″adaptador de LAN virtual″ del mismo modo que controla los adaptadores de LAN reales del 3172. Cada adaptador de LAN virtual tiene su propia dirección MAC, que permite al Network Utility aparecer al sistema principal como uno o más adaptadores de LAN en una red de área local real.

Se puede conectar cualquier subcanal individual (o pareja) a uno o más adaptadores de LAN virtuales. Esto es necesario para permitir que una aplicación de sistema principal individual se comunique con diferentes tipos de LAN (Red en Anillo, Ethernet, FDDI) a través del mismo subcanal. Las tramas destinadas a LAN se dirigen al destino correcto por el Tipo de LAN y Número de LAN de la cabecera de trama.

Sin embargo, a la inversa esto sólo es válido para las conexiones LSA. Un adaptador de LAN virtual LCS individual sólo se puede conectar a un subcanal. Esta restricción mejora el rendimiento al transmitir datos ya que permite al manejador de red virtual dirigir al subcanal correcto las tramas destinadas al sistema principal, sin forzar al manejador de red a examinar la dirección MAC o la dirección IP de cada trama destinada al sistema principal. Múltiples VTAM pueden compartir un solo manejador de red LSA individual si cada uno abre un SAP con un número exclusivo. Esto no puede realizarse en el caso del manejador de red LCS porque todo el tráfico TCP/IP utiliza el número de SAP multiprotocolo 'AA'x. Consulte la Figura 28.

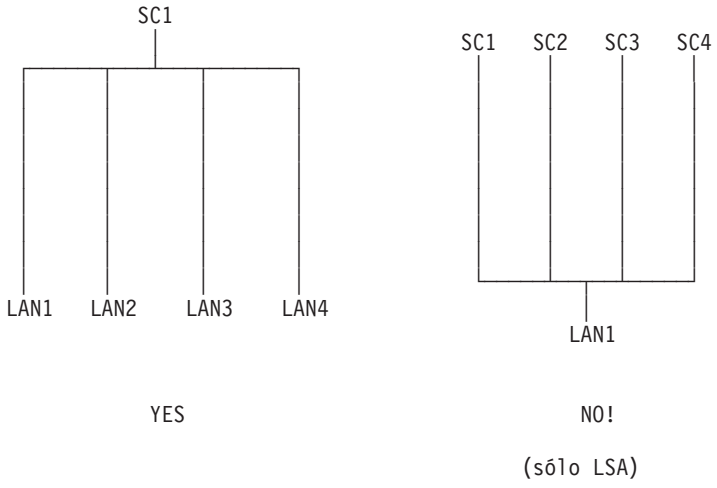


Figura 28. Configuración de LAN a subcanal

Grupos MPC+: MPC+ no utiliza los conceptos de adaptador de LAN virtual comunes a las interfaces LSA y LCS, porque MPC+ no soporta un aspecto de pasarela de LAN para el Network Utility. La interfaz equivalente para MPC+ es el grupo MPC+. Un grupo MPC+ es un conjunto de subcanales ESCON configurados para actuar como un solo conducto de datos entre el sistema principal y el Network Utility. Un grupo MPC+ consta al menos de un subcanal de ″lectura″ y al menos de un subcanal de ″grabación″. Se puede designar cualquier número de subcanales como de lectura o grabación y se pueden definir múltiples grupos MPC+, supeditándose a un máximo de 64 subcanales totales por Network Utility.

Se pueden enviar datos a través de cualquier subcanal activo de un grupo MPC+ o a través de todos los subcanales activos. El punto final MPC+ es responsable de mantener el orden de los datos en un grupo. El número de subcanales se fija cuando se define el grupo MPC+.

Los grupos MPC+ se identifican en el microcódigo que utiliza la misma designación de ″tipo de LAN″ y ″número de LAN″ que los adaptadores de LAN virtuales. A medida que el microcódigo desempaqueta las tramas, se proporciona a cada trama un ″tipo de LAN″ de MPC+ y un ″número de LAN″ que corresponde al grupo MPC+ asociado con el subcanal en el que se ha recibido. Esto permite al microcódigo y al manejador de red procesar tramas MPC+ de un modo coherente con las tramas LSA y LCS.

Bucle de retorno LLC: El Bucle de retorno LLC es una extensión del concepto de adaptador de LAN virtual para permitir conexiones VTAM con las funciones APPN y DLSw en el Network Utility. Para establecer una conexión SNA, la interfaz LSA crea una conexión LLC entre ella misma y el dispositivo remoto a través de la LAN utilizando tramas IEEE 802.2. Consulte la Figura 29.

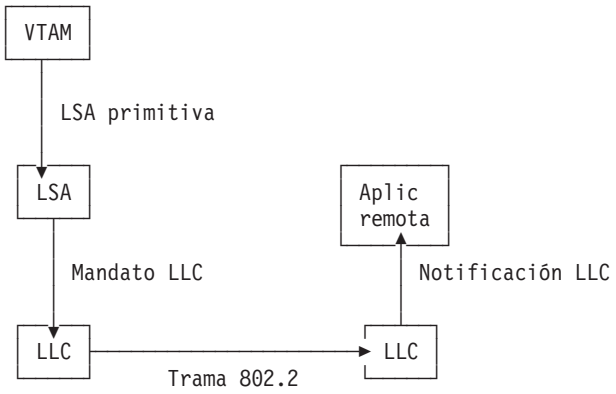


Figura 29. Conexión LLC normal

El Bucle de retorno LLC permite al Network Utility comunicarse directamente con otros usuarios LLC (APPN y DLSw) en el Network Utility. En lugar de convertir los mandatos LLC de LSA en tramas 802.2, éstos se convierten en notificaciones LLC y se envían al usuario LLC apropiado. Consulte la Figura 30 en la página 208.

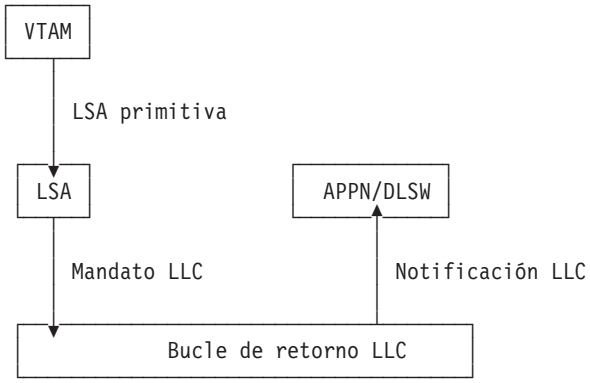


Figura 30. Conexión de bucle de retorno LLC

El Bucle de retorno LLC permite al Nodo de red APPN de Network Utility actuar como el nodo adyacente en VTAM. También permite a VTAM conectarse a aplicaciones y dispositivos remotos utilizando la Conmutación de enlace de datos sin necesitar cambios en el soporte LSA de VTAM, porque la conexión de bucle de retorno aparece igual que una conexión LLC normal en VTAM.

Configuraciones de ejemplo

Esta sección describe cuatro configuraciones de ejemplo que utilizan el Network Utility como una pasarela de canal en un sistema principal. Tres de los ejemplos muestran configuraciones de canal ESCON y una muestra un canal paralelo. Estas configuraciones son:

- Pasarela de canal ESCON (SNA e IP)
- Pasarela de canal paralelo (SNA e IP)
- Pasarela de canal ESCON (APPN e IP)
- Pasarela de canal ESCON - Alta disponibilidad

Todas estas configuraciones pueden crearse utilizando el modelo de Network Utility TN1 o TX1. No necesitará la función adicional proporcionada por el modelo TN1 a no ser que esté planeando configurar la función de servidor TN3270E en la misma máquina.

Pasarela de canal ESCON

Este escenario se muestra en la Figura 31 en la página 209. El Network Utility se configura para soportar tráfico SNA e IP en el sistema principal desde ubicaciones remotas y segmentos de LAN de la ubicación principal. El adaptador de canal ESCON se configura con una interfaz directa LSA para transportar el tráfico SNA y una interfaz LCS para efectuar el reenvío IP.

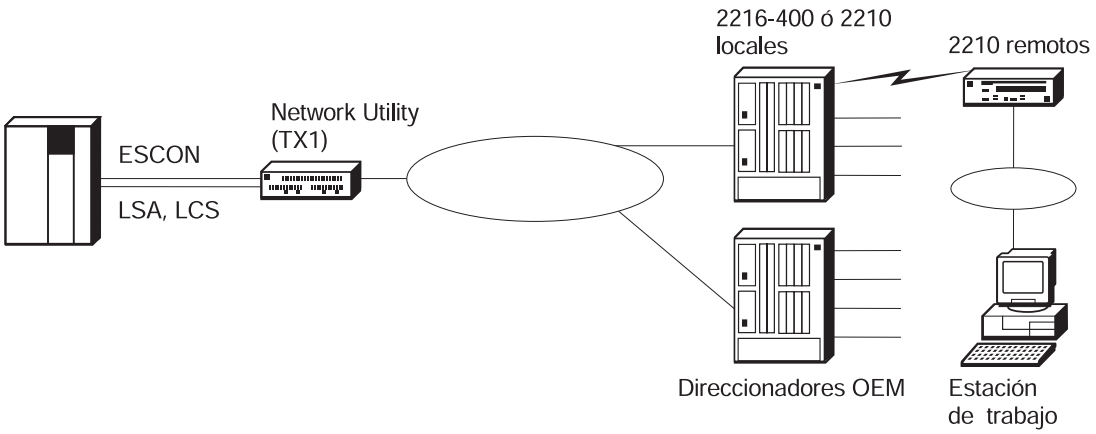


Figura 31. Pasarela de canal ESCON

Claves para la configuración

Las definiciones de subcanal para las interfaces LCS y LSA deben coincidir con los parámetros utilizados en el sistema principal para definir el Network Utility en el subsistema de canal de sistema principal. Los parámetros de subcanal claves a configurar en el Network Utility se muestran en la Tabla 70.

Tabla 70. Parámetros de configuración de subcanal de Network Utility

Mandatos	Descripción
device	Dirección de la unidad transmitida en la vía de canal para seleccionar el Network Utility. También se denomina número de subcanal en la arquitectura de E/S S/370. Es un número hexadecimal de dos dígitos en el rango de 00 a FF. Este valor se define en el IOCP (Input/Output Configuration Program) (Programa de configuración de entrada/salida) de sistema principal mediante la sentencia UNITADD, en la instrucción de macro CNTLUNIT para el dispositivo real. **Valores válidos:** X'00' a X'FF' **Valor por omisión:** Ninguno
cu	Dirección de Unidad de control definida en el sistema principal para el Network Utility. Este valor se define en el IOCP de sistema principal mediante la sentencia CUADD, en la instrucción de macro CNTLUNIT. **Valores válidos:** X'0' a X'F' **Valor por omisión:** X'0'

Tabla 70. Parámetros de configuración de subcanal de Network Utility (continuación)

Mandatos	Descripción
link	Este parámetro es significativo cuando se utiliza un IBM 9032 ESCON Director (ESCD) entre el Network Utility y el sistema principal. Cuando se utiliza un ESCD, la dirección de enlace es el número de puerto del Direccionador ESCON (ESCD) al que está conectado el *sistema principal*. Si hay dos ESCD en la vía, es el número de puerto del lado del sistema principal del ESCD definido con la conexión dinámica. Cuando no hay ningún ESCD en la vía de comunicaciones, este valor debe establecerse en X'01'. **Valores válidos:** X'01' a X'FE' **Valor por omisión:** X'01'
lpar	Número de partición lógica. Permite que varias particiones lógicas de sistema principal compartan una fibra ESCON. Este valor se define en el IOCP de sistema principal mediante la instrucción de macro RESOURCE. Si el sistema principal no está utilizando el EMIF (ESCON Multiple Image Facility) (Recurso de imagen múltiple ESCON), utilice el valor por omisión de 0 para el número de LPAR. **Valores válidos:** X'0' a X'F' **Valor por omisión:** X'0'

Parámetros LPAR y CU: Al definir una interfaz LSA, LCS o MPC+ en el Network Utility, necesita especificar valores correctos para los parámetros CU y LPAR.

Notas acerca del parámetro CU:

Es necesario establecer el valor para el parámetro CU si se tienen múltiples LPAR o múltiples imágenes de MVS u OS/390 que necesitan acceder al Network Utility. Si es así, necesitará crear una definición de interfaz (LSA, LCS o MPC+) para cada LPAR y cada una utilizará un valor diferente para el parámetro CU.

Además, el valor del parámetro CU debe coincidir con el del parámetro CUADD en la macro CNTLUNIT de la definición de IOCP.

Anteriormente, siempre que se configuraba una nueva (partición) LPAR, se tenía que configurar con ella un número de CU exclusivo. Con el PTF01, el número de CU y LPAR son independientes para ESCON. No se necesita un número de CU exclusivo para cada número de LPAR. Esto aumenta mucho la flexibilidad de configuración de usuario y simplifica la operación en grandes sistemas principales.

Notas acerca del parámetro LPAR:

La primera cuestión es determinar si el sistema principal está particionado en múltiples particiones lógicas (LPAR). Si no lo está, el parámetro LPAR será cero.

Si lo está, necesitará una macro RESOURCE en las definiciones del IOCP (Input/Output Configuration Program) de sistema principal que especifican cada partición por nombre y asignan un valor numérico a cada una. Este valor numérico se utiliza al configurar el Network Utility para el parámetro LPAR.

La segunda cuestión es determinar si los identificadores de vía de canal (CHPID) se comparten entre una o más LPAR[19].

Si no está utilizando canales compartidos (o si no tiene EMIF), el valor para el parámetro LPAR será 0.

El número máximo de LPAR por adaptador ESCON ha aumentado de 32 a 64. Con el fin de soportar esto, hemos aumentado el número máximo de subcanales por adaptador de 32 a 64 y aumentado el número máximo de redes virtuales por adaptador de 16 a 32. Esto es una ventaja para los usuarios de protocolo LSA que necesitan configurar más de 32 particiones LPAR.

La Figura 32 en la página 212 muestra un ejemplo donde el sistema principal está particionado pero las vías de canal no están compartidas entre las LPAR.

19. Necesita EMIF para compartir canales entre las LPAR.

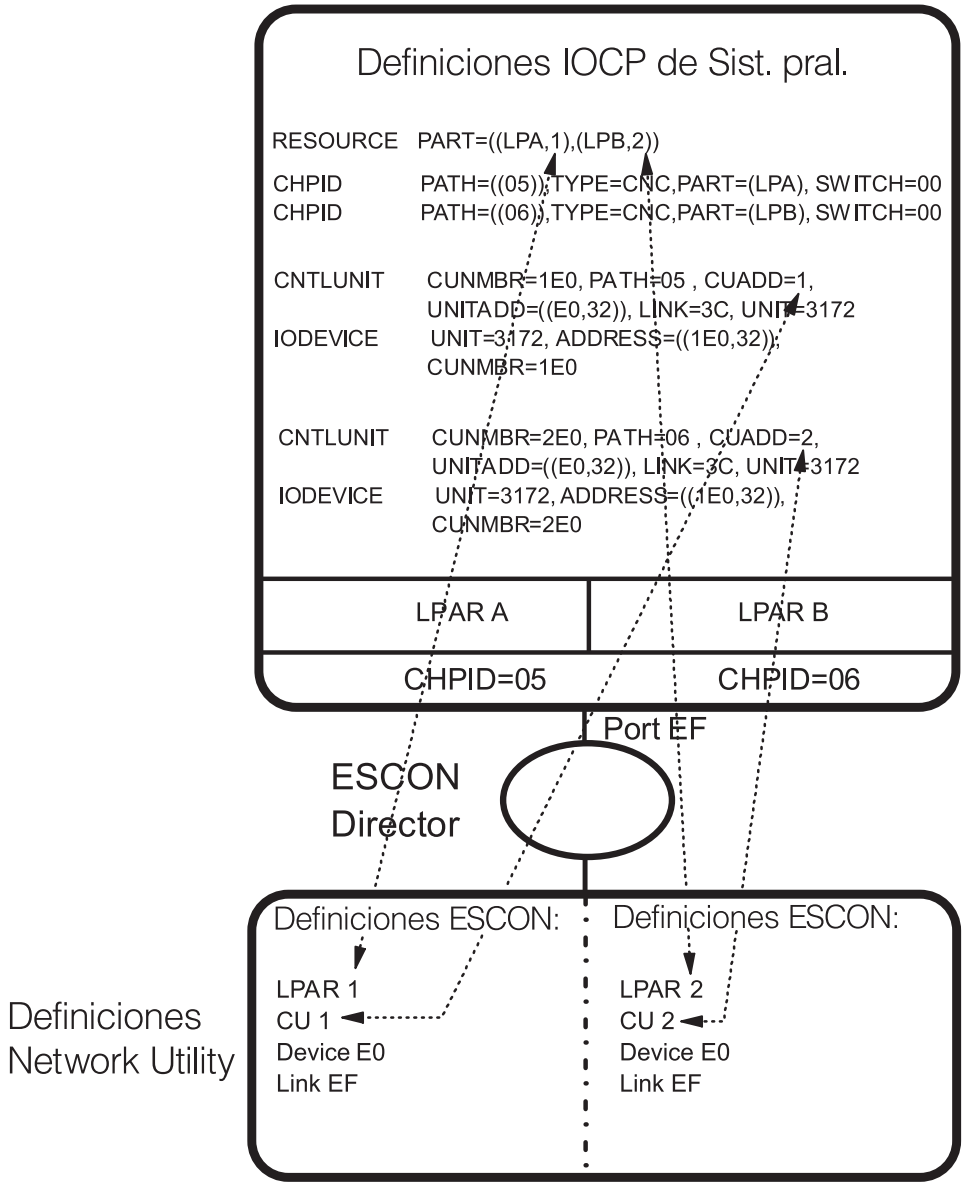


Figura 32. Relaciones entre parámetros de sistema principal y de Network Utility (CHPID no compartidos)

Si está utilizando EMIF en el sistema principal, múltiples LPAR pueden compartir el mismo CHPID en el Network Utility. En este caso, necesitará no obstante dos interfaces definidas en el Network Utility y cada una tendrá un valor diferente especificado para el parámetro CU. Los otros parámetros pueden utilizar los mismos valores. La Figura 33 en la página 213 muestra un ejemplo donde el sistema principal está particionado y se utiliza EMIF para permitir que ambas particiones utilicen el mismo CHPID.

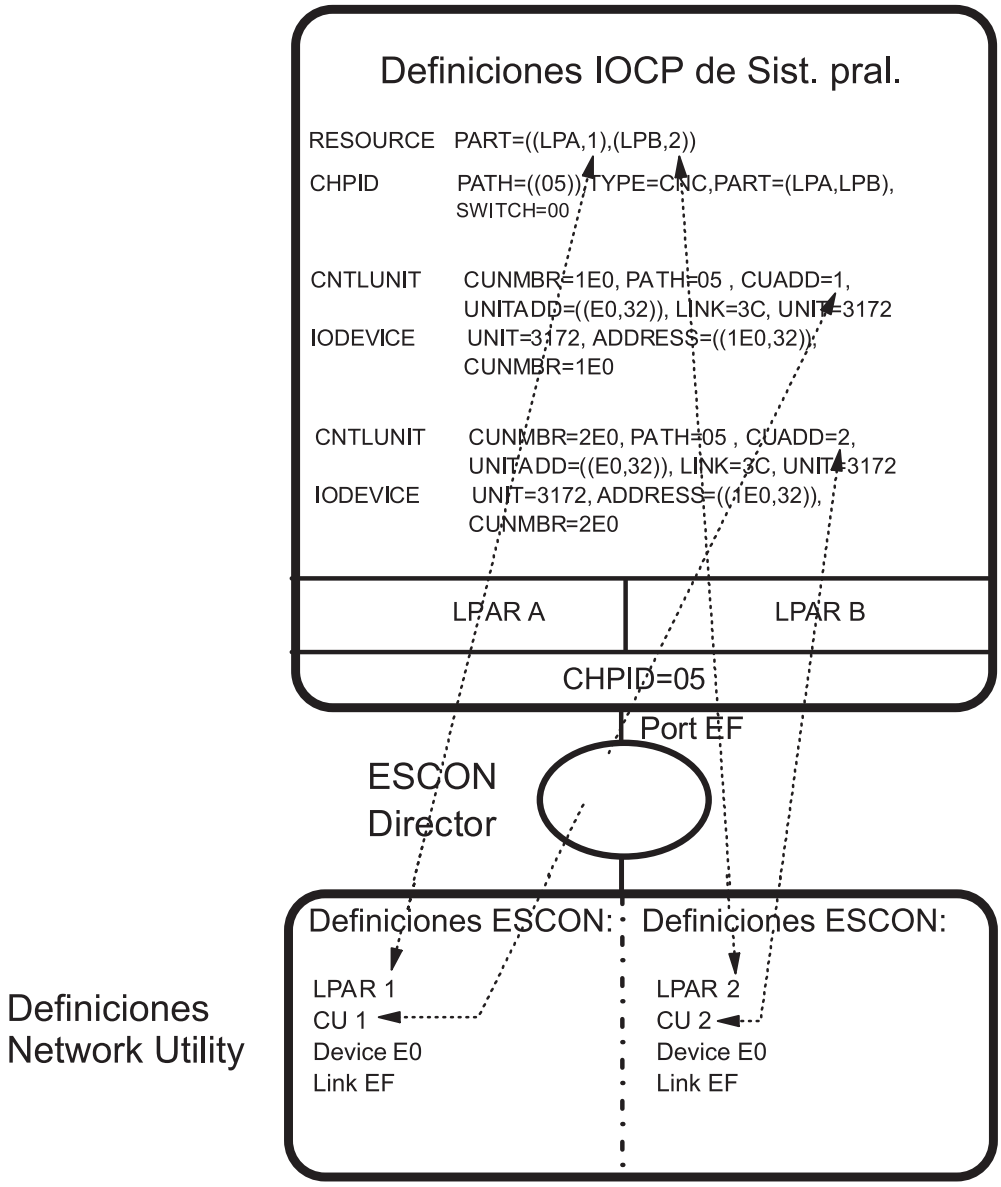


Figura 33. Relaciones entre parámetros de sistema principal y de Network Utility (Canales compartidos)

La interfaz directa LSA: La Figura 34 en la página 214 muestra cómo se correlacionan los parámetros de configuración para el Network Utility con los parámetros de sistema principal para una definición de interfaz LSA.

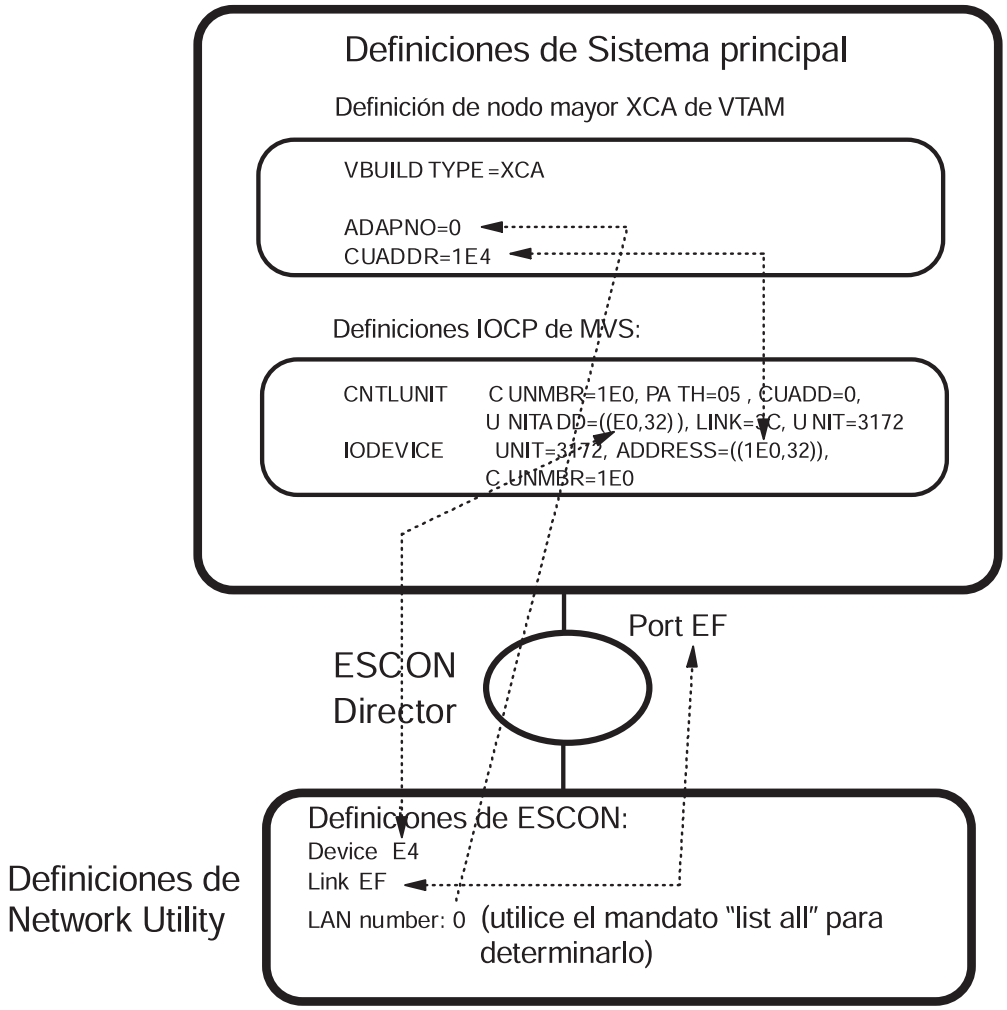


Figura 34. Relaciones entre los parámetros de sistema principal y de Network Utility - LSA

Notas:

1. LSA utiliza un solo subcanal bidireccional entre el sistema principal y el Network Utility. VTAM emite un mandato de lectura inmediatamente a continuación de cada mandato de grabación para recuperar datos del canal.
2. La dirección de dispositivo especificada en la definición de interfaz LSA de Network Utility debe estar dentro del rango especificado en el parámetro UNITADD de la macro CNTLUNIT desde el IOCP. Por ejemplo, el parámetro UNITADD de la Figura 34 muestra que 32 direcciones de dispositivo (decimales) que empiezan en E0 (hex) se están reservando para la definición de Network Utility. Se ha especificado una dirección de dispositivo E4 para la interfaz LSA de Network Utility. Dado que E4 está en el rango entre E0 y FF hex, esto es correcto siempre que ningún otro dispositivo (o interfaz en este Network Utility) intente utilizar dicho subcanal.
3. El valor especificado en el parámetro CUADDR de la definición de nodo principal XCA de VTAM debe estar en el rango especificado en el parámetro ADDRESS de la macro IODEVICE desde el IOCP. Por ejemplo, el parámetro CUADDR de la definición de nodo principal XCA de la Figura 34 es 1E4 hex, que está en el rango de 1E0 a 1FF que especifica el parámetro ADDRESS de la sentencia IODEVICE.

4. Los valores especificados para el parámetro ADDRESS en la macro IODEVICE y el parámetro UNITADD en la macro CNTLUNIT están relacionados ***por convenio solamente***. En este ejemplo, el valor para el parámetro ADDRESS se ha determinado a partir del valor para el parámetro UNITADD añadiendo delante del valor de UNITADD un ***identificador de canal lógico*** (en este caso 1). Esto sucederá con frecuencia. Sin embargo, al definir la dirección de dispositivo en la definición LSA de Network Utility, utilice el parámetro UNITADD y no el parámetro ADDRESS para determinar el rango válido de valores.
5. Al definir una interfaz directa LSA en el Network Utility, se asocia la interfaz con una de las interfaces de LAN en el Network Utility. En efecto, esto pone la interfaz directa LSA en este mismo segmento de LAN. Cada trama con una dirección de destino de la dirección MAC del adaptador de Network Utility en este segmento de LAN se reenvía automáticamente a través del canal al sistema principal.

Consulte el “Capítulo 18. Definiciones de sistema principal de ejemplo” en la página 259 para obtener una explicación más detallada y más ejemplos de definiciones de sistema principal para este tipo de interfaz.

Para obtener una visión completa de los parámetros de configuración necesarios para este escenario, consulte la Tabla 19 en la página 158.

La interfaz LCS: Al definir una interfaz LCS se crea una LAN virtual en el Network Utility. Hay dos estaciones IP en esta LAN: el Network Utility y el sistema principal. Esta LAN debe ser una subred IP exclusiva en la red. También se necesita una dirección MAC para la interfaz LCS. Después de crear la interfaz LCS, no se olvide de asignar la dirección IP a esta interfaz.

El Network Utility proporciona tres procedimientos para operar la interfaz LCS:

1. Direccionamiento LCS

   El soporte LCS descrito más arriba y documentado en las configuraciones de ejemplo es el soporte LCS 2216 inicial suministrado en MAS V1R1.1. Este tipo de soporte LCS pasa el tráfico IP del sistema principal a la función de direccionamiento dentro del Network Utility. Si está sustituyendo un 3172 por un Network Utility configurado con este tipo de soporte LCS, necesitará configurar una subred IP adicional para el segmento de LAN virtual dentro del Network Utility.
2. Puentes LCS

   MAS V3.2 introduce los ″Puentes LCS″ (oficialmente llamado ″Paso a través TCP/IP″), para permitir la sustitución de 3172 sin cambios en la topología IP de la red. En esta modalidad, el Network Utility simplemente establece puentes de tráfico IP entre un puerto de puente LCS y otros puertos de puente configurados. No se efectúa ningún direccionamiento IP dado que las tramas se transfieren de un puerto a otro. Para habilitar esta modalidad, no se especifica una dirección IP para la interfaz LCS, pero sí se define una dirección MAC y se habilitan los puentes en ella. Consulte la publicación de MAS V3.2 *Guía del usuario de software* para obtener más información sobre cómo configurar esta función.
3. Emulación LCS 3172

   El PTF01 de MAS V3.2 deja disponible un tercer tipo de soporte LCS, que se puede llamar ″Emulación 3172″. Esta modalidad LCS refleja exactamente el comportamiento del 3172 al correlacionar una interfaz LCS virtual con una sola interfaz de LAN. A diferencia de los Puentes LCS, donde existen múltiples vías entre las diversas interfaces habilitadas para puente, el Paso a través LCS

define vías fijas independientes entre subcanales específicos y adaptadores de LAN específicos. El tráfico de una vía no puede verse en ningún otro lugar. Para habilitar esta modalidad, se habilita la emulación 3172 para esta modalidad, no se especifica ninguna dirección IP y se hace referencia a un adaptador de LAN específico en lugar de definir una dirección MAC LCS utilizando el parámetro ″NET″ al definir la LCS. Al realizar esta acción, se elige el tipo de LAN y la dirección MAC de la LAN a la que se está conectando.

Esta función de pasarela de canal permite al Network Utility funcionar como sustituto de un 3172 de paso en la redes TCP/IP. Las tramas recibidas de un sistema principal TCP/IP se pasan directamente a un adaptador de LAN de sentido directo, sin utilizar las funciones de puentes y de direccionador IP del Network Utility. Las tramas IP y ARP recibidas por un adaptador de LAN asociado con la función de Paso a través LCS se pasan directamente a LCS para entregarlas al sistema principal TCP/IP. El Network Utility sustituye la función LCS 3172 sin necesitar cambios en la topología de red IP o sin añadir saltos de puente adicionales, como lo hacían los métodos LCS anteriores.

A partir del PTF01 de la V3.2, puede añadir dinámicamente una nueva interfaz virtual ESCON (LSA, MPC + o LCS) utilizando una LPAR que no esté configurada actualmente. Anteriormente, una red añadida dinámicamente sólo se podía configurar con subcanales en una LPAR ya configurada. Para añadir una interfaz con una nueva vía lógica de LPAR era necesario inhabilitar la interfaz de canal física entera. Para utilizar el nuevo soporte, configure interfaces de repuesto, añada la nueva interfaz virtual utilizando “talk 6” y active la nueva red utilizando “talk 5”.

Pasarela de canal paralelo

Este escenario se muestra en la Figura 35. Es idéntico a la pasarela de canal ESCON excepto en que la conexión al sistema principal es a través de un Adaptador de bus e identificador S/370 (Canal paralelo) en lugar de un canal ESCON. Como la pasarela ESCON, esta configuración utiliza una conexión LSA directa para el tráfico SNA y una interfaz LCS para el tráfico IP.

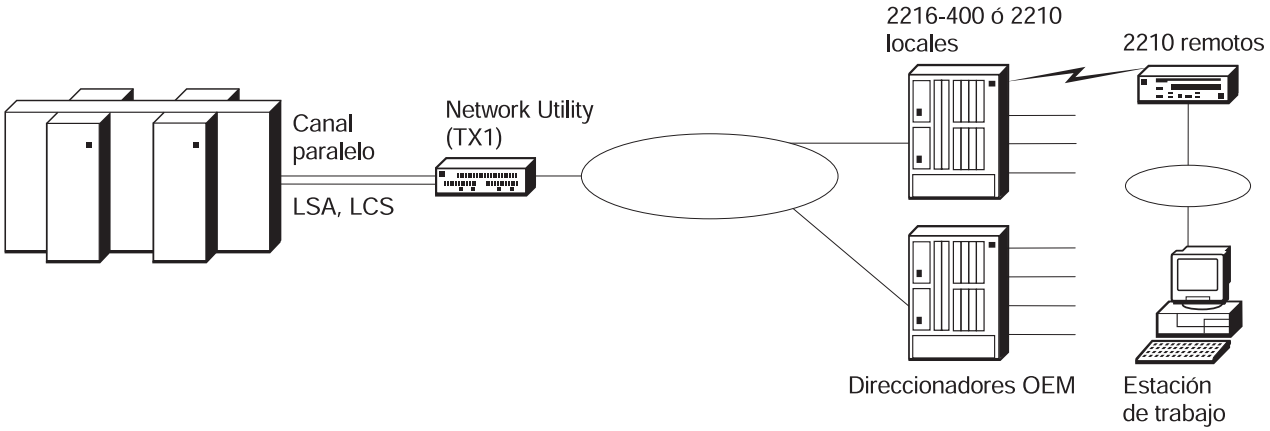


Figura 35. Pasarela de canal paralelo

Claves para la configuración

La configuración para este escenario es muy similar a la configuración para la pasarela ESCON (consulte el apartado “Pasarela de canal ESCON” en la página 208). La configuración de las interfaces LSA y LCS necesita menos parámetros porque no se necesitan valores de LPAR, dirección de enlace (Link

Address) o unidad de control (Control Unit) para una conexión de bus e identificador. La dirección de dispositivo sigue siendo necesaria para identificar el Network Utility en el canal.

Para obtener una visión completa de los parámetros de configuración necesarios para este escenario, consulte la Figura 8 en la página 142. Asimismo, el "Capítulo 18. Definiciones de sistema principal de ejemplo" en la página 259 contiene un ejemplo de la definición IOCP de sistema principal para un Network Utility con un Adaptador de canal paralelo.

Pasarela de canal (APPN e IP a través MPC+)

Este escenario se muestra en la Figura 36. Aquí, se utiliza un Grupo de canales de múltiples vías (MPC+) para transportar el tráfico IP y APPN entre el Network Utility y el sistema principal. MPC+ utiliza un grupo de subcanales ESCON para maximizar el rendimiento de la transferencia de datos.

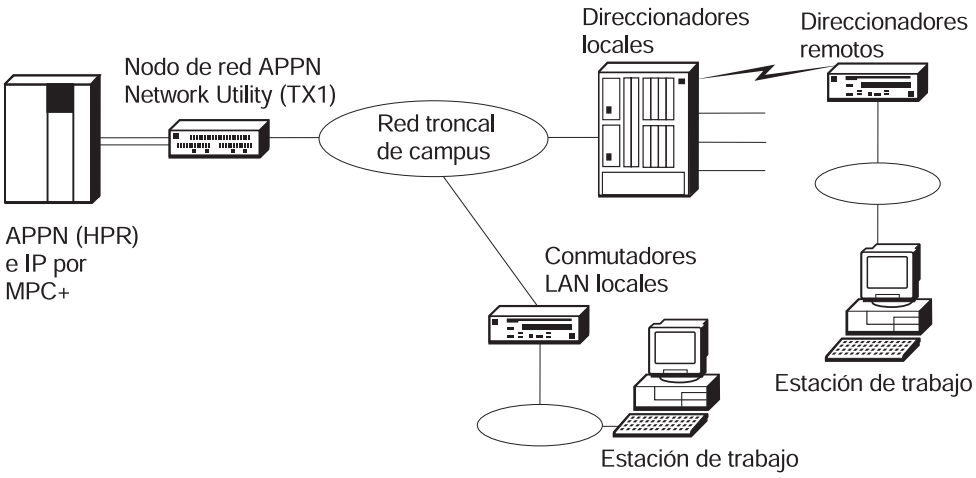


Figura 36. Pasarela de canal (APPN e IP)

El tráfico APPN que viene a través del Network Utility está compuesto por varios tipos diferentes desde los direccionadores de las bifurcaciones remotas:

- El tráfico TN3270 procedente de los servidores TN3270E de la bifurcaciones que se configuran con una conexión APPN al sistema principal. (Consulte el apartado "Servidor TN3270E distribuido" en la página 147 para ver un ejemplo de este tipo de configuración).
- El tráfico DLUR procedente de los direccionadores de las bifurcaciones que proporcionan soporte para los dispositivos PU 2.0 (dependientes).
- El tráfico de sistema principal a sistema principal APPN procedentes de procesadores distribuidos (por ejemplo procesadores AS/400) que se comunican con el sistema principal en la ubicación central.

En cada uno de los casos anteriores, el Network Utility proporciona sólo reenvío ANR del tráfico APPN. [20] Sin embargo, además de proporcionar la función ANR, el Network Utility en este escenario podría también configurarse para soporte de servidor TN3270E y soporte DLUR. El soporte DLUR podría proporcionar dispositivos PU 2.0 en el campus local con acceso al sistema principal y el servidor

20. Las sesiones RTP son entre los nodos APPN de cada extremo de las conversaciones.

TN3270E podría proporcionar soporte TN3270 para las estaciones de trabajo y las impresoras del campus local o para las bifurcaciones que no tuvieran un servidor TN3270E distribuido.

Claves para la configuración

Tenga en cuenta lo siguiente al configurar el Network Utility para este escenario:

- Puede definir un grupo MPC+ independiente para el tráfico APPN y TCP/IP o puede definir un solo grupo compartido entre APPN y TCP/IP.
- Un grupo MPC+ puede tener hasta 64 subcanales. Debe tener definidos un subcanal de lectura y un subcanal de grabación como mínimo. Desde la línea de mandatos de talk (desde el indicador `ESCON Add Virtual`), se utiliza el mandato **sub addr** para añadir un subcanal de lectura mientras que se utiliza el mandato **sub addw** para añadir un subcanal de grabación.
- TCP/IP se configura en una interfaz MPC+ del mismo modo que se configura para otras interfaces. Específicamente, la configuración de una dirección IP para el manejador de red virtual MPC+ habilita TCP/IP a través de la interfaz MPC+.
- APPN se configura a través de la conexión MPC+ del mismo modo que se configura para otras interfaces. Cuando utilice el mandato **add port**, especifique un tipo de puerto **M** para MPC+.
- Para ejecutar tráfico APPN / HPR a través de un Canal MPC+, es necesario crear dos definiciones de VTAM:
  - Un elemento de Lista de recursos de transporte (TRL) que defina el control de línea, los subcanales, el número de almacenamientos intermedios y los programas de canal a utilizar
  - Un nodo principal SNA local con una definición de PU local
- Al igual que las definiciones LSA y LCS, los parámetros de subcanal deben coincidir con los parámetros utilizados en las definiciones de sistema principal al definir el Network Utility en el subsistema de canal de sistema principal. Consulte la Tabla 70 en la página 209 para obtener una descripción de los parámetros de subcanal y la Figura 37 en la página 219 para ver un diagrama de cómo se correlacionan estos parámetros con los parámetros de sistema principal para una definición de MPC+.

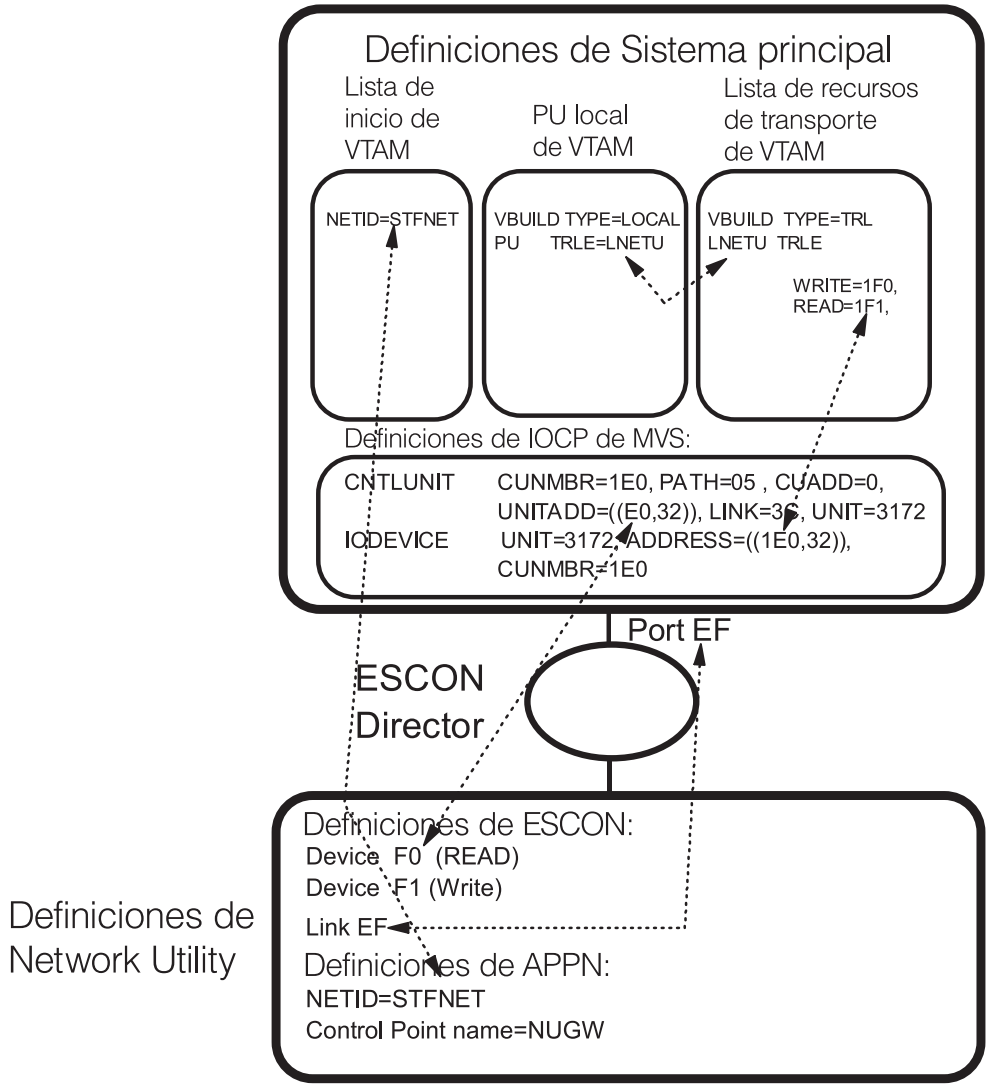


Figura 37. Relaciones entre parámetros de sistema principal y Network Utility - MPC+

Notas:

1. Las direcciones de dispositivo especificadas en la definición de interfaz MPC+ de Network Utility deben estar en el rango especificado en el parámetro UNITADD de la macro CNTLUNIT del IOCP. Por ejemplo, el parámetro UNITADD de la Figura 37 muestra que se están reservando 32 direcciones de dispositivo (decimales) que empiezan en E0 (hex) para la definición de Network Utility. Las direcciones de dispositivo F0 y F1 se han especificado para la interfaz MPC+ de Network Utility. Dado que F0 y F1 están en el rango de E0 a FF hex, esto es correcto a condición de que ningún otro dispositivo (o interfaz en este Network Utility) intente utilizar estos mismos subcanales.
2. Los valores especificados en la definición de nodo principal TRL de VTAM deben estar dentro del rango especificado en el parámetro ADDRESS de la macro IODEVICE del IOCP. Por ejemplo, la definición de nodo principal TRL de la Figura 37 especifica 1F0 y 1F1, que están en el rango 1E0 a 1FF que especifica el parámetro ADDRESS de la sentencia IODEVICE.
3. Los valores especificados para el parámetro ADDRESS en la macro IODEVICE y el parámetro UNITADD en la macro CNTLUNIT están relacionados ***por convenio solamente***. En este ejemplo, el valor para el parámetro ADDRESS

se ha determinado a partir del valor para el parámetro UNITADD añadiendo delante del valor de UNITADD un ***identificador de canal lógico*** (en este caso 1). Esto sucederá con frecuencia. Sin embargo, al definir direcciones de dispositivo en la definición MPC+ de Network Utility, utilice el parámetro UNITADD y no el parámetro ADDRESS para determinar el rango válido de valores.

Consulte el “Capítulo 18. Definiciones de sistema principal de ejemplo” en la página 259 para ver ejemplos de estas definiciones de sistema principal.

Protocolos de direccionamiento dinámicos en la interfaz ESCON

En un entorno de un solo sistema principal no es necesario ejecutar un protocolo de direccionamiento (por ejemplo RIP) en la subred ESCON. En este caso, es suficiente añadir el Network Utility como la pasarela por omisión en el perfil TCP/IP de sistema principal.

Sin embargo, si hay múltiples sistemas principales o múltiples pasarelas Network Utility, deberá considerar la posibilidad de ejecutar RIP en la interfaz ESCON. La ejecución de un protocolo de direccionamiento dinámico en este entorno le permite direccionar eludiendo anomalías de red si existe una vía alternativa.

El Network Utility soporta RIP V1 y V2. RIP V2 ofrece subredes de longitud variable y otras características avanzadas que no ofrece RIP V1 y es, por consiguiente, la opción recomendada.

Importación de la subred ESCON a OSPF

Si está ejecutando OSPF en la red, deberá importar la subred ESCON a OSPF (a no ser que el TCP/IP del sistema principal soporte OSPF). Si no se realiza esta acción, sólo las estaciones de trabajo conectadas directamente a una interfaz en el Network Utility podrán acceder al sistema principal TCP/IP en la interfaz ESCON.

Para obtener una visión completa de los parámetros de configuración necesarios para este escenario, consulte la Figura 13 en la página 146.

Pasarela de canal ESCON - Alta disponibilidad

Este escenario se muestra en la Figura 38 en la página 221. Utiliza Network Utilities redundantes, cada uno con una conexión de canal ESCON al sistema principal. Asimismo, las redes troncales de campus se han duplicado y cada Network Utility se conecta a una red troncal diferente.

Con esta configuración, aún puede acceder al sistema principal aunque tenga una anomalía en una de las redes troncales o un Network Utility del campus. El tráfico que viene de los 2216 seguirá teniendo una vía válida al sistema principal a través una red troncal y el Network Utility del campus. Esto es válido para el tráfico IP y SNA.

El Direccionador ESCON (ESCD) es importante en esta configuración, especialmente en entornos Sysplex paralelos, porque le permite encajar totalmente las conexiones entre las pasarelas y las LPAR en el sysplex. Esto proporciona el más alto nivel de tolerancia a anomalías para el acceso al sistema principal.

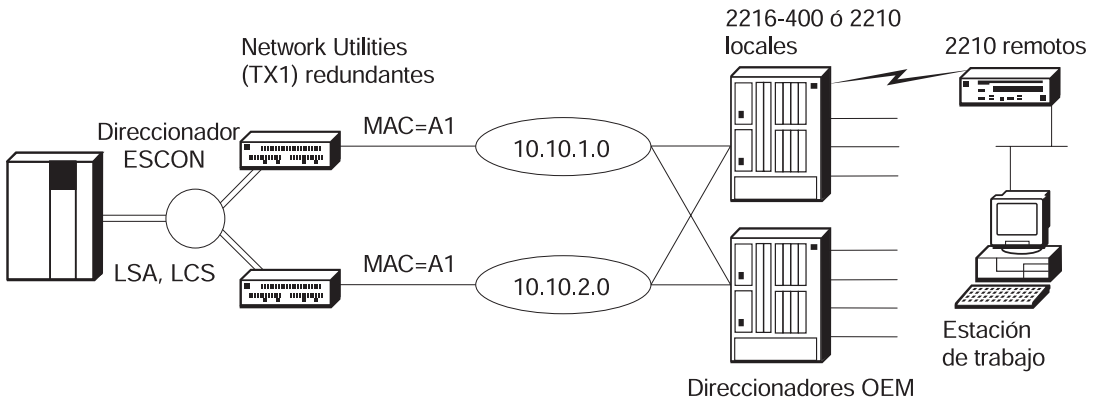


Figura 38. Pasarela de canal ESCON - Alta disponibilidad

Claves para la configuración

La configuración para este escenario es muy parecida a la del escenario del apartado “Pasarela de canal ESCON” en la página 208. Cada Network Utility se configura como una Pasarela de canal LAN con una interfaz LSA y LCS independiente definida en cada uno. Consulte la Tabla 19 en la página 158 para conocer los parámetros necesarios para configurar un Network Utility como una pasarela de Canal LAN.

Puesto que cada Network Utility está en una Red en Anillo diferente, se puede utilizar la misma dirección MAC para la interfaz de Red en Anillo de cada uno. Sin embargo, la dirección IP utilizada para cada interfaz debe ser diferente porque cada interfaz está en una subred diferente.

Nota: Mientras que este ejemplo muestra el uso de conexiones LSA y LCS en el canal ESCON, el uso de MPC+ es igualmente efectivo en el entorno de alta disponibilidad.

Gestión de la función de pasarela

Los ejemplos de configuración de este capítulo y del apartado “Pasarela de canal de LAN DLSw” en la página 241 muestran usos diferentes de los DLC de canal:

- Una interfaz LSA directa se correlaciona con una interfaz de LAN sin compromiso de DLSw o APPN en el reenvío de tramas.
- Una interfaz virtual MPC+ o de direccionamiento LCS aparece en el código de direccionamiento IP como otra interfaz e IP efectúa su función normal de direccionamiento para reenviar tramas a otras interfaces.

  Una interfaz de Puentes LCS aparece en el código de puente como otro puerto de puente de LAN y los puentes efectúan su función normal para reenviar tramas a otros puertos.
- La interfaz virtual LSA de bucle de retorno aparece como un enlace en DLSw o APPN.
- Una interfaz virtual MPC+ puede aparecer como un enlace en APPN.

Para gestionar el rango completo de la función de pasarela de Network Utility, necesita gestionar IP, los puentes, DLSw y APPN según sea apropiado. Esta sección no incluye estas funciones de capa superior sino que, en lugar de ello, se centra en los modos en que se pueden supervisar y gestionar interfaces físicas y virtuales de canal.

Supervisión de la línea de mandatos

Acceda a los mandatos de talk 5 que muestran el estado de los recursos de canal jerárquicamente del modo siguiente:

1. Desde el indicador *, escriba **talk 5** y pulse **Intro** para obtener el indicador +.
2. Desde el indicador +, escriba **int**, pulse **Intro** y anote el número de interfaz lógica para la interfaz ESCON o PCA física en la que está interesado.

   La interfaz física se denomina comúnmente *red base* y puede tener diversas interfaces virtuales LSA, LCS o MPC+ definidas además de ella. La red base y todas las interfaces virtuales tienen cada una un número de interfaz lógica diferente.
3. Desde el indicador +, escriba **net** *número red base* y pulse **Intro** para obtener el subproceso Console ESCON o PCA. El indicador de mandatos cambia a `ESCON>` o `PCA>` según convenga.

   En estos indicadores, puede utilizar el mandato **li nets** para ver el estado actual de cada interfaz virtual (LSA, LCS, MPC+) utilizando esta red base. También puede escribir **li sub** para ver la configuración de subcanal actualmente en ejecución para esta red base.
4. Desde el indicador `ESCON>` o `PCA>` de la red base, escriba **net** *número red virtual* y pulse **Intro** para ver más detalles acerca de una interfaz virtual determinada que utilice esta red base. El indicador de mandatos cambia a `LSA>`, `LCS>` o `MPC+>`, en función del tipo de interfaz virtual que seleccione.

   Cada uno de este indicadores soporta un mandato **list**, para mostrar información de estado actual y configuración pertinente al tipo de interfaz virtual.
5. Para restituir desde cualquiera de estos niveles anidados, escriba **exit** y pulse **Control-p** para volver al indicador *.

Para obtener ejemplos una explicación detallada de la salida de estos mandatos, consulte el capítulo ″Configuring and Monitoring the ESCON and Parallel Channel Adapters″ de la publicación *MAS Guía del usuario de software*.

Soporte de anotación cronológica de sucesos

Los sucesos que se producen dentro de las funciones de canal están cubiertos por los subsistemas ELS siguientes:

ESC Sucesos ESCON de capa baja
PCA Sucesos de canal paralelo de capa baja
LSA Sucesos relacionados con interfaces virtuales LSA
LCS Sucesos relacionados con interfaces virtuales LCS
MPC+ Sucesos relacionados con interfaces virtuales MPC+

Para habilitar la anotación cronológica de sucesos, escriba **event** desde talk 5 o talk 6 para obtener el subproceso Console o Config de ELS. Si desea que la salida de la anotación cronológica vaya a talk 2, escriba **disp sub** *nombre subsistema* y pulse **Intro** para habilitar el informe de errores normal o **disp sub** *nombre subsistema* **all** para habilitar todos los mensajes. Para obtener la máxima visión en un problema, puede habilitar uno de los subsistemas ESCON o PCA y uno de los subsistemas de interfaz virtual. Si utiliza estos mandatos desde talk 5, puede ir inmediatamente a talk 2 y supervisar los sucesos a medida que se producen.

Puede hacerse una idea de la sucesos indicados por cada uno de estos subsistemas utilizando el mandato **li sub** *nombre subsistema* desde el subproceso ELS de talk 5 o talk 6.

Soporte de gestión SNA

Desde una consola de operador VTAM o NetView/390, puede controlar los recursos SNA asociados con la función de pasarela directa de LSA, DLSw o APPN, como se describe en el apartado “NetView/390” en la página 102.

La propia función de canal no envía alertas SNA. No envía trampas que pueden convertirse en alertas, pero se pueden habilitar trampas para mensajes ELS de canal y utilizar los productos mencionados en el apartado “IBM Nways Manager para AIX” en la página 99 para convertir esas trampas en alertas.

Soporte de trampas y MIB SNMP

El Network Utility soporta una MIB específica de empresa de IBM para ESCON. Esta MIB proporciona acceso a la información siguiente:

- Una lista de interfaces físicas y el estado de señal de fibra de cada una
- Una lista de enlaces de canal y el estado de conexión a sistema principal de cada uno
- Una lista de estaciones de canal con estadísticas de configuración y de tráfico normal/de errores para cada una.

La MIB ESCON no define ninguna trampa. Las funciones de canal paralelo no tienen soporte MIB.

Las interfaces de canal paralelo y ESCON se representan en la MIB de interfaces (RFC 1573), de modo que una estación de gestión puede acceder a sus estadísticas de estado y de tráfico básico por interfaz. El Network Utility permite a una estación de gestión controlar el estado de interfaz y puede enviar trampas para informar cuándo las interfaces se activan o desactivan.

Soporte de aplicación de gestión de red

La aplicación basada en Java de Network Utility descrita en el apartado “Productos IBM Nways Manager” en la página 98 proporciona soporte integrado para la MIB ESCON y la MIB de interfaces. Puede ver el estado de las interfaces codificado en color así como paneles específicos que presentan información clave de estas MIB. También puede utilizar soporte de navegador integrado para ver la información en una de estas MIB.

Puede inhabilitar o habilitar la emisión de trampas de activación/desactivación de interfaz desde los productos Nways Manager.

Capítulo 15. Detalles de configuración de ejemplo de pasarela de canal

Este capítulo contiene diagramas y tablas de parámetros de configuración para varias de las configuraciones de red de pasarela de canal de ejemplo del “Capítulo 14. Pasarela de canal” en la página 203. Los valores de parámetros mostrados proceden de configuraciones de prueba de trabajo reales.

Para obtener una explicación de las columnas y los convenios de las tablas de parámetros de configuración, consulte el apartado “Convenios de las tablas de configuración de ejemplo” en la página 131.

Las páginas World Wide Web de Network Utility contienen archivos de configuración binarios que coinciden con estas tablas de parámetros de configuración. Para acceder a estos archivos, siga el enlace Download desde:

```
http://www.networking.ibm.com/networkutility
```

Las configuraciones documentadas en este capítulo son:

Tabla 71. Referencia cruzada de información de configuraciones de ejemplo

Descripción de la configuración	Tabla de parámetros
“Pasarela de canal ESCON” en la página 208	Tabla 72
“Pasarela de canal paralelo” en la página 216	Tabla 73 en la página 228
“Pasarela de canal (APPN e IP a través MPC+)” en la página 217	Tabla 74 en la página 233

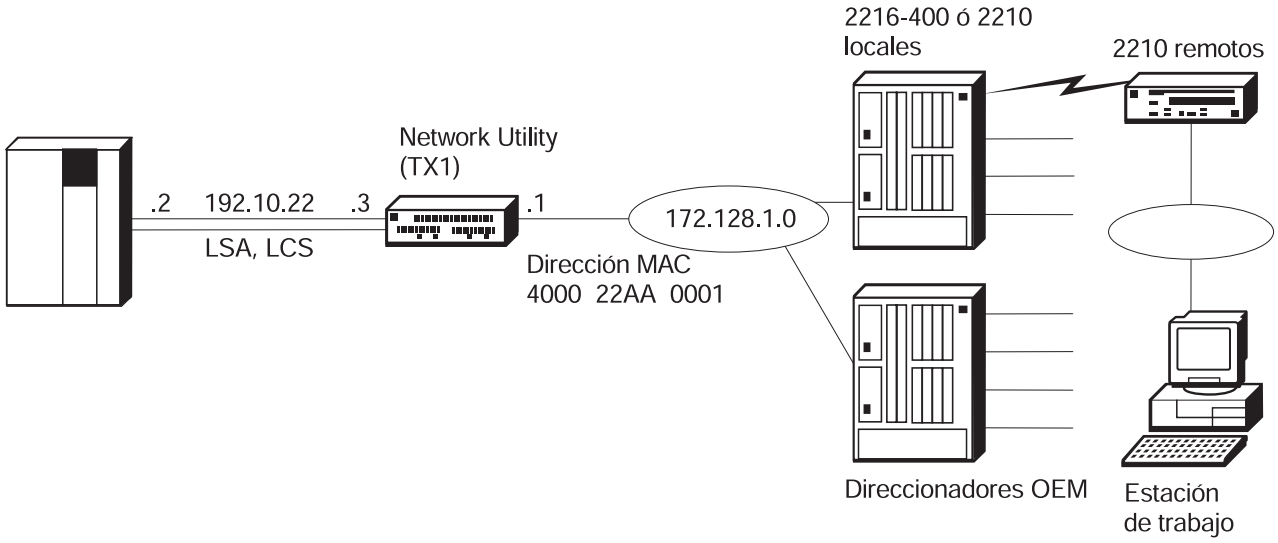


Figura 39. Pasarela de canal ESCON

Tabla 72. Pasarela de canal ESCON. Consulte la página 208 para obtener una descripción y la página 225 para ver un diagrama de esta configuración.

Nav. por prog. conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Dispositivos Adaptadores Ranuras	Ranura 1: TR de 2 puertos Ranura 2: ESCON	`Ver "add device" en la fila siguiente`	1

Tabla 72. Pasarela de canal ESCON (continuación). Consulte la página 208 para obtener una descripción y la página 225 para ver un diagrama de esta configuración.

Nav. por prog. conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Dispositivos Adaptadores Puertos	Ranura 1 Puerto 1: Interfaz 0: TR Ranura 2 Puerto 1: Interfaz 1: ESCON	Config>**add dev tok** Config>**add dev esc**	2
Dispositivos Interfaces	Interfaz 0 Dirección MAC: 400022AA0001	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:01**	
Dispositivos Adaptadores de canal Interfaces ESCON Interfaces ESCON	Interfaz 2 (nueva definición) Número de red base: 1 Tipo de protocolo: LSA Trama de datos máxima: 2052 Número de red LAN: 0 (**Add** para crear interfaz 2)	Config>**net 1** ESCON Config>**add lsa** (añadida como interfaz 2) ESCON Add Virtual>**maxdata 2052** ESCON Add Virtual>**net 0** (cont. en misma sesión con fila sig.)	3,4,5
Dispositivos Adaptadores de canal Interfaces ESCON Subcanales ESCON	Interfaz 2 (resaltar interfaz LSA) Dirección de dispositivo: E4 Dirección de enlace: EF (pulsar en **Add**)	ESCON Add Virtual>**subchannel add** ESCON Add LSA Subchannel>**device E4** ESCON Add LSA Subchannel>**link EF** (escribir **exit** dos veces y luego **list all**)	6
Dispositivos Adaptadores de canal Interfaces ESCON Interfaces ESCON	Interfaz 3 (nueva definición) Número de red base: 1 Tipo de protocolo: LCS Tipo de LAN: Red en Anillo Trama de datos máxima: 2052 Dirección MAC: 400022AA0009 (**Add** para crear interfaz 3)	Config>**net 1** ESCON Config>**add lcs** (añadida como interfaz 3) ESCON Add Virtual>**lantype token** ESCON Add Virtual>**Maxdata 2052** ESCON Add Virt.>**mac 40:00:22:AA:00:09** (cont. en misma sesión con fila sig.)	
Dispositivos Adaptadores de canal Interfaces ESCON Subcanales ESCON	Interfaz 3 (resaltar interfaz LCS) Dirección de dispositivo: E0 Dirección de enlace: EF (pulsar en **Add**)	ESCON Add Virtual>**subchannel add** ESCON Config LCS Subchannel>**device E0** ESCON Config LCS Subchannel>**link EF** (escribir **exit** dos veces y luego **list all**)	7
Sistema General	Nombre de sistema: NU_A Ubicación: XYZ Contacto: Administrador	Config>**set host** Config>**set location** Config>**set contact**	
Sistema SNMP Config General	SNMP (seleccionado)	Config>**p snmp** SNMP Config>**enable snmp**	
Sistema SNMP Config Comunidades General	Nombre de comunidad: admin Tipo acceso: Trampa lect.-grab. Vista de comunidad: Toda	SNMP Config>**add community** SNMP Config>**set comm access write**	
Protocolos IP General	Dirección interna: 172.128.252.1 ID de direccionador: 172.128.1.1	Config>**p ip** IP config>**set internal 172.128.252.1** IP config>**set router-id 172.128.1.1**	
Protocolos IP Interfaces	Interfaz 0 (TR ranura 1 puerto 1) Dirección IP: 172.128.1.1 Másc. subred: 255.255.255.0 Interfaz 3 (Interfaz LCS) Dirección IP: 192.10.22.3 Másc. subred: 255.255.255.0	IP config>**add address** (una vez por i/f)	8

Tabla 72. Pasarela de canal ESCON (continuación). Consulte la página 208 para obtener una descripción y la página 225 para ver un diagrama de esta configuración.

Nav. por prog. conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Protocolos IP OSPF General	OSPF (seleccionado)	Config>**p ospf** OSPF Config>**enable ospf**	8
Protocolos IP OSPF Config. de área General	Número de área: 0.0.0.0 Área apéndice (no seleccionada)	OSPF Config>**set area**	
Protocolos IP OSPF Direccion. límite AS	Direccionamiento de límite AS (seleccionado para habilitar) Importar rutas directas (seleccionado para habilitar)	OSPF config>**enable as** Import direct routes (Aceptar otros valores por omisión)	9
Protocolos IP OSPF Interfaces	Interfaz 0 OSPF (seleccionado)	OSPF Config>**set interface** Interface IP address: **172.128.1.1** Attaches to area: **0.0.0.0** (Aceptar otros valores por omisión)	

Notas:

1. **add dev** define un solo puerto, no un adaptador.
2. El programa de configuración asigna automáticamente un número de interfaz a todos los puertos de un adaptador y el usuario suprime los que no desea utilizar. Desde la línea de mandatos, escriba el mandato **add dev** para cada puerto que desee utilizar y el número de interfaz (también conocido como ″número de red″) es la salida del mandato.
3. Al seleccionar una interfaz de tipo LSA, el campo “LAN type” se inhabilita (queda sombreado) y aparecen los recuadros de selección “LAN net number” y “loopback”.
4. El campo “LAN number” está inhabilitado porque el direccionador asigna un valor automáticamente. Este valor debe configurarse en la definición de sistema principal para “ADAPTNO”.
5. Al añadir (“Add”) la interfaz, se generará una nueva interfaz y a ésta se le asignará el siguiente número de interfaz disponible.
6. Los valores entrados al configurar los subcanales deben coincidir con los valores configurados en el sistema principal. Consulte el “Capítulo 18. Definiciones de sistema principal de ejemplo” en la página 259 para ver ejemplos de cómo hacer coincidir estos valores.
7. Al añadir subcanales para una interfaz virtual LCS, sólo es necesario definir un subcanal aunque LCS necesita dos. LCS utiliza automáticamente el siguiente subcanal además del definido aquí. LCS utilice la dirección de dispositivo par (E0 en este caso) como subcanal de grabación y la dirección impar (E1) como subcanal de lectura.
8. También puede utilizar RIP en lugar de OSPF.
9. Necesita importar rutas directas a OSPF desde la interfaz ESCON porque OSPF no está habilitado en la interfaz ESCON. En lugar de ello, la subred de la interfaz ESCON se importa a OSPF en el Network Utility y entonces se propaga a la red. Esto es necesario para evitar que se produzcan mensajes de error en el sistema principal si el Network Utility envía las actualizaciones de OSPF a través de la conexión LCS. TCP/IP en el sistema principal no soporta (aún) anuncios de estado de enlace (Link State Advertisements) de un direccionador OSPF.

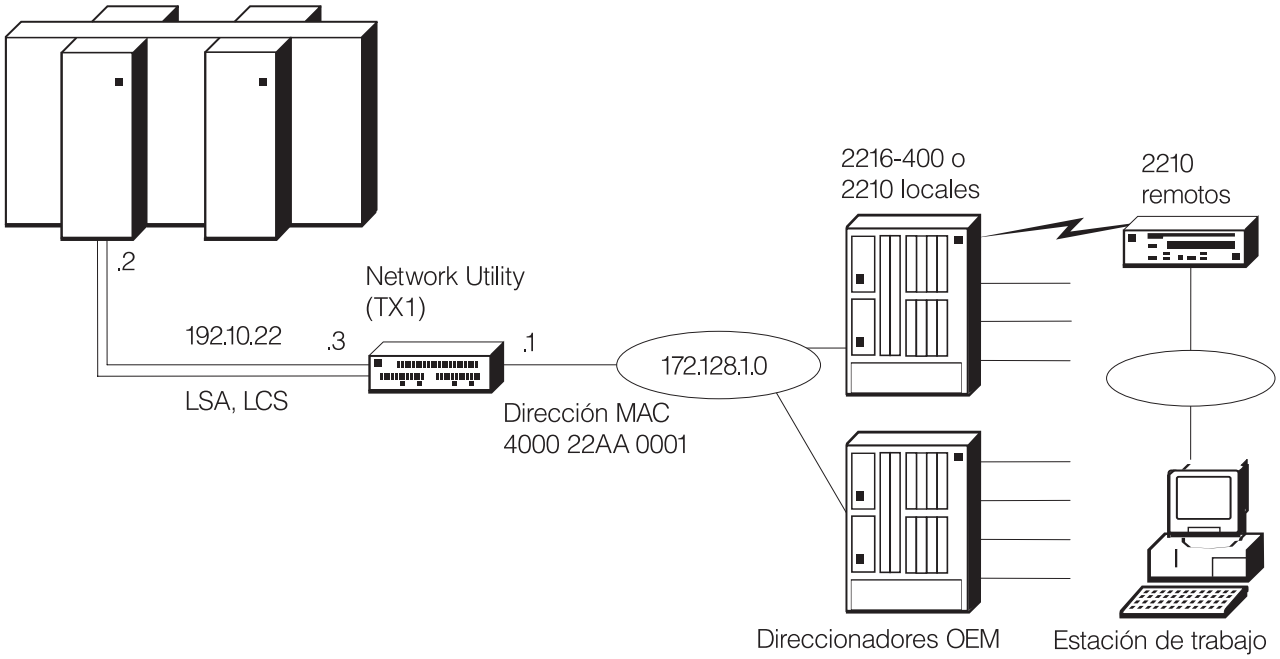


Figura 40. Pasarela de canal paralelo

Tabla 73. Pasarela de canal paralelo. Consulte la página 216 para obtener una descripción y la página 228 para ver un diagrama de esta configuración.

Nav. por prog. conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Dispositivos Adaptadores Ranuras	Ranura 1: TR de 2 puertos Ranura 2: Ad. canal paral. (PCA)	Ver "add device" en la fila siguiente	1
Dispositivos Adaptadores Puertos	Ran. 1/Puerto 1: Interfaz 0: TR Ran. 2/Puerto 1: Interfaz 1: PCA	Config>**add dev tok** Config>**add dev PCA**	2
Dispositivos Interfaces	Interfaz 0 Dirección MAC: 400022AA0001	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:01**	
Dispositivos Adaptadores de canal Interfaces PCA Interfaces PCA	Interfaz 2 (nueva definición) Número de red base: 1 Tipo de protocolo: LSA Número de red LAN: 0 (**Add** para crear interfaz 2)	Config>**net 1** PCA Config>**add lsa** (añadida como interfaz 2) PCA Add Virtual>**net 0** (cont. en misma sesión con fila sig.)	3,4,5
Dispositivos Adaptadores de canal Interfaces PCA Subcanales PCA	Interfaz 2 (resaltar interfaz LSA) Dirección de dispositivo: 00 Tipo de subcanal: lect./grab. (pulsar en **Add**)	PCA Add Virtual>**subchannel add** PCA Add LSA Subchannel>**device 00** (Escribir **exit** dos veces y luego **list all**)	6
Dispositivos Adaptadores de canal Interfaces PCA Interfaces PCA	Interfaz 3 (nueva definición) Número de red base: 1 Tipo de protocolo: LCS Dirección MAC: 400022AA0009 (**Add** para crear interfaz 3)	Config>**net 1** PCA Config>**add lcs** (añadida como interfaz 3): PCA Add Virtual>**mac 40:00:22:AA:00:09** (cont. en misma sesión con fila sig.)	
Dispositivos Adaptadores de canal Interfaces PCA Subcanales PCA	Interfaz 3 (resaltar interfaz LCS) Dirección de dispositivo: 02 Tipo de subcanal: grabación (pulsar en **Add**)	PCA Add Virtual>**subchannel add** PCA Add LCS Subchannel>**device 02** (Escribir **exit** dos veces y luego **list all**)	7

Tabla 73. Pasarela de canal paralelo (continuación). Consulte la página 216 para obtener una descripción y la página 228 para ver un diagrama de esta configuración.

Nav. por prog. conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Sistema General	Nombre de sistema: NU_A Ubicación: XYZ Contacto: Administrador	Config>**set host** Config>**set location** Config>**set contact**	
Sistema SNMP Config General	SNMP (seleccionado)	Config>**p snmp** SNMP Config>**enable snmp**	
Sistema SNMP Config Comunidades General	Nombre de comunidad: admin Tipo acceso: Trampa lect.-grab. Vista de comunidad: Toda	SNMP Config>**add community** SNMP Config>**set comm access write**	
Protocolos IP General	Dirección interna: 172.128.252.1 ID de direccionador: 172.128.1.1	Config>**p ip** IP config>**set internal 172.128.252.1** IP config>**set router-id 172.128.1.1**	
Protocolos IP Interfaces	Interfaz 0 (TR ranura 1 puerto 1) Dirección IP: 172.128.1.1 Másc. subred: 255.255.255.0 Interfaz 3 (Interfaz LCS) Dirección IP: 192.10.22.3 Másc. subred: 255.255.255.0	IP config>**add address** (una vez por i/f)	8
Protocolos IP OSPF General	OSPF (seleccionado)	Config>**p ospf** OSPF Config>**enable ospf**	8
Protocolos IP OSPF Config. de área General	Número de área: 0.0.0.0 Área apéndice (no seleccionada)	OSPF Config>**set area**	
Protocolos IP OSPF Direccionamiento límite AS	Direccionamiento de límite AS (seleccionado para habilitar) Importar rutas directas (seleccionado para habilitar)	OSPF Config>**enable as** Import direct routes (Aceptar otros valores por omisión)	9
Protocolos IP OSPF Interfaces	Interfaz 0 OSPF (seleccionado)	OSPF Config>**set interface** Interface IP address: **172.128.1.1** Attaches to area: **0.0.0.0** (Aceptar otros valores por omisión)	

Notas:

1. **add dev** define un solo puerto, no un adaptador.
2. El programa de configuración asigna automáticamente un número de interfaz a todos los puertos de un adaptador y el usuario suprime los que no desea utilizar. Desde la línea de mandatos, escriba el mandato **add dev** para cada puerto que desee utilizar y el número de interfaz (también conocido como ″número de red″) es la salida del mandato.
3. Al seleccionar una interfaz de tipo LSA, el campo “LAN type” se inhabilita (queda sombreado) y aparecen los recuadros de selección “LAN net number” y “loopback”.
4. El campo “LAN number” está inhabilitado porque el direccionador asigna un valor automáticamente. Este valor debe configurarse en la definición de sistema principal para “ADAPTNO”.
5. Al añadir (“Add”) la interfaz, se generará una nueva interfaz y a ésta se le asignará el siguiente número de interfaz disponible.
6. Los valores entrados al configurar los subcanales deben coincidir con los valores configurados en el sistema principal. Consulte el “Capítulo 18. Definiciones de sistema principal de ejemplo” en la página 259 para ver ejemplos de cómo hacer coincidir estos valores.
7. Al añadir subcanales para una interfaz virtual LCS, sólo es necesario definir un subcanal aunque LCS necesita dos. LCS utiliza automáticamente el siguiente subcanal además del definido aquí. LCS utiliza la dirección de dispositivo par (02 en este caso) como subcanal de grabación y la dirección impar (03) como subcanal de lectura.
8. También puede utilizar RIP en lugar de OSPF.
9. Necesita importar rutas directas a OSPF desde la interfaz PCA porque OSPF no está habilitado en la interfaz PCA. En lugar de ello, la subred de la interfaz PCA se importa a OSPF en el Network Utility y entonces se propaga a la red. Esto es necesario para evitar que se produzcan mensajes de error en el sistema principal si el Network Utility envía las actualizaciones de OSPF a través de la conexión LCS. TCP/IP en el sistema principal no soporta (aún) anuncios de estado de enlace (Link State Advertisements) de un direccionador OSPF.

El Network Utility proporciona tres procedimientos para operar la interfaz LCS:

El ejemplo siguiente ilustra la configuración de Paso a través LCS:

```
*t 6
Gateway user configuration
config>add dev esc
Device Slot #(1-8) [1] ?3
Adding ESCON Channel device in slot 3 port 1 as interface #4
Use "net 4" to configure ESCON Channel parameters
Config>net 4
ESCON Config>add lcs
ESCON Add Virtual>?
LANtype
MAC address
MAXdata
BLKtimer
ACKlen
SUBchannels
ENable 3172 Emulation
Exit
ESCON Add Virtual>enable
Enabling LCS 3172 Emulation for network 5.
Please set the Network link using the "Net" command.
ESCON Add Virtual>?
BLKtimer
ACKlen
SUBchannels
DISable 3172 Emulation
NET link
Exit
ESCON Add Virtual>net 0
ESCON Add Virtual>sub add
```

```
Please add or configure one subchannel for an LCS virtual interface.
Although LCS requires two subchannels, it is only necessary to specify
one subchannel.  An adjacent subchannel will be chosen such that the
two subchannels will form a sequential pair with the write subchannel
(device address is even) before the read subchannel (device address
is odd).
ESCON Config LCS subchannel>?
LINk address (ESCD Port)
LPAR number
CU logical address
Device address
Exit
ESCON
ESCON Config LCS Subchannel>link f7
ESCON Config LCS Subchannel>lpar 0
ESCON Config LCS Subchannel>cu 0
ESCON Config LCS Subchannel>dev 20
ESCON Config LCS Subchannel>ex
ESCON Add Virtual>ex
>

ESCON Config>list
Net   5   Protocol: LCS    LAN type: Token Ring         LAN number: 0
          3172 Emulation is enabled
          MAC address: Obtained from net 0
          Block timer:    5 ms   ACK length:    10 bytes
ESCON config>list all
Net   5   Protocol: LCS    LAN type: Token Ring         LAN number: 0
          3172 Emulation is enabled
          MAC address: Obtained from net 0
          Block timer:    5 ms   ACK length:    10 bytes
          Read Subchannels:
          Sub  0   Dev addr: 21  LPAR: 0  Link addr: F7    CU addr: 0
          Write Subchannels:
          Sub  1   Dev addr: 20  LPAR: 0  Link addr: F7    CU addr:  0

ESCON Config
```

El ejemplo siguiente ilustra el indicador t 5 con la Emulación 3172 habilitada:

```
LCS> list all

LCS Virtual Adapter
LCS Information for Net 5
--- ----------- --- --- --
LAN Type: Token-Ring           LAN Number: 0
Local Read Subchannel number:  1
Local Write Subchannel number: 0
MAC Address: 08005AFE0144
LCS 3172 Emulation to net 0
Status: Down
```

La Figura 41 en la página 232 muestra cómo se correlacionan los parámetros entre el sistema principal y el Network Utility para una definición de interfaz LCS.

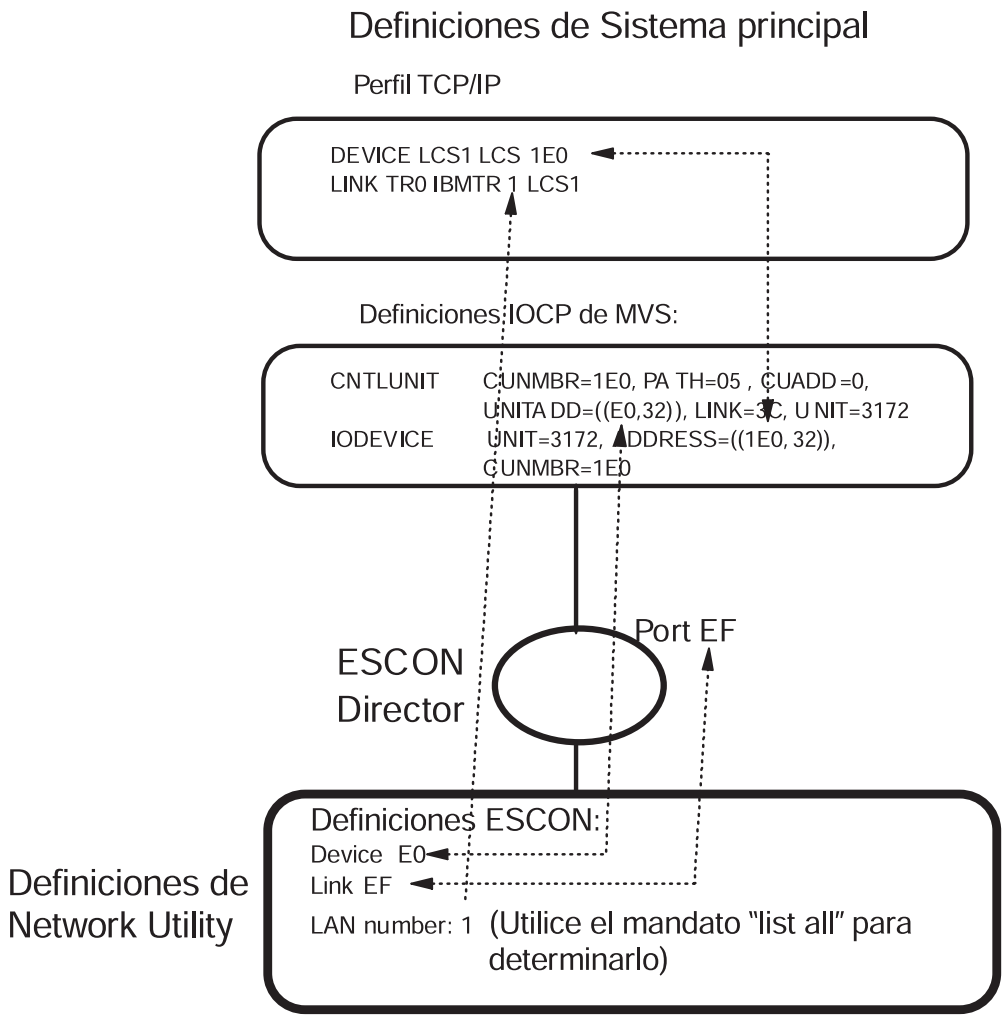


Figura 41. Relaciones entre parámetros de sistema principal y Network Utility - LCS

Notas:

1. LCS utiliza una pareja de subcanales, uno para lectura y otro para grabación. Al configurar los subcanales utilizados por la interfaz LCS, en realidad sólo necesita especificar una dirección de subcanal. LCS asigna automáticamente dos subcanales adyacente para la conexión LCS, uno para la lectura (la dirección de dispositivo es impar) y otro para la grabación (la dirección de dispositivo es par).
2. La dirección de dispositivo especificada en la definición de interfaz LCS de Network Utility debe estar dentro del rango especificado en el parámetro UNITADD de la macro CNTLUNIT desde el IOCP. Por ejemplo, el parámetro UNITADD de la Figura 41 muestra que se están reservando 32 direcciones de dispositivo (decimales) que empiezan en E0 (hex) para la definición de Network Utility. Se ha especificado una dirección de dispositivo de E0 para la interfaz LCS de Network Utility. El Network Utility también asignará automáticamente E1. Dado que E0 y E1 están en el rango E0 a FF hex, esto es correcto a condición de que ningún otro dispositivo (o interfaz de este Network Utility) intente utilizar los mismos subcanales.
3. El valor especificado en la sentencia DEVICE del perfil TCP/IP de sistema principal debe estar dentro del rango especificado en el parámetro ADDRESS de la macro IODEVICE desde el IOCP. Por ejemplo, la sentencia DEVICE del

perfil TCP/IP del sistema principal de la Figura 41 en la página 232 es 1E0 hex, que está en el rango 1E0 a 1FF que especifica el parámetro ADDRESS de la sentencia IODEVICE.

4. Los valores especificados para el parámetro ADDRESS en la macro IODEVICE y el parámetro UNITADD en la macro CNTLUNIT están relacionados ***por convenio solamente***. En este ejemplo, el valor para el parámetro ADDRESS se ha determinado a partir del valor para el parámetro UNITADD añadiendo delante del valor de UNITADD un ***identificador de canal lógico*** (en este caso 1). Esto sucederá con frecuencia. Sin embargo, al definir la dirección de dispositivo en la definición de LCS del Network Utility, utilice el parámetro UNITADD y no el parámetro ADDRESS para determinar el rango válido de valores.

Consulte el “Capítulo 18. Definiciones de sistema principal de ejemplo” en la página 259 para obtener una mayor explicación y más ejemplos de definiciones de sistema principal para este tipo de interfaz.

Para obtener una visión completa de los parámetros de configuración necesarios para este escenario, consulte la Tabla 19 en la página 158.

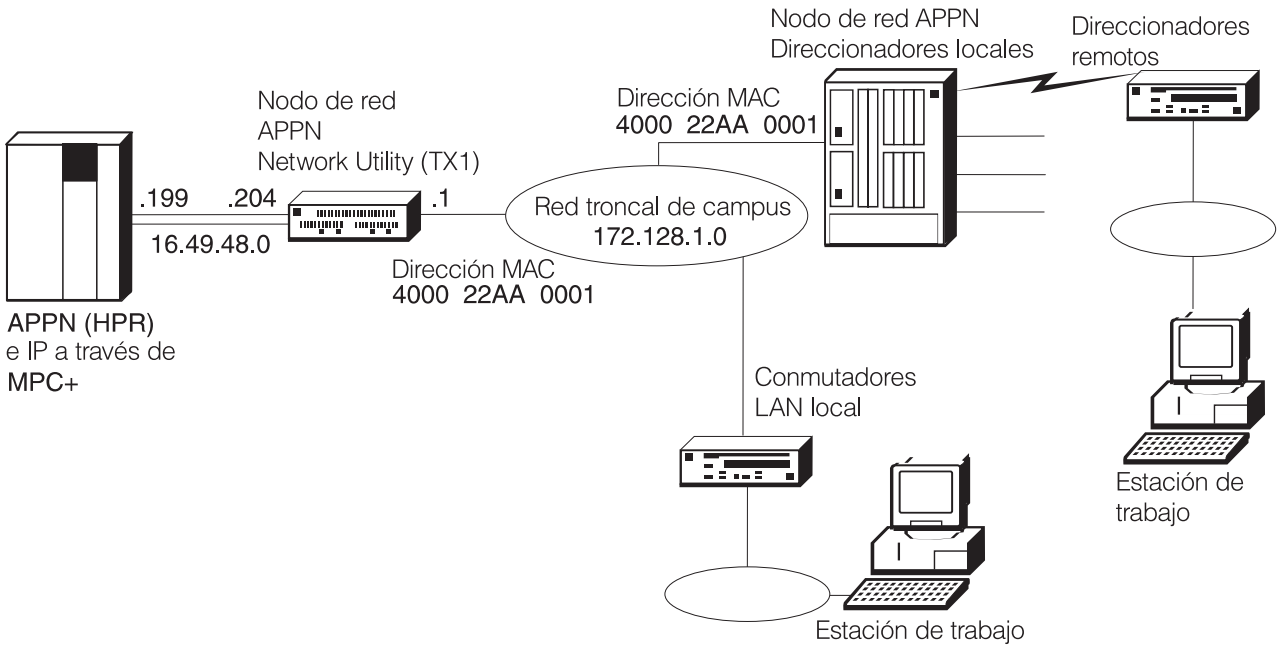


Figura 42. Pasarela de canal (APPN e IP a través de MPC+)

Tabla 74. Pasarela de canal (APPN e IP a través de MPC+). Consulte la página 217 para obtener una descripción y la página 233 para ver un diagrama de esta configuración.

Nav. por prog. conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Dispositivos Adaptadores Ranuras	Ranura 1: TR de 2 puertos Ranura 2: ESCON	`Ver "add device" en la fila siguiente`	1
Dispositivos Adaptadores Puertos	Ran. 1/Puerto 1: Inter. 0: TR Ran. 2/Puerto 1: Inter. 1: ESCON	`Config>`**`add dev tok`** `Config>`**`add dev esc`**	2

Tabla 74. Pasarela de canal (APPN e IP a través de MPC+) (continuación). Consulte la página 217 para obtener una descripción y la página 233 para ver un diagrama de esta configuración.

Nav. por prog. conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Dispositivos Interfaces	Interfaz 0 Dirección MAC: 400022AA0001	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:01**	
Dispositivos Adaptadores de canal Interfaces ESCON Interfaces ESCON	Interfaz 2 (nueva definición) Número de red base: 1 Tipo de protocolo: MPC+ (**Add** para crear interfaz 2)	Config>**net 1** ESCON Config>**add mpc** (añadida como interfaz 2) ESCON Add Virtual> (cont. en misma sesión con fila sig.)	3
Dispositivos Adaptadores de canal Interfaces ESCON Subcanales ESCON	(resaltar interfaz 2) Dirección de dispositivo: F0 Dirección de enlace: EF Tipo de subcanal: Lectura (**Add** para definir subcanal) Dirección de dispositivo: F1 Dirección de enlace: EF Tipo de subcanal: Grabación (**Add** para definir subcanal)	ESCON Add Virtual>**sub addr** ESCON Add MPC+ Read Subchannel>**dev f0** ESCON Add MPC+ Read Subchannel>**link ef** ESCON Add MPC+ Read Subchannel>**exit** ESCON Add Virtual>**sub addw** ESCON Add MPC+ Write Subchannel>**dev f1** ESCON Add MPC+ Write Subch.>**link ef** (escribir **exit** dos veces y luego **list all**)	4
Sistema General	Nombre de sistema: NU_A Ubicación: XYZ Contacto: Administrador	Config>**set host** Config>**set location** Config>**set contact**	
Sistema SNMP Config General	SNMP (seleccionado)	Config>**p snmp** SNMP Config>**enable snmp**	
Sistema SNMP Config Comunidades General	Nombre de comunidad: admin Tipo acceso: Trampa lect.-grab. Vista de comunidad: Toda	SNMP Config>**add community** SNMP Config>**set comm access write**	5
Protocolos IP General	Dirección interna: 172.128.252.1 ID de direccionador: 172.128.1.1	Config>**p ip** IP config>**set internal 172.128.252.1** IP config>**set router-id 172.128.1.1**	
Protocolos IP Interfaces	Interfaz 0 (TR ranura 1 puerto 1) Dirección IP: 172.128.1.1 Másc. subred: 255.255.255.0 Interfaz 2 (interfaz MPC+) Dirección IP: 16.49.48.204 Másc. subred: 255.255.255.0	IP config>**add address** (una vez por i/f)	
Protocolos IP OSPF General	OSPF (seleccionado)	Config>**p ospf** OSPF Config>**enable ospf**	6
Protocolos IP OSPF Config. de área General	Número de área: 0.0.0.0 Área apéndice (no seleccionada)	OSPF Config>**set area**	
Protocolos IP OSPF Direcc. de límite AS	Direccionamiento de límite AS (seleccionado para habilitar) Importar rutas directas (seleccionado para habilitar)	OSPF Config>**enable as** Import direct routes (Aceptar otros valores por omisión)	7

Tabla 74. Pasarela de canal (APPN e IP a través de MPC+) (continuación). Consulte la página 217 para obtener una descripción y la página 233 para ver un diagrama de esta configuración.

Nav. por prog. conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Protocolos IP OSPF Interfaces	Interfaz 0 OSPF (seleccionado)	OSPF Config>**set interface** Interface IP address: **172.128.1.1** Attaches to area: **0.0.0.0** (Aceptar otros valores por omisión)	
Protocolos APPN General	Nodo red APPN (para habil.) ID de red: STFNET Nomb. punto de control: NUGW	Config>**p appn** APPN config> **set node** Enable APPN Network ID: **STFNET** Control point name: **NUGW** (Aceptar otros valores por omisión)	
Protocolos APPN Interfaces	(resaltar Red en Anillo interfaz 0) (pulsar en la pestaña Configure) Def. puerto APPN (para habil.) Nombre de puerto: TR001	APPN config>**add port** APPN Port Link Type: **TOKEN RING** Port name: **TR001** Enable APPN (Aceptar otros valores por omisión)	
Protocolos APPN Interfaces	(resaltar Red en Anillo interf. 0) (pulsar pestaña Link stations) TRTG001 (nueva definición) Pestaña General-1: Nombre est. enl.: TRTG001 Pestaña General-2: Direcc. MAC nodo adyac.: 400022AA0011 Tipo de nodo adyacente: Nodo de red APPN (**Add** para crear Estac. enlace)	APPN config>**add link** Port name for the link stat.: **TR001** Station name: **TRTG001** MAC addr. of adj. node: **400022AA0011** (Aceptar otros valores por omisión)	8
Protocolos APPN Interfaces	(resaltar interf. 2 ESCON-MPC+) (pulsar pestaña Configure) Def. puerto APPN (para habil.) Nombre de puerto: MPC001	APPN config>**add port** APPN Port Link Type: **MPC** Interface Number: **2** Port name: **MPC001** Enable APPN (Aceptar otros valores por omisión)	
Protocolos APPN Interfaces	(resaltar interf. 2 ESCON-MPC+) (pulsar pestaña Link stations) MPCTG001 (nueva definición) Pestaña General-1: Nomb. est. enl.: MPCTG001 Pestaña General-2: Tipo de nodo adyacente: Nodo de red APPN (**Add** para crear Est. enlace)	APPN config>**add link** Port name for the link stat.: **MPC001** Station name: **MPCTG001** Adj. Node Type: **0** = APPN Netw. Node (Aceptar otros valores por omisión)	

Notas:

1. **add dev** define un solo puerto, no un adaptador.
2. El programa de configuración asigna automáticamente un número de interfaz a todos los puertos de un adaptador y el usuario suprime los que no desea utilizar. Desde la línea de mandatos, escriba el mandato **add dev** para cada puerto que desee utilizar y el número de interfaz (también conocido como ″número de red″) es la salida del mandato.
3. Al añadir (“Add”) la interfaz, se generará una nueva interfaz y a ésta se le asignará el siguiente número de interfaz disponible.
4. Los valores entrados al configurar los subcanales deben coincidir con los valores configurados en el sistema principal. Consulte el “Capítulo 18. Definiciones de sistema principal de ejemplo” en la página 259 para ver ejemplos de cómo hacer coincidir estos valores.
5. Sólo necesita una comunidad SNMP con capacidad para grabación si desea bajar archivos de configuración directamente del programa de configuración al direccionador. SNMP no es necesario para enviar mediante TFTP un archivo de configuración al direccionador.
6. También puede utilizar RIP en lugar de OSPF.
7. Necesita importar rutas directas a OSPF desde la interfaz ESCON porque OSPF no está habilitado en la interfaz ESCON. En lugar de ello, la subred de la interfaz ESCON se importa a OSPF en el Network Utility y entonces se propaga a la red. Esto es necesario para evitar que se produzcan mensajes de error en el sistema principal si el Network Utility envía las actualizaciones OSPF a través de la conexión MPC+. TCP/IP en el sistema principal no soporta (aún) anuncios de estado de enlace (Link State Advertisements) de un direccionador OSPF.
8. La dirección MAC de destino de este ejemplo es el direccionador local del lado derecho de la red troncal de campus de la Figura 42 en la página 233. Este direccionador también se ha configurado para ser un nodo de red APPN.

Capítulo 16. Conmutación de enlace de datos

Visión general

Esta sección introduce la Conmutación de enlace de datos (DLSw) y resume la función DLSw implementada en el Network Utility.

¿Qué es DLSw?

DLSw es una tecnología estándar inventada por IBM para transportar protocolos orientados a conexión, principalmente SNA y NetBIOS, a través de redes troncales IP. Los direccionadores DLSw de los bordes de una red IP contestan las peticiones de establecimiento de enlace de las estaciones finales nativas SNA y NetBIOS, buscan entre los direccionadores DLSw iguales uno que sirva a la estación final de destino y luego definen una vía y datos de aplicación de relay entre las estaciones finales a través del direccionador igual.

El protocolo que fluye entre los direccionadores DLSw se documenta en el RFC 1795, ″Data Link Switching: Switch to Switch Protocol″. Las aclaraciones acerca de este protocolo y las mejoras de escalabilidad basada en IP de multidistribución se documentan en el RFC 2166, ″DLSw v2.0 Enhancements″.

Muchas implementaciones de DLSw proporcionan una función *DLSw local* que conecta dos enlaces en un solo direccionador, en lugar de conectarlos a través de una red IP a otro direccionador DLSw. En función de los tipos de DLC implicados, esta función puede ser equivalente a la de un FRAD o PAD X.25.

Función DLSw de Network Utility

La implementación de DLSw de Network Utility es casi idéntica en función a la de los direccionadores IBM 2210 y 2216. Puede manejar los siguientes protocolos de estación final:

- SNA
  - PU 4/5 a PU 2.0 (e IBM 5394 en SDLC)
  - T2.1 a T2.1
  - PU 4/5 a PU 4/5
- NetBIOS
  - Sesiones de punto a punto
  - Tráfico de datagramas de difusión
- Gestor de red LAN
  - LNM en servidores de puente (p.ej., LBS, CRS, REM)
  - LNM en distribuidor inteligente 8235
  - LNM en Gestión de estaciones LAN

DLSw de Network Utility puede comunicarse con estaciones finales a través de los tipos de control de enlace de datos (DLC) siguientes:

- LLC 802.2

  Se puede transportar LLC a través de cualquiera de estos tipos de interfaz:
  - Red en Anillo
  - Ethernet (adaptadores a 10 Mbps o 10/100 Mbps)
  - FDDI
  - Enlaces PPP habilitados para puentes remotos

  - PVC y SVC de Frame Relay habilitados para puentes remotos (formatos de tramas de puente RFC 1490/2427)
  - Emulación de LAN ATM
  - Puentes nativos ATM (formatos de tramas de puente RFC 1483)
- SDLC

  DLSw puede representar la estación primaria en una línea de múltiples puntos, múltiples estaciones secundarias o una sola estación totalmente negociable en una línea de punto a punto.
- QLLC

  DLSw soporta cualquier combinación de PVC y SVC QLLC en una sola interfaz X.25. Puede manejar circuitos virtuales paralelos en la misma dirección remota DTE, así como llamadas de entrada de SVC no configuradas.
- APPN

  Puede configurar APPN para conectarse a la función DLSw que reside en el mismo Network Utility. Esto permite a APPN tener enlaces con cualquier estación final SNA PU 2.0 o T2.1 de la red DLSw, sin necesitar que APPN esté presente en los direccionadores remotos (especialmente de sucursal).
- LSA de canal

  DLSw soporta una interfaz interna en la función LSA de canal ESCON y paralelo que reside en el mismo Network Utility. Esto permite al sistema principal tener enlaces con cualquier estación final SNA de la red DLSw, sin necesitar productos independientes de direccionador DLSw de ubicación central y de pasarela de canal.

Con DLSw remoto (a través de IP a otro direccionador), DLSw de Network Utility soporta la conversión de tramas TCP DLSw a cualquiera de los tipos DLC soportados. DLSw local se soporta sólo para combinaciones específicas de tipos de DLC, como se muestra aquí:

	LLC	SDLC	QLLC	APPN	LSA de canal
LLC	(1)	x	x		x
SDLC	x	x	x	x	x
QLLC	x	x	x	x	x
APPN		x	x		x
CHANNEL	x	x	x	x	

Nota:
1 - Deberá utilizar puentes para la conectividad local de LLC a LLC. La única excepción soportada por DLSW local es LLC en un puerto de puente Frame Relay que esté configurado como puerto BAN (Boundary Access Node) (Nodo de acceso de límite).

La lista siguiente resume algunas de las demás posibilidades y características de DLSw de Network Utility de IBM.

- Compatibilidad dinámica con todos los estándares de protocolo DLSw

  DLSw de IBM soporta el RFC 1434+, RFC 1795 (Versión 1 de DLSw 1) y el RFC 2166 (Versión 2 de DLSw). Detecta dinámicamente el nivel de protocolo de cada direccionador asociado sin preconfiguración y puede manejar simultáneamente asociados en diferentes niveles de protocolo.
- Asociados dinámicos y a petición

  DLSw de IBM soporta el arranque de conexiones TCP en asociados configurados sólo cuando es necesario, así como el descubrimiento de estaciones finales servidas por asociados no configurados y el arranque de esas conexiones TCP a petición.
- Descubrimiento de IP de multidistribución

Con la simple configuración de direcciones o grupos IP de multidistribución, DLSw de IBM puede efectuar búsquedas de multidistribución para las estaciones finales y los asociados. DLSw de IBM proporciona diversas extensiones dinámicas en el estándar DLSw de la Versión 2, que incluyen el registro de recursos y la configuración de grupo simplificada.

- Prioridad del tráfico

  Existen opciones de configuración que no sólo le permiten controlar la prioridad de SNA frente a NetBIOS, sino también las prioridades de circuito individuales. Esto es además del amplio soporte del BRS (Bandwidth Reservation System) (Sistema de reserva de anchura de banda) para la prioridad de tráfico a nivel de interfaz.

- Filtro avanzado y entradas de antememoria estática

  DLSw de IBM incluye un amplio soporte para listas de direcciones MAC y nombres NetBIOS y almacenamiento en antememoria estática, permitiéndole controlar qué enlaces se utilizan para buscar recursos así como qué asociados remotos se prefieren.

- Equilibrio de carga y tolerancia de errores

  DLSw de IBM puede almacenar en antememoria múltiples asociados remotos y seleccionar entre ellos basándose en la prioridad de vecindad, en el soporte de tamaño de trama mayor o en quién es el primero en responder. También puede utilizar la característica de prioridad de vecindad para asegurarse de que un direccionador de la ubicación central sólo sirve de reserva de otro.

  Para configuraciones que incluyen direcciones MAC duplicadas, puede inhabilitar la característica de prioridad de vecindad o establecer parámetros de antememoria para controlar las vías utilizadas para alcanzar dichas direcciones MAC.

Configuraciones de ejemplo

Esta sección describe tres configuraciones de ejemplo que utilizan la característica Conmutación de enlace de datos del Network Utility. Estas configuraciones son:

- Receptor de LAN DLSw
- Pasarela de canal de LAN DLSw
- Pasarela de canal de DLSw X.25

Receptor de LAN DLSw

Este escenario se muestra en la Figura 43 en la página 240. En este escenario, el tráfico SNA de las ubicaciones remotas utiliza DLSw para volver al centro de datos.

El Network Utility está en el centro de datos en el segmento de LAN de red troncal. Es un asociado DLSw con cada direccionador remoto y, como tal, necesita una sesión TCP con cada uno. La ventaja de este planteamiento es que todos los ciclos de CPU necesarios para gestionar estas sesiones TCP y para terminar las conexiones DLSw se concentran en el Network Utility. Sin el Network Utility, esta carga de trabajo puede consumir los direccionadores locales o la pasarela de sistema principal (si es capaz de DLSw).

Desde la perspectiva del sistema principal, se establece un puente para el tráfico LLC2 SNA hacia el Network Utility desde la pasarela de sistema principal. La pasarela de sistema principal es un IBM 3745/46, un IBM 3746 con el Multiaccess Enclosure (MAE) o un IBM 2216.

Puede aprovecharse del Adaptador de Red en Anillo de 2 puertos del Network Utility haciendo pasar el tráfico SNA encapsulado en IP por un puerto y entregando el tráfico SNA LLC2 en el otro puerto de Red en Anillo. De este modo, tiene el doble de anchura de banda disponible con la ventaja adicional de separar el tráfico IP y SNA en anillos independientes. Dado que el Network Utility proporciona reconocimientos locales LLC (spoofing) (simulación) en el sistema principal para cada conexión LLC, esto reduce una cantidad considerable de tráfico de la red troncal del campus en entornos de red grandes.

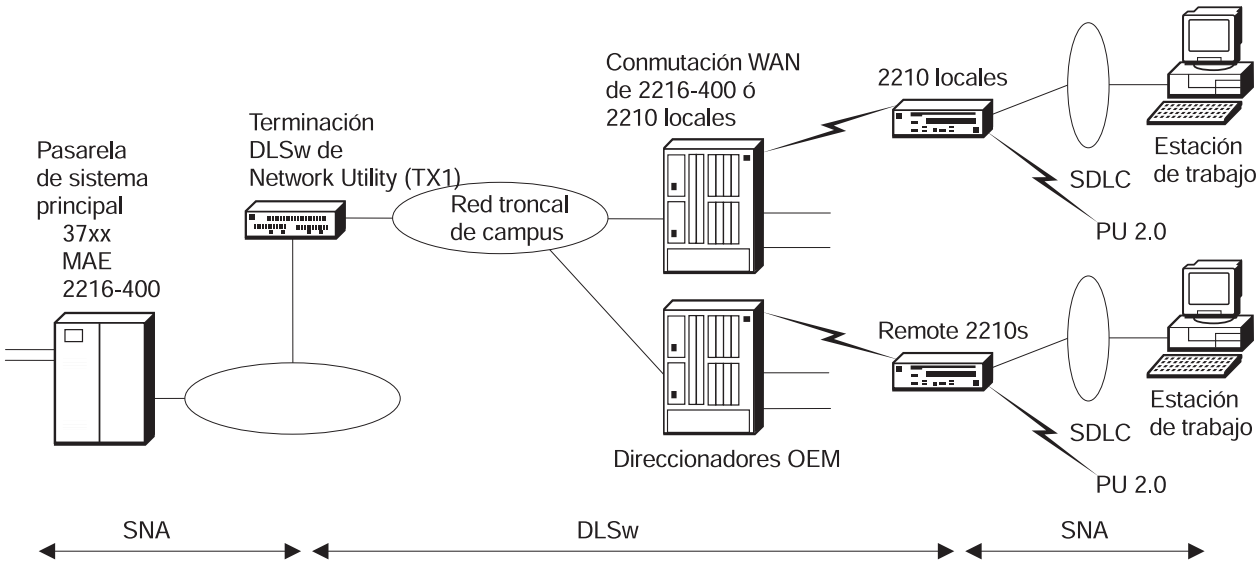


Figura 43. Receptor de LAN DLSw

Claves para la configuración

En la mayor parte, se trata de una configuración DLSw estándar. Sin embargo, deberá tener presentes los puntos siguientes al configurar el Network Utility como un Receptor de LAN DLSw:

- Para este escenario, deberá configurar el Network Utility para permitir sesiones TCP desde cualquiera de los direccionadores remotos. A éstos se les denomina vecinos dinámicos DLSw. Esto le evita tener que definir la dirección IP de cada asociado DLSw del Network Utility. El valor por omis¡ón para vecinos dinámicos es ″Enabled″ (habilitados).
- El Network Utility introduce un nuevo parámetro para las implementaciones de DLSw de IBM que le permite especificar cómo se reenvían las tramas de explorador. Esto es especialmente importante en la dirección de salida desde la ubicación central. El parámetro se denomina *enable/disable forwarding explorers* (habilitar/inhabilitar exploradores de reenvío) y le proporciona la flexibilidad para especificar cualquiera de las opciones siguientes:
  - Inhabilitar el reenvío de tramas de explorador

    Esta opción inhabilita por completo el reenvío de tramas de explorador.
  - Reenviar tramas de explorador sólo a la conexión TCP local

    Si desea impedir que las tramas de explorador salgan en los enlaces de WAN, puede especificar esta opción. Éste es el valor por omisión para el Network Utility.
  - Reenviar tramas de explorador a todos los asociados DLSw

    Con esta opción, las tramas de explorador se envían a todos los asociados DLSw.

Para obtener una visión completa de los parámetros de configuración necesarios para el escenario de Receptor de LAN DLSw, consulte la Tabla 76 en la página 252.

Pasarela de canal de LAN DLSw

Este escenario se muestra en la Figura 44. Igual que en el escenario de receptor de LAN DLSw, el Network Utility termina las sesiones DLSw desde los direccionadores remotos. Sin embargo, en este caso, hay un Adaptador de canal ESCON en el Network Utility. En lugar de establecer puentes para el tráfico desde la función DLSw al segmento de LAN, esta configuración lo pasa directamente al canal a través de una interfaz de bucle de retorno LSA configurada en el Network Utility.

Esta configuración también demuestra el uso del Network Utility para soportar tráfico SNA del campus local al sistema principal. Este tráfico sale por un puente de la red troncal del campus a través de la interfaz de bucle de retorno LSA. Todos los dispositivos SNA de la red se configuran con la misma dirección MAC de destino de sistema principal que es la dirección MAC de la interfaz de bucle de retorno LSA. Esto incluye los dispositivos de la ubicación principal así como los dispositivos de las ubicaciones remotas.

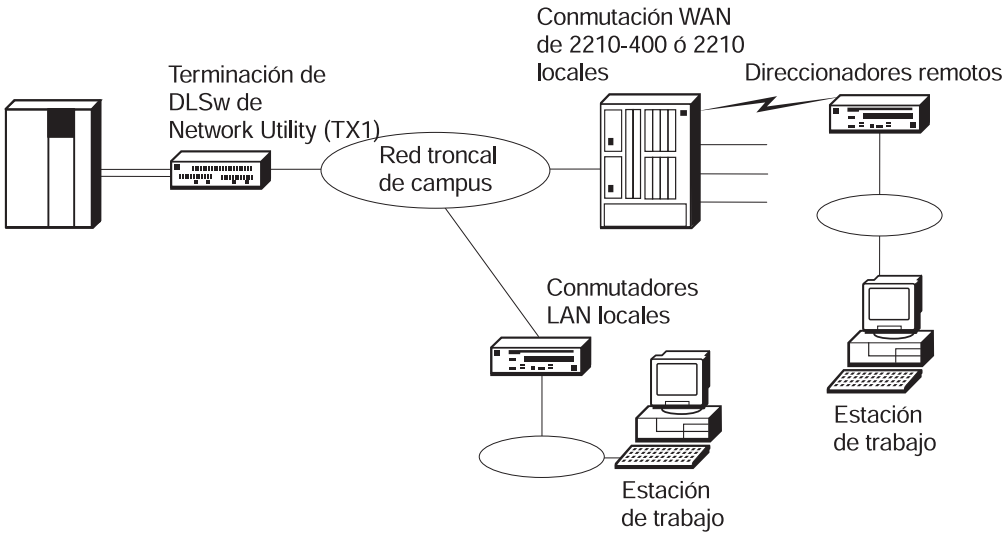


Figura 44. Pasarela de canal de LAN DLSw

Nota: Este ejemplo ilustra el uso del Network Utility como pasarela de canal sólo para el tráfico DLSw. Sin embargo, muchas de las funciones ilustradas en las configuraciones de ejemplo de Pasarela de canal de la página 208 pueden combinarse con la terminación DLSw en una configuración de pasarela de canal válida.

Claves para la configuración

Tenga en cuenta los puntos siguientes al configurar el Network Utility como Pasarela de canal de LAN DLSw:

- Se debe configurar una interfaz LSA y se debe habilitar el bucle de retorno en esta interfaz. La habilitación del bucle de retorno crea una LAN virtual en el Network Utility. Los dos únicos dispositivos de esta LAN son el sistema principal y el punto de terminación DLSw. Se define una dirección MAC en la interfaz LSA

que representa el sistema principal en el canal. Ésta es la dirección MAC de destino que se configura en los dispositivos de sentido directo.

Nota: También puede definir una conexión directa LSA para el tráfico que debe entrar por puentes desde los segmentos de LAN locales. Si realiza lo anterior, los dispositivos de estos segmentos tendrán una dirección MAC de destino diferente desde los dispositivos remotos porque la interfaz directa LSA tendrá una dirección MAC diferente de la interfaz de bucle de retorno LSA.

- Al configurar DLSw, necesita abrir los SPA SNA para la interfaz LSA así como la interfaz de Red en Anillo.
- La configuración de subcanal para la interfaz LSA debe coincidir con los parámetros configurados en el sistema principal. Consulte la Tabla 70 en la página 209 para obtener una descripción de los parámetros de subcanal y el "Capítulo 18. Definiciones de sistema principal de ejemplo" en la página 259 para ver definiciones de sistema principal de ejemplo. Esta información le ayudará a ver cómo se correlacionan estos parámetros.
- Necesita configurar una *conexión TCP local*. Esto se lleva a cabo definiendo un asociado DLSw cuya dirección IP sea la dirección interna del Network Utility. Ésta se utiliza para el tráfico que se coloca en puentes desde los segmentos de LAN locales hasta el sistema principal. Este tráfico se coloca en puentes en el Network Utility en DLSw donde la conexión TCP local pasa el tráfico a la interfaz de bucle de retorno LSA.
- El Network Utility soporta actualmente un máximo de 2048 estaciones de enlace por pareja dirección MAC/SAP (por ejemplo, una dirección MAC de destino de 400022AA0099 con el SAP 04). Si necesita más de 2048 estaciones de trabajo, tiene que definir otra interfaz LSA con un SAP diferente o una dirección MAC diferente. Recuerde que cada interfaz LSA necesita un subcanal de los 64 disponibles en un adaptador de canal ESCON. También deberá definir el nodo principal XCA correspondiente para soportar cada interfaz LSA.

Pasarela de canal X.25

Este escenario se muestra en la Figura 45 en la página 243. Utiliza DLSw local en el Network Utility para correlacionar entre direcciones X.25 y parejas de dirección MAC/SAP. El transporte a través de la WAN es QLLC (Qualified Logical Link Control) (Control de enlace lógico cualificado) nativo, un protocolo que permite a los dispositivos SNA comunicarse a través de redes X.25. En el Network Utility, DLSw local efectúa la conversión de protocolo entre las tramas QLLC y LLC2.

Desde la perspectiva de dispositivo remoto, hay dos casos a tener en cuenta:

1. Un dispositivo en un segmento de LAN conectado al direccionador de bifurcación

   En la estación de trabajo, la aplicación SNA genera una trama LLC que desea enviar al sistema principal. Si el direccionador de bifurcación es un IBM 2210, esta trama LLC se coloca en un puente en la función DLSw 2210, que realiza tres cosas:

   a. La conversión de protocolo de la trama LLC a una trama QLLC
   b. Correlaciona la pareja dirección MAC/SAP de destino con la dirección DTE (SVC) o LCN X.25 (PVC) apropiada
   c. Pasa la trama QLLC a X.25

La función PAD X.25 del direccionador de bifurcación crea los paquetes de capa de enlace LAPB y los envía a través de PVC (o SVC).

Si algún producto diferente del IBM 2210 hace el papel de direccionador de bifurcación, necesita efectuar estas mismas funciones pero puede hacerlo sin utilizar la DLSw local.

2. Un dispositivo directamente en la red X.25 (por ejemplo, una Unidad de control IBM 3174 o una máquina de pasarela eNetwork Communications Server conectada a través de un Adaptador de conector de área amplia)

   En estos dispositivos, SNA utiliza QLLC como tipo DLC nativo. Genera una trama QLLC y la envía a través del PVC (o SVC) configurado.

En cada uno de estos casos, en el Network Utility, los paquetes LAPB se reciben a través del circuito X.25 y se pasan a QLLC y luego a DLSw. DLSw realiza dos cosas:

1. La conversión de protocolo de QLLC a una trama LLC2
2. La correlación de dirección DTE (SVC) o LCN X.25 (PVC) en la dirección MAC/SAP para la interfaz de bucle de retorno local LSA

Entonces se pasa el tráfico a la interfaz de bucle de retorno LSA para el transporte a través del canal ESCON.

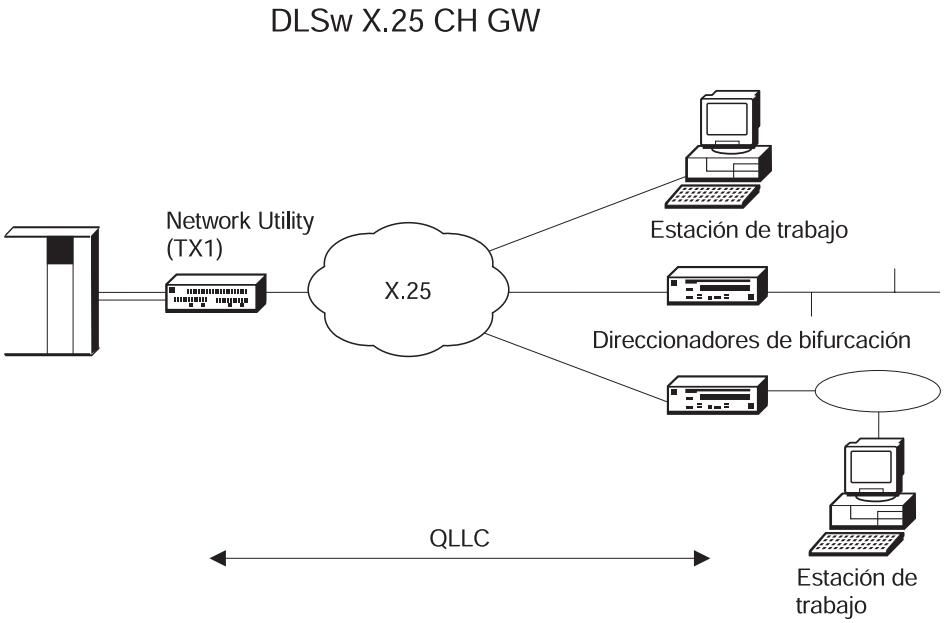


Figura 45. Pasarela de canal de DLSw X.25

Claves para la configuración

La lista siguiente resume las tareas generales de configuración que necesita efectuar para este escenario. Consulte las demás configuraciones de bucle de retorno LSA y DLSw para obtener detalles. La interfaz de bucle de retorno LSA se configura igual que en el apartado “Pasarela de canal de LAN DLSw” en la página 241.

- Añadir y configurar las interfaces ESCON y LSA.
- Añadir y configurar la interfaz X.25. Desde la línea de mandatos, utilice el mandato **net** de talk 6 para entrar en el subproceso Config de X.25 y, a continuación, utilice los mandatos siguientes:
  - **set address** (para establecer la dirección DTE local)

  - **add protocol dlsw** (para añadir DLSw como un protocolo X.25)
  - **add pvc** o **add svc** (añadir los PVC individuales o el rango de SVC)
- Configurar la dirección IP interna como en otros ejemplos.
- Configurar DLSw
  - Configurar DLSw general (habilitar, segmento SRB, reenviar exploradores localmente).
  - Configurar la conexión TCP local de DLSw.
  - Configurar DLSw para el bucle de retorno LSA (abrir SAP en la interfaz LSA).

Además de estas tareas generales, necesita configurar DLSw de Network Utility para correlacionar las direcciones X.25 con la dirección MAC del bucle de retorno LSA. Existen tres modos de efectuar dicha acción:

- Configurar las estaciones X.25 individualmente en DLSw, cada una con su propia dirección MAC de destino. Esta opción se aplica a los PVC y los SVC.
- Configurar una lista de ID de conexión, cada uno de los cuales tiene su propia dirección MAC de destino. Algunas estaciones X.25 pueden enviar un ID de conexión cuando efectúan una llamada y el Network Utility compara este valor con la lista configurada. Esta opción sólo se aplica a los SVC.
- Configurar una dirección MAC de destino por omisión para llamadas de entrada que no contienen un ID de conexión. Esta opción sólo se aplica a los SVC.

El resto de esta sección describe cómo configurar cada uno de estos tres métodos de correlación de dirección.

Si el número de las estaciones X.25 remotas es relativamente pequeño, puede configurar cada dispositivo X.25 remoto en DLSw para que se correlacione con la dirección MAC de bucle de retorno LSA. Para efectuar dicha acción utilizando la línea de mandatos, entre **talk 6** en el indicador * y escriba lo siguiente:

- **protocol dls**
  - **add qllc station** (una vez para cada estación X.25 remota). El sistema le solicita:
    - El número de interfaz (interfaz X.25)
    - PVC o SVC
    - El número de canal lógico (para PVC) o la dirección DTE (para SVC)
    - MAC y SAP de origen (puede generarlos DLSw)
    - MAC y SAP de destino (entre la dirección MAC de bucle de retorno LSA)
    - Tipo de PU
    - Bloque/número de XID (si el tipo de PU es 2)

Para efectuar esta acción utilizando el Programa de configuración, realice lo siguiente:

- Protocols/DLSw/Interfaces/Serial-X25/QLLC Stations
  - añada una estación QLLC (entre la misma información que más arriba)

Si las estaciones X.25 remotas pueden configurarse para enviar un ID de conexión cuando efectúan una llamada[21], puede configurar DLSw para correlacionar los valores de ID de conexión con las direcciones MAC de destino. Para efectuar dicha acción utilizando la línea de mandatos, entre **talk 6** en el indicador * y escriba lo siguiente:

- **protocol dls**
  - **add qllc destination** (una vez para cada ID de conexión válido). El sistema le solicita:
    - ID de conexión

21. Los productos QLLC presentan con frecuencia este parámetro como una contraseña de conexión.

- MAC y SAP de destino (entre la dirección MAC de bucle de retorno LSA)

Para efectuar esta acción utilizando el Programa de configuración, realice lo siguiente:
- Protocols/DLSw/QLLC Destinations
  – añada un destino QLLC (entre la misma información que más arriba)

Finalmente, si no es factible configurar cada estación X.25 remota o utilizar un ID de conexión, puede utilizar la característica de DLSw ANYCALL para aceptar cualquier llamada X.25 de entrada y correlacionarla con la dirección MAC de bucle de retorno LSA. Para efectuar dicha acción utilizando la línea de mandatos, entre **talk 6** en el indicador * y escriba lo siguiente:
- **protocol dls**
  – **add qllc destination** (una vez más puede añadir los ID de conexión específicos si lo desea). El sistema le solicita:
    - El ID de conexión (utilice la palabra 'ANYCALL')
    - MAC y SAP de destino (entre la dirección MAC de bucle de retorno LSA)

Para efectuar esta acción utilizando la herramienta de configuración, realice lo siguiente:
- Protocols/DLSw/QLLC Destinations
  – añada un destino QLLC (entre la misma información que más arriba)

Gestión de DLSw

Esta sección presenta algunos de los modos en que puede supervisar y gestionar la función DLSw.

Supervisión de la línea de mandatos

DLSw soporta un amplio conjunto de mandatos para visualizar el estado, modificar dinámicamente parámetros de configuración y controlar de forma activa el estado de las conexiones. Estos mandatos se describen detalladamente en la publicación *MAS Consulta de configuración y supervisión de protocolos Volumen 1*, en el capítulo ″Configuring and Monitoring DLSw″. Para acceder a ellos, entre **talk 5** en el indicador * y **protocol dls** en el indicador +.

Algunos mandatos especialmente útiles para supervisar el estado son:

list tcp sess
: Muestra el estado de todas las conexiones TCP conocidas a los direccionadores asociados. Puede ver el estado de las conexiones TCP a medida que se activan y desactivan, así como el nivel del protocolo DLSw en uso y estadísticas de resumen sobre el número de circuitos DLSw que utilizan cada conexión. Si configura DLSw para aceptar conexiones TCP sólo desde asociados dinámicos (no configurados), este mandato visualiza el estado de las conexiones como las han iniciado los direccionadores remotos. No habrá ningún estado si los direccionadores remotos no están arrancando activamente las conexiones TCP.

  Si configura una ″conexión TCP local″ para habilitar la función DLSw local, esta conexión se indica como tal en la salida del mandato para que pueda distinguirse de las conexiones asociadas remotas.

list dls sess all
: Muestra el estado de todas la sesiones DLSw activas. Una sesión, también denominada circuito, se define mediante un cuádruple de dirección MAC y SAP y corresponde a un enlace SNA, no a una sesión LU-LU SNA.

Normalmente las estaciones finales SNA activan y desactivan las sesiones, de modo que la salida de este mandato es dinámica. Para cada sesión, se ven las direcciones MAC y SAP de identificación, el estado, el asociado a través del cual está conectada la sesión y un identificador que se puede utilizar con el mandato **list dls sess detail** para obtener más información. Las sesiones DLSw locales (las que sólo incluyen este direccionador) se muestran como dos líneas de salida de este mandato.

Dado que un Network Utility puede tener fácilmente cientos o miles de sesiones activas, puede utilizar diferentes variaciones del mandato **list dls session** para visualizar sólo un subconjunto de ellas. En lugar de la palabra clave ″all″, utilice palabras clave diferentes para mostrar sólo los circuitos a través de un asociado determinado o sólo aquéllos que están en un estado determinado, etc. Existen aproximadamente 10 palabras claves definidas para seleccionar sesiones. La salida de todos estos mandatos hace una pausa cuando la pantalla se llena, esperando a que se pulse una tecla para continuar o salir. Pulse la barra espaciadora para ver la siguiente pantalla de salida.

list dls mem
Muestra el estado de varias agrupaciones de memoria DLSw, así como el estado de congestión de memoria para todas las sesiones activas.

list llc sess all
Muestra información de estado específica de LLC 802.2 para todas las sesiones DLSw que utilizan LLC como protocolo entre el direccionador y la estación final. Éstas incluyen sesiones que se ejecutan a través de LAN, canal, ATM e interfaces WAN colocadas en puentes remotos. La salida del mandato incluye más información de estado así como la ruta de origen a la estación final, si es aplicable.

list sdlc sess all
Muestra información de estado específica de SDLC para todas las sesiones DLSw que utilizan SDLC como protocolo entre el direccionador y la estación final. La salida del mandato incluye información de direccionamiento SDLC así como información de estado. Si está trabajando con dispositivos SDLC, este mandato es más útil que el mandato genérico **list dls sess**.

list qllc sess
Muestra información de estado específica de QLLC para todas las sesiones DLSw que utilizan QLLC a través de X.25 como protocolo entre el direccionador y la estación final. La salida del mandato incluye información de direccionamiento QLLC así como información de estado detallada. Dado que el direccionador soporta SVC dinámicos de entrada, este mandato es esencial para ver el estado de los PVC y los SVC QLLC configurados y dinámicos.

DLSw soporta la modificación dinámica bajo talk 5 de la inmensa mayoría de parámetros que se pueden configurar bajo talk 6. DLSw sigue el modelo estándar donde los cambios efectuados bajo talk 5 tienen un efecto inmediato pero no sobreviven a un rearranque del sistema, mientras que los cambios efectuados bajo talk 6 sólo tienen efecto después de un rearranque del sistema. Los mandatos de talk 5 **list** muestran los valores que están actualmente activos en el producto en ejecución.

Los mandatos de talk 5 **delete** y **disable** le proporcionan la posibilidad de romper una conexión DLSw existente. Por ejemplo, puede utilizar **delete dls** *número*

sesión para borrar una sesión que se ha colgado y permitir a las estaciones finales volverla a activar. Las secuencias **delete/add** y **disable/enable** son métodos potentes para reciclar conexiones TCP, SDLC y QLLC configuradas.

Soporte de anotación cronológica de sucesos

DLSw tiene definidos varios cientos de mensajes ELS, desde mensajes informativos acerca de sucesos normales hasta avisos de condiciones de error graves. He aquí algunos de los tipos de sucesos DLSw que pueden generar mensajes ELS:

- Errores de inicialización y configuración
- Tramas de conexión TCP de asociado o de posibilidades enviadas o recibidas
- Tramas de explorador enviadas o recibidas para una dirección MAC determinada o nombre NetBIOS
- Tramas de definición/desactivación de circuito enviadas o recibidas
- Tramas de definición/desactivación de enlace DLC enviadas o recibidas
- Tramas de datos enviadas o recibidas en circuitos activos
- Cambios de ventana de ritmo en circuitos activos
- Errores de asignación de memoria
- Flujos de protocolo inesperados, tramas descartadas
- Flujos de tramas que no coinciden con la configuración

Aunque estos mensajes los utilizan principalmente los técnicos de software para resolver problemas, un usuario con conocimientos básicos del protocolo DLSw y de los flujos de activación de enlaces DLC deberá poder encontrarles sentido y depurar errores de configuración simples. Mediante la activación de estos mensajes ELS y la observación de la salida a través de talk 2, podrá al menos responder a la pregunta ″¿Sucede alguna cosa?″

″DLS″ es uno de los *subsistemas* con nombre dentro de ELS. Para activar el conjunto estándar de mensajes de error, escriba **disp sub dls** desde el menú de sucesos bajo talk 6 o talk 5. Para activar todos los mensajes DLSw, entre **disp sub dls all**. Los mandatos correspondientes para desactivar mensajes empiezan con **nodisp**. Para obtener información general sobre cómo controlar y ver los mensajes ELS, consulte el apartado “Supervisión de mensajes de sucesos” en la página 92.

Si está intentando rastrear un intento de activación de enlace, puede que los mensajes DLSw solos no le muestren la imagen completa. Puede activar los mensajes ELS para el tipo de DLC subyacente del modo siguiente:

LLC disp sub llc all
SDLC disp sub sdlc all
QLLC disp sub qllc all disp sub x253 all (capa 3 de X.25, la capa de paquete)
LSA de canal
disp sub lsa all

Consulte la publicación *Guía de mensajes del sistema para el registro cronológico de sucesos* (en CD-ROM y la página Web del 2216) para obtener una lista completa de mensajes individuales y su significado.

Soporte de gestión SNA

Desde una consola de operador VTAM o NetView/390, puede controlar los enlaces, la PU y las LU implicadas con DLSw como se describe en el apartado “NetView/390” en la página 102.

A diferencia de APPN, DLSw de Network Utility no envía alertas SNA. Envía trampas (descritas en la sección siguiente) y desencadena mensajes ELS que pueden generar trampas. Puede utilizar los productos mencionados en el apartado “IBM Nways Manager para AIX” en la página 99 para convertir dichas trampas en alertas.

Soporte de trampas y MIB SNMP

DLSw de Network Utility proporciona soporte completo de sólo lectura y soporte parcial de lectura-grabación para la MIB DLSw estándar de IETF documentada en RFC 2024. Esta gran MIB proporciona visibilidad a la mayoría de información importante de configuración, estado y contabilidad que deben tener los productos que implementan RFC 1795 y 2166. Esta información incluye:

- Configuración
  - Características de nodo, por ejemplo se habilitan los asociados dinámicos
  - Información de asociados configurados
  - Entradas de directorio/antememoria configuradas
- Estado
  - Nodo activo o inactivo, duración
  - Conexiones TCP activas, duración, información de asociado dinámico
  - Información de directorios/antememoria dinámica
  - Circuitos activos, duración, información de DLC
- Estadísticas y contabilidad
  - Cuentas de conexiones TCP activas e inactivas (normales y erróneas)
  - Cuentas de tramas de datos y control por asociado
  - Cuentas de circuitos activos e inactivos
  - Índices en MIB DLC subyacentes para cuentas de tramas por circuito
  - Cuentas de ritmo para circuitos activos

DLSw de Network Utility soporta todas las trampas definidas en el RFC 2024, informando sobre los sucesos siguientes:

- Se termina una conexión TCP debido a una anomalía de intercambio de posibilidades o una violación de protocolo DLSw
- Se activa o desactiva una conexión TCP
- Se activa o desactiva un circuito

La totalidad de DLSw soporta elementos de datos de control de trampa de modo que una estación de gestión puede establecer las condiciones bajo las que se genera una trampa.

Además del RFC 2024, DLSw de Network Utility soporta extensiones MIB DLSw específicas de IBM para grupos basados en IP de multidistribución y para estaciones QLLC.

Soporte de aplicación de gestión de red

La aplicación basada en Java de Network Utility implementada en los productos de Nways Manager descritos en el apartado “Productos IBM Nways Manager” en la página 98 proporciona soporte integrado para las extensiones MIB DLSw estándares y MIB DLSw específicas de IBM.

Para ver los recursos DLSw y su estado utilizando estos productos, se arrancan paneles específicos que presentan información clave de la MIB DLSw y de las MIB subyacentes de la capa DLC (LLC, SDLC o X.25). También puede utilizar soporte de navegador integrado para ver la información en cualquiera de estas MIB.

Puede controlar la emisión de trampas DLSw desde los productos de Nways Manager, para que una trampa determinada se genere siempre, nunca o sólo bajo determinadas condiciones.

Nways Manager para AIX puede mostrarle una vista de topología de DLSw de la red, incluyendo la conectividad DLSw, los recursos y el estado codificado en color. La topología se renueva a medida que se descubren nodos nuevos. Esta aplicación no presenta la topología de grupos de multidistribución DLSw IP.

Capítulo 17. Detalles de configuración de ejemplo de DLSw

Este capítulo contiene diagramas y tablas de parámetros de configuración para varias de las configuraciones de red DLSw de ejemplo del “Capítulo 16. Conmutación de enlace de datos” en la página 237. Los valores de parámetros mostrados proceden de configuraciones de prueba de trabajo reales.

Para obtener una explicación de las columnas y los convenios de las tablas de parámetros de configuración, consulte el apartado “Convenios de las tablas de configuración de ejemplo” en la página 131.

Las páginas World Wide Web de Network Utility contienen archivos de configuración binarios que coinciden con estas tablas de parámetros de configuración. Para acceder a estos archivos, siga el enlace Download desde:

```
http://www.networking.ibm.com/networkutility
```

Las configuraciones documentadas en este capítulo son:

Tabla 75. Referencia cruzada de información de configuraciones de ejemplo

Descripción de la configuración	Tabla de parámetros
“Receptor de LAN DLSw” en la página 239	Tabla 76 en la página 252
“Pasarela de canal de LAN DLSw” en la página 241	Tabla 77 en la página 255

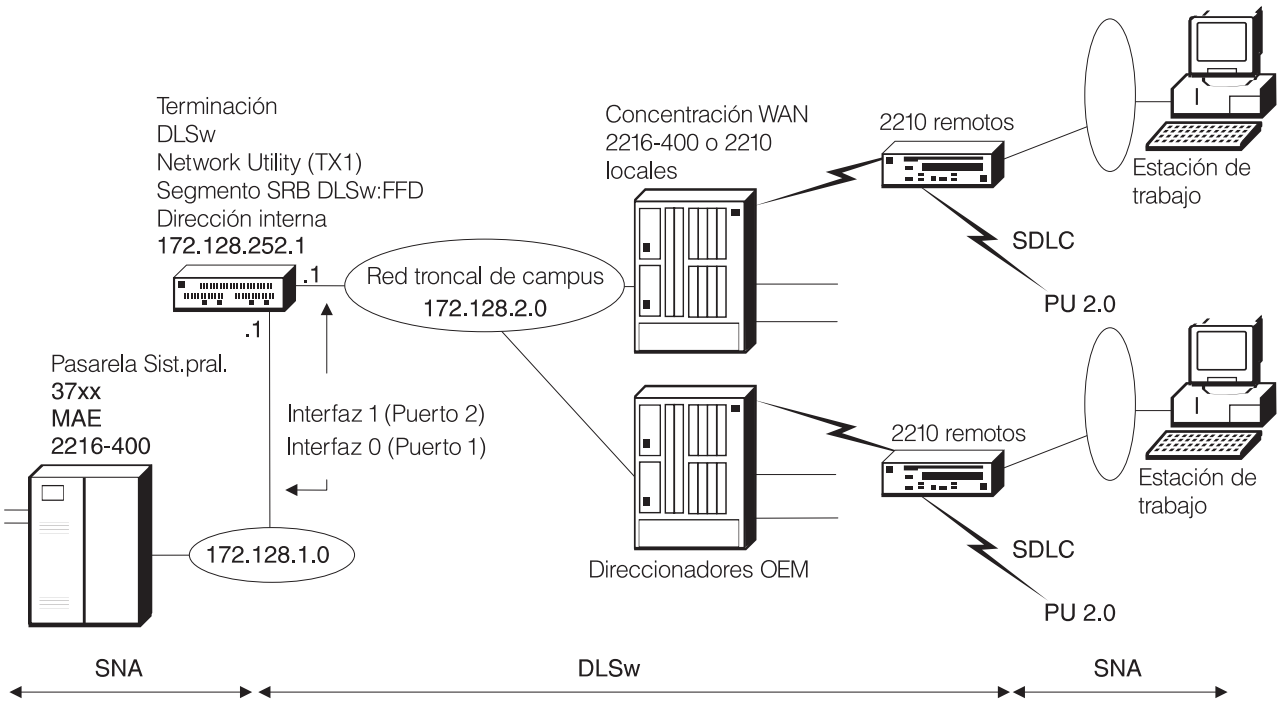


Figura 46. Receptor de LAN DLSw

Tabla 76. Receptor de LAN DLSw. Consulte la página 239 para obtener una descripción y la página 251 para ver un diagrama de esta configuración.

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Dispositivos Adaptadores Ranuras	Ranura 1: TR de 2 puertos	Ver ″add device″ en la fila siguiente	1
Dispositivos Adaptadores Puertos	Ranura 1/Puerto 1: Interf. 0: TR Ranura 1/Puerto 2: Interf. 1: TR	Config>**add dev tok** (una vez por puerto)	2
Dispositivos Interfaces	Interfaz 0 Dirección MAC: 400022AA0001 Tamaño de paquete: 4399 Interfaz 1 Dirección MAC: 400022AA0002 Tamaño de paquete: 4399	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:01** TKR config>**packet 4399** TKR config>**exit** Config>**net 1** TKR config>**set phy 40:00:22:AA:00:02** TKR config>**packet 4399**	
Sistema General	Nombre de sistema: NU_A Ubicación: XYZ Contacto: Administrador	Config>**set host** Config>**set location** Config>**set contact**	
Sistema SNMP Config General	SNMP (seleccionado)	Config>**p snmp** SNMP Config>**enable snmp**	
Sistema SNMP Config Comunidades General	Nombre de comunidad: admin Tipo acceso: Trampa lect.-grab. Vista de comunidad: Toda	SNMP Config>**add community** SNMP Config>**set comm access write**	3
Protocolos IP General	Dirección interna: 172.128.252.1 ID de direccionador: 172.128.1.1	Config>**p ip** IP config>**set internal** IP config>**set router-id**	
Protocolos IP Interfaces	Interf. 0 (TR ranura 1 puerto 1) Dirección IP: 172.128.1.1 Másc. subred: 255.255.255.0 Interf. 1 (TR ranura 1 puerto 2) Dirección IP: 172.128.2.1 Másc. subred: 255.255.255.0	IP config>**add address** (una vez por i/f)	4
Protocolos IP OSPF General	OSPF (seleccionado)	Config>**p ospf** OSPF Config>**enable ospf**	5
Protocolos IP OSPF Config. de área General	Número de área: 0.0.0.0 Área apéndice (no seleccionada)	OSPF Config>**set area**	
Protocolos IP OSPF Interfaces	Interfaz 0 OSPF (seleccionado) Interfaz 1 OSPF (seleccionado)	OSPF Config> **set interface** Interface IP address **172.128.1.1** Attaches to area **0.0.0.0** (Aceptar otros valores por omisión) OSPF Config>**set interface** Interface IP address **172.128.2.1** Attaches to area **0.0.0.0** (Aceptar otros valores por omisión)	

Tabla 76. Receptor de LAN DLSw (continuación). Consulte la página 239 para obtener una descripción y la página 251 para ver un diagrama de esta configuración.

Nav. por prog. de conf.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Protocolos DLSw General General	DLSw (seleccionado) Segmento SRB: FFD Reenv. exploradores: inhabilitado	Config>**p dls** DLSw Config>**enable dls** DLSw Config>**set srb** DLSw Config>**disable forward all**	6
Protocolos DLSw General Vecinos dinámicos	Vecinos dinámicos (seleccionado)	DLSw Config>**enable dynamic**	7
Protocolos DLSw Interfaces	Interfaz 0 (TR ranura 1 puerto 1) Tipo SAP: SNA (SAP 0,4,8,C)	DLSw Config>**open 0 sna**	8
Protocolos Puentes General	Puentes (seleccionado) DLSw (seleccionado)	Config>**p asrt** ASRT config>**enable br** ASRT config>**enable dls**	9
Protocolos Puentes Interfaces	Interfaz 0 (TR ranura 1 puerto 1) Puerto de puentes (selecc.) Soportes de interfaz: SRB Número de segmento: 001 Tamaño de MTU: 4399	(se supone 'enable br') ASRT config>**disable transp 1** ASRT config>**enable source 1** ASRT config>**delete port 2**	10

Notas:

1. **add dev** define un solo puerto, no un adaptador.
2. El programa de configuración asigna automáticamente un número de interfaz a todos los puertos de un adaptador y el usuario suprime los que no desea utilizar. Desde la línea de mandatos, escriba el mandato **add dev** para cada puerto que desee utilizar y el número de interfaz (también conocido como ″número de red″) es la salida del mandato.
3. Sólo necesita una comunidad SNMP con capacidad para grabación si desea bajar archivos de configuración directamente del programa de configuración al direccionador. SNMP no es necesario para enviar mediante TFTP un archivo de configuración al direccionador.
4. Sólo es necesario configurar la interfaz 1 para que IP para DLSw funcione correctamente en este ejemplo. La interfaz 0 se configura aquí para IP, únicamente para realizar la gestión del sistema.
5. También puede utilizar RIP en lugar de OSPF.
6. Inhabilitamos el reenvío de exploradores remotos como filtro general, para evitar que el tráfico LAN de red troncal genere mensajes de búsqueda DLSw en los enlaces WAN en ubicaciones remotas. Esto significa que todos los circuitos deben iniciarlos los direccionadores remotos. Si la red necesita que el sistema principal pueda iniciar las conexiones fuera en las ubicaciones remotas, cambie este parámetro por ″reenviar a todos los iguales DLSw″.

   Si los direccionadores remotos son direccionadores de IBM, puede configurarlos individualmente para controlar qué mensajes de búsqueda desean recibir, utilizando la dirección MAC y las listas de nombres de NetBIOS. También puede configurar si cada uno arrancará su conexión TCP en Network Utility siempre o la desactivará cuando no la utilice, utilizando el parámetro *connectivity setup type*.
7. Tener vecinos dinámicos habilitados es el valor por omisión, de modo que no tiene que cambiar este panel o emitir este mandato. Aquí lo mostramos para hacer notar que éste es el parámetro que permite a los asociados (vecinos) DLSw remotos establecer conexiones TCP con este Network Utility sin que se tengan que definir aquí las direcciones IP. Cada direccionador remoto necesita configurarse con la dirección IP interna (172.128.252.1) de este Network Utility como su dirección asociada.
8. No es necesario abrir los SAP en la Interfaz 1 puesto que esta interfaz sólo transporta tráfico IP y no tráfico LLC.
9. ″enable br″ crea automáticamente los puertos de puente TB para ambas interfaces de Red en Anillo. Los números de puertos de puente son 1 y 2 y son independientes de los números de puerto de adaptador.
10. Los mandatos disable y enable cambian el puerto de puente 1 de TB a SRB. El mandato ″delete port″ desactiva los puentes en la interfaz 1 (puerto de puente 2). Se necesitarían puentes en esta interfaz si fuera necesario soportar puentes de tráfico de estación final local desde la Red troncal de campus al sistema principal.

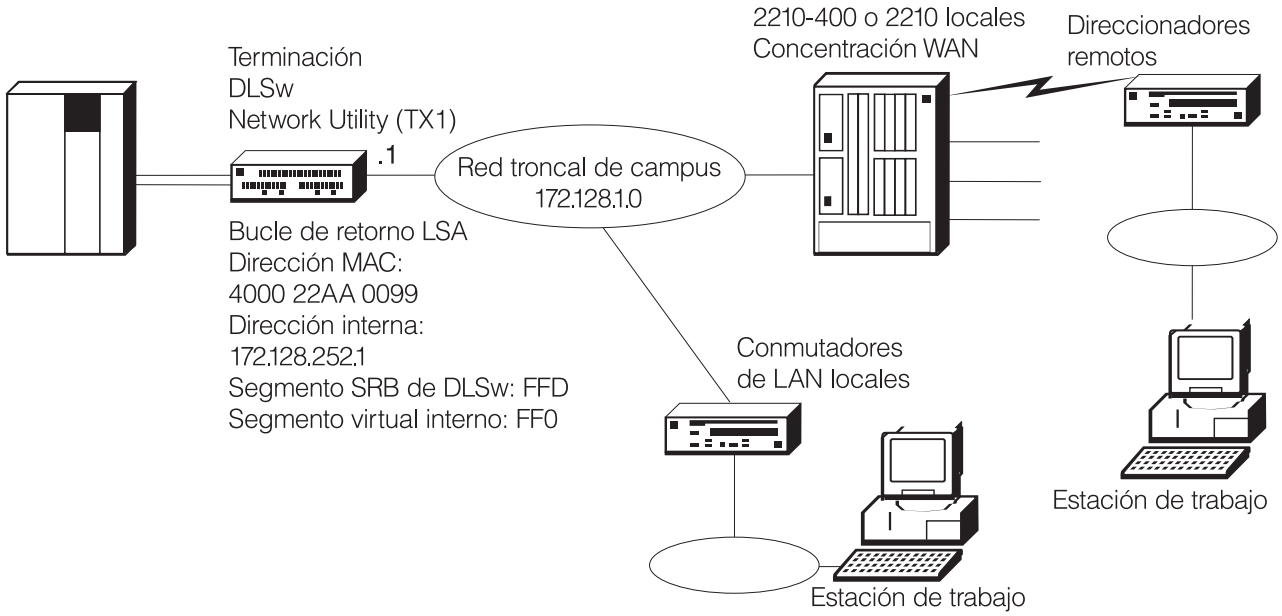


Figura 47. Pasarela de LAN DLSw

Tabla 77. Pasarela de LAN DLSw. Consulte la página 241 para obtener una descripción y la página 255 para ver un diagrama de esta configuración.

Nav. por prog. de confi.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Dispositivos Adaptadores Ranuras	Ranura 1: TR de 2 puertos Ranura 2: ESCON	Ver ″add device″ en la fila siguiente	1
Dispositivos Adaptadores Puertos	Ran. 1/Puerto 1: Interf. 0: TR Ran. 2/Puerto 1: Interf. 1: ESCON	Config>**add dev tok** Config>**add dev escon**	2
Dispositivos Interfaces	Interfaz 0 Dirección MAC: 400022AA0001	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:01**	
Dispositivos Adaptadores de canal Interfaces ESCON Interfaces ESCON	Número de red base: 1 Tipo de protocolo: LSA (realizar esto en primer lugar) Bucle de retorno (seleccionado - realizar esto en segundo lugar) Tipo de LAN: Red en Anillo Tramas de datos máxima: 2052 Dirección MAC: 400022AA0099	Config>**net 1** ESCON Config>**add lsa** (añadida como interfaz 2) ESCON Add Virtual>**enable loopback** ESCON Add Virt.>**mac 40:00:22:AA:00:99** ESCON Add Virtual>**lan tok** ESCON Add Virtual>**maxdata 2052** (cont. en misma sesión con fila sig.)	3
Dispositivos Adaptadores de canal Interfaces ESCON Subcanales ESCON	Interf. 2, Red base 1, Prot. LSA Dirección de dispositivo: E4 Tipo de subcanal: lect./grab. Dirección de enlace: EF	ESCON Add Virtual>**subchannel add** (continuación) ESCON Add LSA Subchannel>**device E4** ESCON Add LSA Subchannel>**link EF** (Escribir **exit** dos veces y luego **list all**)	
Sistema General	Nombre de sistema: NUA_SC1C Ubicación: XYZ Contacto: Admin	Config>**set host** Config>**set location** Config>**set contact**	

Tabla 77. Pasarela de LAN DLSw (continuación). Consulte la página 241 para obtener una descripción y la página 255 para ver un diagrama de esta configuración.

Nav. por prog. de confi.	Valores de programa de config.	Mandatos de la línea de mandatos	Not.
Sistema SNMP Config General	SNMP (seleccionado)	Config>**p snmp** SNMP Config>**enable snmp**	
Sistema SNMP Config Comunidades General	Nombre de comunidad: admin Tipo acceso: Trampa lect.-grab. Vista de comunidad: Toda	SNMP Config>**add community** SNMP Config>**set comm access write**	4
Protocolos IP General	Dirección interna: 172.128.252.1 ID de direccionador: 172.128.1.1	Config>**p ip** IP config>**set internal** IP config>**set router-id**	
Protocolos IP Interfaces	Interf. 0 (TR ranura 1 puerto 1) Dirección IP: 172.128.1.1 Másc. subred: 255.255.255.0	IP config>**add address**	
Protocolos IP OSPF General	OSPF (seleccionado)	Config>**p ospf** OSPF Config>**enable ospf**	5
Protocolos IP OSPF Config. de área General	Número de área: 0.0.0.0 Área apéndice (no seleccionada)	OSPF Config>**set area**	
Protocolos IP OSPF Interfaces	Interfaz 0 OSPF (seleccionado)	OSPF Config>**set interface** Interface IP address **172.128.1.1** Attaches to area **0.0.0.0** (Aceptar otros valores por omisión)	
Protocolos DLSw General General	DLSw (seleccionado) Segmento SRB: FFD Reenv. expl.: sólo con. TCP local	Config>**p dls** DLSw Config>**enable dls** DLSw Config>**set srb** DLSw Config>**enable forward local**	6
Protocolos DLSw General Vecinos dinámicos	Vecinos dinámicos (seleccionado)	DLSw Config>**enable dynamic**	7
Protocolos DLSw Conexiones TCP	(añadir) Direcc. IP vecino: 172.128.252.1 (dir. IP interna del direccion.)	DLSw Config>**add tcp** DLSw neighbor IP addr.: **172.128.252.1** (Aceptar otros valores por omisión)	8
Protocolos DLSw Interfaces	Interfaz 0 (TR ranura 1 puerto 1) Tipo SAP: SNA (SAP 0,4,8,C) Interfaz 2 (ESCON-LSA) Tipo SAP: SNA (SAP 0,4,8,C)	DLSw Config>**open 0 sna** DLSw Config>**open 2 sna**	9
Protocolos Puentes General	Pestaña General: Puentes (seleccionado) DLSw (seleccionado) Pestaña SRB: Segmento virtual interno: FF0	Config>**p asrt** ASRT config>**enable br** ASRT config>**enable dls**	10
Protocolos Puentes Interfaces	Interfaz 0 (TR ranura 1 puerto 1) Puerto de puentes (selecc.) Soportes de interfaz: SRB Número de segmento: 001 Tamaño de MTU: 2052	(se supone 'enable br') ASRT config>**disable transp 1** ASRT config>**enable source 1**	11

Notas:

1. **add dev** define un solo puerto, no un adaptador.
2. El programa de configuración asigna automáticamente un número de interfaz a todos los puertos de un adaptador y el usuario suprime los que no desea utilizar. Desde la línea de mandatos, escriba el mandato **add dev** para cada puerto que desee utilizar y el número de interfaz (también conocido como ″número de red″) es la salida del mandato.
3. La dirección MAC que representa esta interfaz de bucle de retorno LSA es la dirección MAC de destino que todas las estaciones finales de la red DLSw utilizan para alcanzar el sistema principal a través de este Network Utility.
4. Sólo necesita una comunidad SNMP con capacidad para grabación si desea bajar archivos de configuración directamente del programa de configuración al direccionador. SNMP no es necesario para enviar mediante TFTP un archivo de configuración al direccionador.
5. Puede elegir utilizar RIP en lugar de OSPF.
6. Habilitamos el reenvío local para permitir a las estaciones finales del campus local alcanzar el sistema principal. Inhabilitamos el reenvío de exploradores remotos como filtro general, para evitar que el tráfico LAN de red troncal genere mensajes de búsqueda DLSw en los enlaces WAN en ubicaciones remotas. Esto significa que todos los circuitos remotos deben iniciarlos los direccionadores remotos. Si la red necesita que el sistema principal pueda iniciar las conexiones fuera en las ubicaciones remotas, cambie este parámetro por ″reenviar a todos los iguales DLSw″.

   Si los direccionadores remotos son direccionadores de IBM, puede configurarlos individualmente para controlar qué mensajes de búsqueda desean recibir, utilizando la dirección MAC y las listas de nombres de NetBIOS. También puede configurar si cada uno arrancará su conexión TCP en Network Utility siempre o la desactivará cuando no la utilice, utilizando el parámetro *connectivity setup type*.
7. Tener vecinos dinámicos habilitados es el valor por omisión, de modo que no tiene que cambiar este panel o emitir este mandato. Aquí lo mostramos para hacer notar que éste es el parámetro que permite a los asociados (vecinos) DLSw remotos establecer conexiones TCP con este Network Utility sin que se tengan que definir aquí las direcciones IP. Cada direccionador remoto necesita configurarse con la dirección IP interna (172.128.252.1) de este Network Utility como su dirección asociada.
8. La adición de la dirección IP interna como vecino es necesaria para permitir a DLSw llevar el tráfico de la interfaz ESCON/LSA a la LAN de red troncal.
9. Los SAP se abren en la Interfaz 0 para permitir el flujo LLC en los conmutadores de LAN locales y no son necesarios para que la DLSw remota funcione.
10. ″enable br″ crea automáticamente un puerto de puente TB para la interfaz de Red en Anillo. El número de puerto de puente es 1 y es independiente de los números de puerto de adaptador y de los números de interfaz de sistema.
11. Los mandatos disable y enable cambian el puerto de puente 1 de TB a SRB. Los puentes son necesarios en esta interfaz para soportar que el tráfico de estación final local se repita en bucle a través de DLSw desde la Red troncal de campus al sistema principal.

Capítulo 18. Definiciones de sistema principal de ejemplo

Este capítulo contiene ejemplos de definiciones de sistema principal para el Network Utility en las configuraciones utilizadas en este manual.

Específicamente, se presentan definiciones para los entornos siguientes:
- LSA
- LCS
- MPC+

Adicionalmente, se resaltan las diferencias entre un Network Utility con un adaptador de canal ESCON y un adaptador de canal paralelo.

Para obtener más información sobre la definición de Network Utility en el sistema principal, consulte la publicación *IBM 2216 Nways Multiaccess Connector Guía del usuario de software*, SC30-3886.

Visión general

Existen tres pasos para definir un Network Utility conectado a canal en el sistema principal:

1. Definir el Network Utility en el subsistema de canal de sistema principal

   Esto se efectuará desde el programa de configuración de E/S (IOCP) o la Definición de configuración de hardware (HCD), en función de la versión de MVS. (HCD necesita MVS/ESA SP versión 4.2 o posterior con el número de APAR OY67361.)

   Las sentencias de definición son ligeramente diferentes para un dispositivo conectado a canal ESCON que para un dispositivo conectado a canal paralelo. En el apartado “Definiciones de IOCP de sistema principal de ejemplo” en la página 260 se proporciona un ejemplo de estas definiciones.
2. Definir el Network Utility como una unidad de control en el sistema operativo del sistema principal

   Para la mayoría de los sistemas, las definiciones son las mismas para un adaptador ESCON que para un adaptador de canal paralelo. Obviamente, dependen del sistema operativo que se esté utilizando. En el apartado “Definición del Network Utility en el sistema operativo” en la página 263 se proporciona un ejemplo de estas definiciones.
3. Definir el Network Utility en el TCP/IP o VTAM de sistema principal

   Estas definiciones dependen de si se está definiendo una interfaz LSA (SNA), LCS (TCP/IP) o MPC+ (SNA y/o TCP/IP) en el Network Utility. La sección “Definiciones de VTAM” en la página 264 muestra ejemplos de las definiciones de VTAM necesarias. La sección “Definiciones IP de sistema principal” en la página 270 muestra ejemplos de las definiciones de TCP/IP necesarias.

Definiciones a nivel de subsistema de canal

Las definiciones a este nivel se realizan a través del IOCP o con HCD. Si HCD está disponible, es aconsejable que lo utilice. HCD ofrece un método mejorado de definición de configuración de hardware del sistema. Con HCD se pueden llevar a cabo varios pasos complejos necesarios para entrar datos de configuración de hardware utilizando un diálogo interactivo. Este capítulo sólo presenta las macros IOCP que se generarán desde HCD.

Definiciones de IOCP de sistema principal de ejemplo

En la Figura 48 se muestra un ejemplo de las definiciones necesarias en el IOCP (Programa de configuración de E/S) de sistema principal para un Network Utility configurado con un adaptador ESCON.

```
CHPID                PATH=((05)),TYPE=CNC
CNTLUNIT             CUNUMBR=1E0,PATH=05,CUADD=0,
                     UNITADD=((E0,32)),LINK=3C,UNIT=3172
IODEVICE             UNIT=3172,ADDRESS=((1E0,32)),
                     CUNUMBR=1E0
```

Figura 48. Definiciones de IOCP de sistema principal de ejemplo para el Network Utility (ESCON)

Las secciones siguientes describen las macros IOCP que necesita para definir el Network Utility en el sistema principal.

Sentencia RESOURCE

Ésta identifica las particiones lógicas (LPAR) de sistema principal por nombre y número. Esta sentencia no existe si el sistema principal no está particionado *como es el caso en el ejemplo anterior.*

- PART=((nombre1,x),(nombre2,y)...(nombreX,z))

  El nombre identifica la LPAR y se utiliza en el resto de la definición de vía de canal. El número es el número de LPAR correspondiente. El número de LPAR se utiliza al definir el subcanal en el Network Utility. Si el sistema principal no está particionado, el número de LPAR es siempre 0.

Sentencia de ID de vía de canal (CHPID)

El CHPID identifica el tipo de conexión de canal y a la persona que la utiliza.

- PATH=x

  Identifica de forma exclusiva la vía de canal. Este valor se denomina con frecuencia ″Número de CHPID″.

- TYPE=CNC

  Indica que el canal es un canal ESCON. El tipo de canal es CNC para ESCON y BL para multiplexor de bloques (Adaptador de canal paralelo).

- SWITCH=x

  Identifica qué Direccionador ESCON está en esta vía. Si no se está utilizando ningún direccionador, se omite este parámetro.

- SHARED

  Indica que el CHPID pueden utilizarlo varias LPAR simultáneamente. Si no existe, sólo una LPAR puede utilizar el CHPID a la vez.

- PARTITION=(nombre1,nombre2,...,nombreX)

  Es un formato del parámetro PARTITION y contiene una lista de acceso de LPAR que indica qué particiones tienen acceso a este canal. Los nombres deben incluirse en la sentencia RESOURCE.

- PARTITION=((nombre1,...,nombreX),(nombre2,...,nombreY))

  Es el otro formato del parámetro PARTITION. En este formato, la primera agrupación de nombres es la lista de acceso de LPAR, como más arriba. La segunda agrupación es la lista de LPAR candidatas que un operador puede configurar para tener acceso al canal. La segunda agrupación tendrá como mínimo las mismas LPAR que la primera agrupación y también puede especificar LPAR adicionales.

Sentencia de unidad de control (CNTLUNIT)

Esta sentencia, junto con la sentencia IODEVICE, define la vía desde el sistema principal al Network Utility. Las sentencias CNTLUNIT e IODEVICE se producen en parejas. Si se están definiendo múltiples LPAR para utilizar un solo CHPID, tiene que haber una sentencia CNTLUNIT e IODEVICE para cada LPAR.

- CUNUMBR=x

  Es un identificador para la definición de unidad de control.

- PATH=x

  Este número identifica el CHPID que se está utilizando.

- UNIT=3172

  Identifica el tipo de unidad de control en el otro extremo del canal. El valor es siempre 3172 cuando se habla a un Network Utility. El IBM 3172 era el predecesor de la función de canal ESCON del Network Utility.

- CUADD=x

  Este valor identifica la dirección de unidad de control del Network Utility. El valor por omisión es 0.

- UNITADD=((*direc*,*número*))

  Define el rango de direcciones reservadas para esta unidad de control, donde:

  direc es la dirección hex del primer subcanal asignado a esta unidad de control

  número
  es el número decimal de subcanales que se están asignando a esta unidad de control

  El ejemplo anterior define un rango de 32 direcciones de unidad de control o subcanales, empezando a partir de E0 hex en adelante. Las direcciones de dispositivo especificadas en la definición de interfaz LCS, LSA o MPC+ de Network Utility deben estar dentro de este rango. El Network Utility puede utilizar un máximo de 64 subcanales.

- LINK=xx

  El valor para el parámetro LINK debe establecerse en el puerto del Direccionador ESCON (ESCD) al que está conectado el *Network Utility*. Dado que el ESCD es un conmutador, puede considerar el parámetro de enlace como un número de teléfono que el sistema principal utilizará para comunicarse con el Network Utility a través del conmutador.

Sentencia IODEVICE

Esta sentencia, junto con la sentencia CNTLUNIT, identifica la conexión del Network Utility al sistema principal.

- ADDRESS=(*direc*,*número*)

  Este parámetro identifica el rango de direcciones en el resto del sistema principal, donde:

  direc es la dirección hex que ***se está asignando*** a la primera dirección reservada

  número
  es el número decimal de subcanales reservados

  Esta dirección es diferente de la UNITADD. Se utiliza en el perfil TCP/IP (para LCS), la Definición de nodo principal XCA de VTAM (para LSA) y el TRL de VTAM (para MPC+) para identificar los subcanales que se están utilizando.

- CUNUMBR=x

  Identifica la sentencia CNTLUNIT correspondiente en esta sentencia IODEVICE. Mientras que el valor para este parámetro tiene que ser el mismo para las macros CNTLUNIT e IODEVICE, no tiene que estar relacionado con cualquier otro parámetro. Sin embargo, es una buena idea especificar el mismo valor en el parámetro ADDRESS de la macro IODEVICE. El valor para CUNUMBR no tiene ningún significado fuera de la Definición de vía de canal.
- UNIT=3172

  Identifica el tipo de dispositivo que está en sentido directo. Deberá ser siempre el 3172 si la unidad de control es un Network Utility. El software de IOCP del sistema principal no consulta este campo. Si está migrando desde un IBM 3172 al Network Utility, puede que tenga un valor de UNIT=SCTC en la sentencia de IOCP existente. Éste deberá cambiarse a 3172 para el Network Utility.
- PARTITION=(nombre)

  Es la lista de dispositivos candidatos y contiene una lista de una o más LPAR que tienen acceso al dispositivo. Esta lista es un subconjunto de la lista de LPAR especificadas en la sentencia CHPID y se utiliza para restringir las LPAR de la lista de canales candidatos a las que se les permite utilizar estos dispositivos. Si el sistema principal no está particionado, este campo no aparecerá.

La Figura 49 muestra un ejemplo de las sentencias IOCP para definir un Network Utility con un Adaptador de canal paralelo (PCA).

```
CHPID                PATH=((05)),TYPE=BL
CNTLUNIT             CUNUMBR=640,PATH=05
                     PROTOCL=S4,UNIT=3172
                     SHARED=N,UNITADD=((40,32))
IODEVICE             UNIT=3172,ADDRESS=((640,32))
                     STADET=N,CUNUMBR=640,TIMEOUT=Y
```

Figura 49. Definiciones de IOCP de sistema principal de ejemplo para el Network Utility (PCA)

Tenga en cuenta los puntos siguientes relacionados con las sentencias IOCP para un Network Utility con un PCA.

- El TYPE es BL para Multiplexor de bloques
- El parámetro PROTOCL puede establecerse en los valores siguientes, en función de la posibilidad de dispositivo:

  D Modalidad DCI (Direct-Coupled Interlock) (Interbloqueo de unión directa)

  S Velocidad de corriente de datos máxima de 3,0 Mbps

  S4 Velocidad de corriente de datos máxima de 4,5 Mbps

  Para el Network Utility, establezca el valor en S4. La modalidad de transferencia y el parámetro de canal deben concordar con el valor de PCA para la modalidad de transferencia y la velocidad de transferencia de canal.
- El parámetro UNIT de las sentencias CNTLUNIT e IODEVICE debe establecerse en 3172.
- Cuando un Convertidor ESCON es la vía de canal, el parámetro CHPID TYPE debe establecerse en CVC, de lo contrario se establece en BL.

Definición del Network Utility en el sistema operativo

Las secciones siguientes describen las definiciones necesarias para diversos sistemas operativos del sistema principal.

Definición de Network Utility para VM/SP

Debe definir el Network Utility en un sistema operativo VM/SP actualizando el archivo de configuración de E/S real (DMKRIO) con entradas para el Network Utility en las macros RDEVICE y RCTLUNIT. En el ejemplo siguiente, 640 es la dirección de unidad base y el tamaño del rango de direcciones es 32.

```
RDEVICE ADDRESS=(640,32),DEVTYPE=3088
RCTLUNIT ADDRESS=640,CUTYPE=3088,FEATURE=32-DEVICE
```

Definición de Network Utility para VM/XA y VM/ESA

Debe definir el Network Utility en un sistema operativo VM/Extended Architecture (VM/XA) o VM/ESA actualizando el archivo de configuración de E/S real (HCPRIO) con una entrada para el Network Utility en la macro RDEVICE. En los ejemplos siguientes, 640 y 2A0 son direcciones de unidad de control base. El tamaño del rango de direcciones, como se define en UCW o IOCP, es 8 en ambos ejemplos.

El ejemplo siguiente es una definición HCPRIO de VM/XA:

```
RDEVICE ADDRESS=(640,8),DEVTYPE=CTCA
```

El ejemplo siguiente es una definición HCPRIO de VM/ESA:

```
RDEVICE ADDRESS=(2A0,8),DEVTYPE=CTCA
```

Definición de Network Utility para MVS/XA y MVS/ESA sin HCD

Debe definir el Network Utility en un sistema operativo Multiple Virtual Storage/Extended Architecture (MVS/XA) o MVS/ESA de IBM actualizando el Programa de control MVS con una entrada para el Network Utility en la macro IODEVICE.

Para canales ESCON, un ejemplo de macro IODEVICE es:

```
IODEVICE UNIT=3172,ADDRESS(540,8)
```

Para canales paralelos, un ejemplo de macro IODEVICE es:

```
IODEVICE UNIT=CTC,ADDRESS(640,8)
```

Las direcciones de unidad de control base son 540 y 640. El tamaño del rango de direcciones, como se define en UCW o IOCP, es 8 en ambos ejemplos.

Definición de Network Utility para MVS/ESA con HCD

El componente de definición de configuración de hardware (HCD) de MVS/ESA SP Versión 4.2 y 4.3 con el APAR Núm. OY67361 ofrece un método mejorado para definir la configuración de hardware del sistema para el Network Utility. Puede llevar a cabo los diversos pasos complejos necesarios para entrar datos de configuración de hardware utilizando un diálogo interactivo con HCD.

Los datos de configuración necesarios para el Network Utility son:

- Cuando se utiliza HCD con el APAR Núm. OY67361, defina el Network Utility como (UNIT=3172). Por ejemplo,

  ```
  IODEVICE UNIT=3172,ADDRESS(740,8)
  ```

- Sin HCD, defina el Network Utility para:

– Canales paralelos como un dispositivo 3088 (UNIT = 3088 o CTC)

```
IODEVICE        UNIT=CTC,ADDRESS(840,8)
```

– Canales ESCON como un dispositivo CTC serie (UNIT = SCTC)

```
IODEVICE        UNIT=SCTC,ADDRESS(A40,8)
```

Notas:

1. Si está utilizando HCD para MVS Versión 4 para definir la conexión de sistema principal ESCON, necesitará el APAR Núm. OY67361 para obtener el soporte UIM para la definición de dispositivo (UNIT=3172).
2. Cuando esté migrando la definición de IOCP y definiciones de sistema operativo al entorno HCD, es importante que cambie todas las sentencia de dispositivo de Network Utility al tipo de dispositivo (UNIT=3172).

Definición de Network Utility para VSE/ESA

Debe definir el Network Utility en un sistema operativo VSE/ESA proporcionando una sentencia ADD para cada dirección de unidad de canal en el tiempo de carga del programa inicial (IPL). Codifique el tipo de dispositivo en la sentencia ADD como CTCA, EML como se muestra en el ejemplo siguiente:

```
ADD 640,CTCA,EML
```

La dirección de unidad de control base es 640 en el ejemplo. Para el número de direcciones de unidad de canal añadidas, incremente la macro de almacenamiento IOTAB según esta cuenta.

Definiciones de VTAM

Esta sección proporciona definiciones de VTAM de ejemplo para un nodo principal XCA, una PU local MPC+ y el nodo principal TRL (Transport Resource List) así como un ejemplo de definición de VTAM para soporte APPN y DLUR. También muestra un ejemplo de un nodo principal conmutado para una PU en un servidor TN3270. Esta sección no está destinada a ser una consulta completa del tema. Para obtener más información sobre cómo configurar VTAM, consulte la publicación *CS OS/390 Resource Definition Reference*, SC31-8565.

Definición de nodo principal XCA de VTAM

Cuando se define una pasarela de canal utilizando LSA en VTAM, se necesita una definición para un XCA (External Communications Adapter) (Adaptador de comunicaciones externo). Esta definición es la misma que la utilizada para un IBM 3172. En la Figura 50 en la página 265 se muestra un ejemplo.

```
*********************************************************************
RAINETU VBUILD TYPE=XCA      1

**
**
RANETUP  PORT  ADAPNO=0,     2                      * X
               CUADDR=285,     3                   * X
               MEDIUM=RING,       4                * X
               SAPADDR=4,            5             * X
               TIMER=60
**
*********************************************************************
RANETUG1 GROUP DIAL=YES,CALL=INOUT,DYNPU=YES
*
RANETUL1 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP1 PU   ISTATUS=ACTIVE
RANETUL2 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP2 PU   ISTATUS=ACTIVE
RANETUL3 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP3 PU   ISTATUS=ACTIVE
RANETUL4 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP4 PU   ISTATUS=ACTIVE
RANETUL5 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP5 PU   ISTATUS=ACTIVE
RANETUL6 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP6 PU   ISTATUS=ACTIVE
RANETUL7 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP7 PU   ISTATUS=ACTIVE
RANETUL8 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP8 PU   ISTATUS=ACTIVE
RANETUL9 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP9 PU   ISTATUS=ACTIVE
```

Figura 50. Ejemplo de definición de nodo principal XCA para la conexión directa LSA

Notas:

1 TYPE debe ser XCA

2 ADAPNO es el número de LAN para la interfaz de Network Utility. Este valor se asigna a la interfaz LSA del Network Utility cuando se crea. El valor puede obtenerse desde el Network Utility listando la configuración de la interfaz desde los menús de talk 6 o puede recuperarse entrando el mandato **list nets** desde la consola ESCON de Talk 5. Tenga en cuenta que un valor incorrecto para este parámetro es el error individual más común de la configuración LSA.

3 CUADDR especifica el subcanal a utilizar para comunicarse con el Network Utility. Este valor debe estar en el rango de valores especificados en la sentencia IODEVICE de la definición IOCP.

4 Especifica la topología de LAN física a la que está conectada la interfaz LSA. Esto corresponde al valor especificado para LANtype para la interfaz de Network Utility. Los valores válidos son MEDIUM=RING para Red en Anillo, MEDIUM=CSMACD para Ethernet y MEDIUM=FDDI para una red FDDI (Fiber Distributed Data Interface) (Interfaz de datos distribuidos por fibra).

5 SAPADDR es el número de Punto de acceso de servicio que VTAM desea abrir en el Network Utility. Tenga en cuenta que se trata del SAP SOURCE, no del SAP DESTINATION. Cuando más de un nodo principal

XCA activo hace referencia a la misma LAN, todos los nodos principales XCA tienen que utilizar SAP diferentes.

Sentencia LINE

El campo CALL puede ser uno de los siguientes:

- IN significa que sólo los dispositivos remotos pueden establecer conexiones.
- OUT significa que sólo VTAM puede iniciar conexiones.
- INOUT significa que las conexiones pueden iniciarse en cualquiera de los dos extremos.

Si VTAM va a efectuar una marcación de salida, la definición de Nodo principal conmutado debe especificar un destino con una sentencia PATH.

Un asterisco en la primera columna indica que una sentencia se ha comentado y deberá ignorarse. Un carácter en la última columna indica que la línea siguiente es una continuación de esta línea.

Definiciones de VTAM para una conexión MPC+

Una conexión MPC+ necesita entradas en dos bloques de control VTAM:

- El Nodo principal local
- El Nodo principal de TRL (Transport Resource List)

La Figura 51 muestra una definición de ejemplo para un nodo principal SNA local para una conexión MPC+ de Network Utility. Se trata de la PU local que reside en VTAM que soporta la conexión de canal definida en la TRL. El tipo de conexión debe ser APPN y también necesitará habilitar HPR.

```
LOCNETU  VBUILD TYPE=LOCAL
MPCNETUP PU     TRLE=MPCNETU,
                XID=YES,
                CONNTYPE=APPN,
                CPCP=YES,
                HPR=YES
```

Figura 51. Definición de nodo principal local VTAM

Notas:

1. TYPE debe ser LOCAL en la sentencia VBUILD.
2. TRLE identifica la TRL que se está utilizando. El nombre debe coincidir con el nombre de una TRL existente.
3. XID indica si se intercambiarán XID. Debe ser XID=YES.
4. CONNTYPE debe establecerse en CONNTYPE=APPN dado que APPN es el único protocolo que VTAM utiliza con una conexión MPC+.
5. CPCP especifica que pueden establecerse conexiones CP-CP con APPN a través de esta conexión MPC+. Esto puede establecerse en YES o NO, en función de la topología de APPN.
6. HPR especifica que el tráfico HPR de APPN puede fluir a través de esta conexión MPC+. HPR se utiliza normalmente por omisión, pero esto se asegura si se establece este valor en YES. Esto es importante porque una conexión MPC+ necesita RTP (y HPR).

A continuación, necesita una lista de recursos de transporte para la conexión MPC+ desde el Network Utility. En la Figura 52 se muestra una definición de ejemplo.

```
        VBUILD TYPE=TRL
MPCNETU TRLE   LNCTL=MPC,
               MAXBFRU=9,
               READ=280,
               WRITE=281,
               MPCLEVEL=HPDT,
               REPLYTO=3.0
```

Figura 52. Definición de Lista de recursos de transporte (TRL) de VTAM

Notas:

1. TYPE debe ser TRL.
2. MPCNETU es el nombre que identifica la TRL. Debe coincidir con lo que se ha especificado en el campo TRLE= de la definición de nodo principal local. (Consulte la Figura 51 en la página 266.)
3. LNCTL identifica el tipo de conexión. Debe ser LCNTL=MPC.
4. MAXBFRU es el número de páginas de 4 K por subcanal de lectura.
5. READ/WRITE especifica los subcanales del grupo MPC+ e indica su dirección. Los números de subcanal deben estar en el rango de direcciones especificadas en la sentencia IODEVICE de la definición de IOCP. Pueden existir múltiples parámetros READ y WRITE en la sentencia TRLE pero tiene que haber como mínimo uno de cada.

   Nota: Aquí las designaciones READ y WRITE se realizan desde la perspectiva de HOST. En la definición MPC+ de Network Utility, las designaciones se realizan desde la perspectiva del Network Utility. Por consiguiente, los subcanales designados como READ en el sistema principal ***deben*** designarse como WRITE en el Network Utility y viceversa.
6. REPLYTO es el valor de tiempo de espera de respuesta en segundos.

Definiciones de VTAM para APPN

Si VTAM está configurado para DLUS, deberá ser un nodo de red APPN. Para configurar VTAM como un nodo de red APPN es necesario especificar determinados parámetros en los parámetros de arranque de VTAM. Éstos se muestran en la Figura 53 en la página 268. Establezca CONNTYPE en APPN y NODETYPE en un nodo de red (NN).

```
ASYDE=TERM,IOPURGE=5M,
CONFIG=I0,
CONNTYPE=APPN,
CPCP=YES,
CSALIMIT=0,
DYNADJCP=YES,
ENCRYPTN=NO,
GWSSCP=YES,
HOSTPU=ISTPUS18,
HOSTSA=18,
HPR=RTP,
NETID=USIBMRA,
NODETYPE=NN,
NOTRACE,TYPE=VTAM,IOINT=0
PPOLOG=YES
SORDER=APPN,
SSCPDYN=YES,
SSCPID=18,
SSCPNAME=RAI,
SSCPORD=PRIORITY,
SUPP=NOSUP,
TNSTAT,CNSL,
VRTG=YES
OSITOPO=LLINES,
OSIMGMT=YES
XNETALS=YES
```

Figura 53. Parámetros de arranque de VTAM

Definición estática de VTAM de los recursos TN3270

Las definiciones de VTAM son necesarias para las PU utilizadas por el Servidor TN3270E. Necesitará una definición de nodo principal conmutado para cada PU del servidor TN3270E. Por ejemplo, cada PU del servidor TN3270E puede soportar hasta 253 LU. Si necesita 500 sesiones 3270, necesitará 2 PU en el direccionador y 2 definiciones de PU en VTAM.

La Figura 54 muestra un ejemplo de una definición de nodo principal conmutado de VTAM para una PU de servidor TN3270E que está conectada a través de DLUR y APPN.

```
LOCNETU  VBUILD TYPE=SWNET
MNETUA   PU     ADDR=01,ISTATUS=ACTIVE,VPACING=0,                       *
                DISCNT=NO,PUTYPE=2,SSCPFM=USSSCS,USSTAB=US327X,         *
                IDBLK=077,IDNUM=02216,IRETRY=YES,MAXDATA=521,           *
                MAXOUT=7,MAXPATH=8,PASSLIM=7,PACING=0,ANS=CONTINUE
*********************************************************************
PNETUA   PATH   PID=1,DLCADDR=(1,C,INTPU),DLCADDR=(2,X,07702216),       *
                DLURNAME=MNETUA
*********************************************************************
JC7LU2   LU     LOCADDR=2
JC7LU3   LU     LOCADDR=3
JC7LU4   LU     LOCADDR=4
```

Figura 54. Definiciones de VTAM para una PU de servidor TN3270E (DLUR/APPN)

La Figura 55 en la página 269 muestra un ejemplo de definición de nodo principal conmutado de VTAM para una PU de servidor TN3270E que utiliza una conexión de subárea al sistema principal.

```
LSAP08T VBUILD TYPE=SWNET
PUPS08T PU ADDR=01,IDBLK=077,IDNUM=12244,MAXOUT=7,PACING=0,VPACING=0,
               DLOGMOD=B22NNE,PUTYPE=ANY,
               SSCPFM=USSSCS,MAXDATA=2000,MODETAB=LMT3270
PT08LU2 LU LOCADDR=02,LOGAPPL=TSO
PT08LU3 LU LOCADDR=03,LOGAPPL=TSO
PT08LU4 LU LOCADDR=04,LOGAPPL=TSO
PT08LU5 LU LOCADDR=05,LOGAPPL=TSO
PT08LU6 LU LOCADDR=06,LOGAPPL=TSO
```

Figura 55. Definiciones de VTAM para una PU de servidor TN3270E (Subárea)

Las secciones siguientes proporcionan una visión general de las sentencias de la Definición de nodo principal conmutado.

Sentencia VBUILD

El campo TYPE debe ser TYPE=SWNET.

Sentencia PU

Esta sentencia define el tipo de flujo de datos y el destino. Los parámetros pertinentes son:

- ADDR es un identificador.
- MAXDATA es el tamaño máximo de paquete que VTAM soportará a través de esta interfaz. Este valor se negociará con el Network Utility durante el intercambio de XID.
- IDBLK/IDNUM identifican el dispositivo remoto cuando VTAM se está comunicando con dispositivos PU 2.0 (dependientes).

Sentencia LU

Estas sentencias definen las unidades lógicas (LU) con las que se puede establecer el contacto a través de esta PU. El nombre de la izquierda de cada sentencia es el nombre que el sistema principal utiliza para direccionar cada LU. LOCADDR lo utiliza el Network Utility para identificar la LU correcta en VTAM.

Sentencia PATH

Si VTAM va a efectuar una marcación de salida, la definición de Nodo principal conmutado debe especificar un destino con una sentencia PATH. La sentencia path será diferente en función de si el servidor TN3270E se conecta a través de una conexión de subárea o DLUR/APPN.

Para la conexión de subárea, el formato es:

```
PATH DIALNO=xxyyzzzzzzzzzzzz
```

donde:

- *xx* es un espacio reservado
- *yy* es el número SAP de destino
- *zz* es la dirección MAC de destino

El ejemplo de la Figura 55 no tiene una sentencia PATH porque en este ejemplo, la PU de sentido directo establecerá el contacto con VTAM en lugar de que VTAM efectúe una marcación de salida hacia el dispositivo.

El ejemplo de la Figura 54 en la página 268 muestra una sentencia PATH para una PU de servidor TN3270E que está utilizando DLUR para conectarse al sistema principal. Aquí, la sentencia PATH identifica el nombre de CP del Network Utility (MNETUA) a través del parámetro DLURNAME. Esto es necesario para que se

establezca la conversación LU6.2 entre DLUR y DLUS. Una vez establecida esta sesión, se establecerá la sesión SSCP-PU entre VTAM y la PU de servidor TN3270E utilizando el valor IDBLK/IDNUM especificado por DLCADDR=(2,X,07702216).

Definición dinámica de VTAM de los recursos TN3270

Para obtener la información más reciente, consulte el apartado “Definición dinámica de LU dependientes” en la página 153.

Definiciones IP de sistema principal

Para definir el Network Utility en el sistema principal para una conexión TCP/IP es necesario que efectúe cambios en el perfil TCP/IP de sistema principal. Esta sección proporciona una visión general de las sentencias pertinentes que necesitan modificarse.

Sentencia DEVICE

Esta sentencia define la pareja de subcanal que está siendo utilizada por TCP/IP. El formato es:

```
DEVICE  nombre  LCS  subcanal
```

donde:

- *nombre* identifica la vía de subcanal que se está utilizando. Sólo tiene significado local y puede tener cualquier valor.
- *subcanal* identifica el subcanal par que se está utilizando para esta conexión. Este valor procede de la sentencia IODEVICE de la definición de IOCP. Cuando se especifica, ese subcanal y el siguiente se utilizan ambos.

Un perfil TCP/IP debe contener una sentencia DEVICE para cada pareja de subcanales que se está utilizando.

Sentencia LINK

Esta sentencia identifica las interfaces LCS del Network Utility que se están utilizando en una pareja de subcanales determinada. El formato es:

```
LINK nombre tipolan númerolan nombredispositivo
```

donde:

- *nombre* identifica la interfaz LCS. Sólo tiene significado local y puede tener cualquier valor.
- *tipolan* identifica el tipo de interfaz de LAN que la interfaz LCS de Network Utility está emulando. Los valores permitidos son:
  - IBMTR para Red en Anillo
  - ETHERNET para Ethernet V2
  - 802.3 para Ethernet (IEEE 802.3)
  - ETHERor802.3 para cualquier formato Ethernet aceptado
  - FDDI para FDDI
- *númerolan* identifica qué interfaz LCS del Network Utility se está utilizando. El *númerolan* se genera secuencialmente para cada *tipolan* en el Network Utility al añadir una interfaz LCS. El *númerolan* puede encontrarse entrando **list nets** desde la consola ESCON de Talk 5. Tenga en cuenta que el *númerolan* ***no*** es el número de red. Tener el *númerolan* incorrecto es el error de configuración individual más común para una interfaz LCS.

- *nombredispositivo* correlaciona la interfaz LCS con una pareja de subcanales. Debe coincidir con una sentencia DEVICE definida anteriormente.

Pueden haber múltiples sentencias LINK asociadas con una sola sentencia DEVICE. Tiene que haber una interfaz LCS en el Network Utility para cada sentencia LINK.

Sentencia HOME

Esta sentencia especifica la(s) dirección (direcciones) IP de la pila TCP/IP del sistema principal. El formato es:

```
HOME     direcciónip1     enlace1
         direcciónip2     enlace2
```

donde:

- *direcciónipX* especifica una dirección IP en el sistema principal.
- *enlaceX* especifica el enlace que está asociado con esta dirección IP.

Tiene que haber sólo una dirección HOME para cada sentencia LINK. La dirección HOME debe estar en la misma subred IP que la dirección IP de la interfaz LCS del Network Utility, pero ***deben ser direcciones diferentes***.

Sentencia GATEWAY

Esta sentencia identifica la información de direccionamiento IP para el sistema principal. Se divide en tres secciones:

- Rutas directas son rutas conectadas directamente al sistema principal. La subred que contiene la interfaz LCS de Network Utility es una ruta directa.
- Rutas indirectas son rutas a las que se puede acceder a través de direccionadores. Por ejemplo, las subredes de las LAN del Network Utility son rutas indirectas.
- Ruta por omisión es la ruta a utilizar si el sistema principal no tiene una ruta directa o indirecta a una dirección IP.

Rutas directas

El formato para las Rutas directas es:

```
red primersalto nombreenlace tamañopqt submáscara subvalor
```

donde:

- *red* es la partes sin subredes de la dirección IP.
- *primersalto* indica la dirección IP del siguiente salto en la red IP. Para las Rutas directas, debe ser un signo igual (=).
- *nombreenlace* identifica qué enlace debe utilizar el sistema principal para llegar a las direcciones de esta ruta. Para rutas accesibles a través del Network Utility, éste debe ser el nombre de la sentencia LINK asociada con la interfaz LCS en esta subred.
- *tamañopqt* es el tamaño máximo de trama a utilizar en la interfaz. Debe ser menor que o igual al tamaño de paquete definido en la configuración LCS del Network Utility. Un valor de DEFAULTSIZE indica que se utilizará el tamaño de paquete por omisión.
- *submáscara* especifica la máscara de subred utilizado en este enlace. La máscara de subred debe corresponder a la máscara de subred definida para la interfaz LCS en la configuración de IP del Network Utility. Este campo también

puede establecerse en HOST para identificar una conexión de punto a punto. En este caso, el campo de red debe contener la dirección IP completa de la interfaz LCS.

- *subvalor* especifica la parte con subredes de la dirección IP y, junto con el campo red, debe especificar totalmente la subred IP asociada con esta interfaz LCS.

Rutas indirectas

El formato para las Rutas indirectas es:

```
red primersalto nombreenlace tamañopqt submáscara subvalor
```

donde:

- *red* es la dirección completa de la subred IP.
- *primersalto* indica la dirección IP del siguiente salto en la red IP. Para Rutas indirectas accesibles a través del Network Utility, debe ser la dirección IP de la interfaz LCS del Network Utility.
- *nombreenlace* identifica qué enlace debe utilizar el sistema principal para llegar a las direcciones de esta ruta. Para rutas accesibles a través del Network Utility, éste debe ser el nombre de la sentencia LINK asociada con la interfaz LCS en esta subred.
- *tamañopqt* es el mismo valor que para Rutas directas.
- *submáscara* debe ser 0 o estar en blanco si el campo de red contiene la dirección de subred completa.
- *subvalor* debe dejarse en blanco si no se ha especificado ninguna máscara de subred.

Rutas por omisión

El formato para las Rutas por omisión es:

```
red primersalto nombreenlace tamañopqt submáscara subvalor
```

donde:

- *red* debe ser DEFAULTNET.
- *primersalto* indica la dirección IP del siguiente salto en la red IP. Para las Rutas por omisión en el Network Utility, ésta debe ser la dirección IP de la interfaz LCS del Network Utility.
- *nombreenlace* identifica qué enlace debe utilizar el sistema principal para llegar a las direcciones de esta ruta. Para rutas accesibles a través del Network Utility, éste debe ser el nombre de la sentencia LINK asociada con la interfaz LCS en esta subred.
- *tamañopqt* es el mismo valor que para Rutas directas.
- *submáscara* debe ser 0 o estar en blanco.
- *subvalor* debe estar en blanco.

Sentencia START

Esta sentencia hace que se inicien los subcanales especificados. El formato es:

```
START nombredispositivo
```

donde *nombredispositivo* es el nombre en la sentencia DEVICE anterior.

Debe haber una sentencia START para cada sentencia DEVICE si el cliente desea activar los dispositivos cuando se inicia TCP/IP. Si la sentencia START no está aquí, los dispositivos pueden iniciarse utilizando el archivo OBEY. Tenga en cuenta que el nombre indicado aquí es el de la sentencia DEVICE, no de la sentencia

LINK. Tenga también en cuenta que la interfaz LCS de Network Utility permanecerá en estado DOWN hasta que se haya emitido START desde TCP/IP.

Definiciones TCP/IP de sistema principal para LCS

Esta sección le proporciona ejemplos de las sentencias anteriores necesarias si está definiendo una conexión LCS.

1. Sentencia DEVICE:

   ```
   DEVICE LCS1 LCS 210
   ```

   donde LCS1 es el nombre de dispositivo que se está definiendo, LCS es el tipo de dispositivo y 210 es el subcanal (de grabación de Network Utility) de lectura del sistema principal utilizado para esta definición.

2. Sentencia LINK

   ```
   LINK ETHLCS1 802.3 0 LCS1
   ```

   donde ETHLCS1 es el nombre de enlace, 802.3 es el tipo de LAN a la que se conecta la interfaz LCS en el Network Utility, 0 es el número de LAN asignado por el Network Utility y LCS1 es el nombre del dispositivo (de la sentencia device anterior).

   Nota: Recuerde que el Network Utility asigna automáticamente el número de LAN al definir la interfaz LCS. Puede obtenerlo emitiendo un mandato `list all` desde el indicador ESCON Config> en el proceso talk 6 de la consola del Network Utility.

3. Mandato HOME

   ```
   HOME 9.24.106.72 ETHLCS1
   ```

   donde 9.24.106.72 es la dirección IP de esta interfaz LCS y ETHLCS1 es el nombre del enlace.

4. Mandato GATEWAY

   ```
   GATEWAY 9.24.106   9.24.106.1   ETHLCS1   4096  0
   ```

   donde 9.24.106 es la dirección IP para la red, 9.24.106.1 es la dirección IP del direccionador por omisión, ETHLCS1 es el nombre de enlace definido por la sentencia LINK anterior, 4096 es el tamaño de MTU, 0 es la máscara de subred y el valor de subred se ha dejado en blanco.

5. Activar el perfil TCP/IP

   Para activar el dispositivo definido en el paso 1, emita el mandato siguiente:

   ```
   start lcs1
   ```

Definiciones TCP/IP de sistema principal para MPC+

Los pasos para configurar TCP/IP en el sistema principal para una conexión MPC+ son los mismos que para una conexión LCS. Sin embargo, la sintaxis para los mandatos device y link es ligeramente diferente. Para una conexión MPC+, la sintaxis para el mandato device es:

```
DEVICE IPTRL1 MPCPTP
```

donde IPTRL1 es el nombre del TRL que esta conexión utilizará y MPCPTP especifica un enlace MPC de punto a punto.

Para definir el enlace, la sintaxis es:

```
LINK LINK1 MPCPTP IPTRL1
```

donde LINK1 es el nombre de enlace y los otros dos parámetros son los mismos que los utilizados en la sentencia device.

Capítulo 19. Redes privadas virtuales

La Internet se ha convertido en una infraestructura de redes troncales común de bajo coste. Debido a su alcance universal, muchas compañías han considerado la posibilidad de construir una red privada virtual (VPN) segura a través de la Internet pública. El reto del diseño de una VPN para el entorno de negocios global actual será aprovechar la red troncal de la Internet pública para las comunicaciones entre compañías y dentro de las compañías, mientras se sigue proporcionando la seguridad y la fiabilidad de la red corporativa privada tradicional autoadministrada.

Este capítulo define una VPN y explica las ventajas de implementar una VPN. También proporciona consideraciones acerca de la seguridad y aspectos de planificación y describe soluciones VPN disponibles hoy en el mercado.

VPN - Introducción y ventajas

Con el explosivo crecimiento de Internet, las compañías están empezando a preguntar *¿Cuál es el mejor modo en que podemos aprovechar la Internet para nuestro negocio?* Inicialmente, las compañías proporcionaban ubicaciones Web corporativas para promocionar la imagen, los productos y los servicios de su compañía. En la actualidad las posibilidades de Internet son ilimitadas y el foco ha cambiado al e-business — la utilización del alcance global de Internet para acceder fácilmente a aplicaciones y datos clave de negocio que residen en sistemas de I/T tradicionales. Ahora las compañías pueden ampliar el alcance de sus aplicaciones y datos de forma segura y efectiva de costes en todo el mundo a través de la implementación de soluciones VPN seguras.

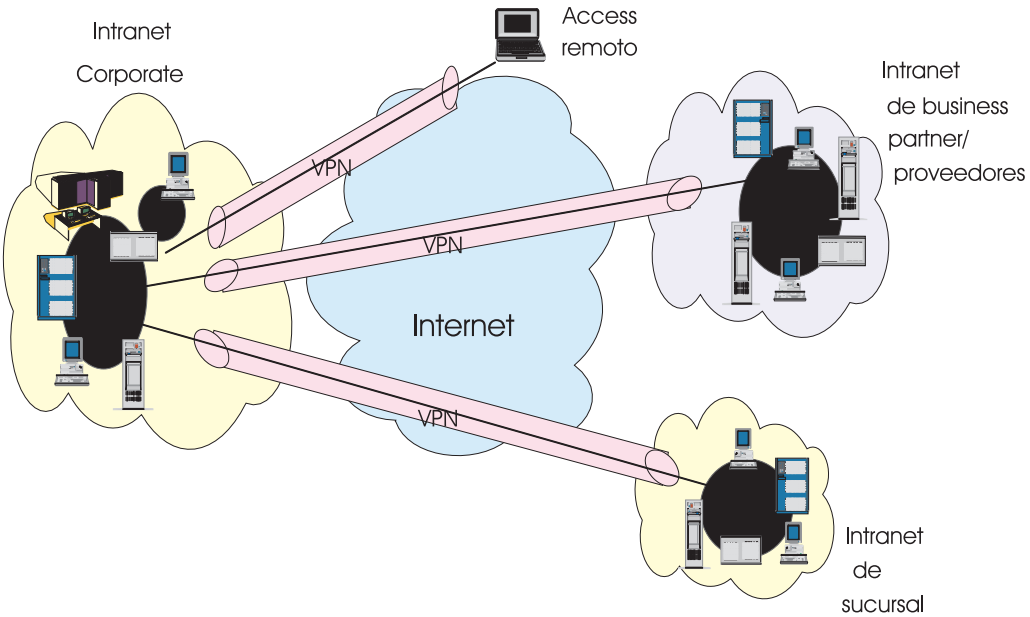


Figura 56. Redes privadas virtuales

Una VPN es una extensión de la intranet privada de una empresa en una red pública, por ejemplo Internet, que crea una conexión privada segura, esencialmente mediante un túnel privado. Las VPN transmiten la información por Internet conectando usuarios remotos, sucursales y business partners en una red corporativa ampliada, como se muestra en la Figura 56. Los suministradores de

servicio de Internet (ISP) ofrecen el acceso efectivo de costes a Internet (a través de líneas directas o números de teléfono locales), permitiendo a las compañías eliminar sus costosas líneas alquiladas actuales, las llamadas de larga distancia y los números de teléfono gratuitos.

Infraestructura de seguridad IP de IETF

Dentro del modelo de pilas de protocolos de comunicaciones por capas, la capa de red (IP en el caso de la pila TCP/IP) es la capa más baja que puede proporcionar seguridad de extremo a extremo. Los protocolos de seguridad de la capa de red proporcionan protección general para todos los datos de aplicación de la capa superior transportados en la carga útil de un datagrama IP, sin necesitar que un usuario modifique las aplicaciones.

Las soluciones se basan en la infraestructura abierta de arquitectura de Seguridad IP (IPSec) definida por el Grupo de trabajo IPSec de IETF. IPSec se denomina infraestructura porque proporciona una larga base duradera y estable para proporcionar seguridad de capa de red. Puede acomodar los algoritmos criptográficos de la actualidad y también puede acomodar algoritmos más nuevos y más potentes a medida que éstos están disponibles. Son necesarias las implementaciones de IPv6 para soportar IPSec y se recomiendan encarecidamente las implementaciones de IPv4. Además de proporcionar las funciones de seguridad básicas para la Internet, IPSec proporciona bloques de construcción flexibles a partir de los cuales se pueden construir VPN robustas y seguras.

El Grupo de trabajo IPSec se ha concentrado en definir protocolos para encargarse de varias áreas principales:

- Autentificación del origen de los datos: verifica que cada datagrama lo haya originado el remitente que afirma serlo y no se puede repudiar
- Integridad de datos: verifica que el contenido del datagrama no se haya modificado por el camino, ya sea deliberadamente ya sea debido a errores aleatorios
- La confidencialidad de los datos: oculta el texto claro de un mensaje, normalmente utilizando cifrado
- Protección de reproducción: asegura que un intruso no pueda interceptar un datagrama y reproducirlo posteriormente sin ser detectado
- Gestión automatizada de claves criptográficas y Asociaciones de seguridad (SA): asegura que la política de VPN de una compañía pueda implementarse de forma conveniente y precisa por la red ampliada sin necesidad de efectuar configuraciones grandes o manuales (estas funciones hacen que el tamaño de una VPN pueda ampliarse a cualquier tamaño que necesite el negocio).

La lista siguiente presenta los protocolos IPSec principales:

- Authentication Header (Cabecera de autentificación) (AH) de IP proporciona autentificación del origen de datos, integridad de datos y protección de reproducción.
- Encapsulating Security Payload (ESP) (Carga activa de seguridad de encapsulación) de IP proporciona confidencialidad de datos, autentificación de origen de datos, integridad de datos y protección de reproducción.
- Internet Security Association and Key Management Protocol (Protocolo de gestión de claves y asociación de seguridad de Internet) (ISAKMP) proporciona un método para definir asociaciones de seguridad y gestionar sus claves criptográficas automáticamente.

- Oakley proporciona el protocolo de gestión de claves criptográficas utilizado por ISAKMP.
- Internet Key Exchange (Intercambio de claves de Internet) (IKE) con signaturas digitales o clave compartidas proporciona automatización a la gestión de claves, de modo que no es necesario generar claves de forma manual. Durante las negociaciones de la Fase 1, se intercambian las claves criptográficas y las partes autentifican la identidad del otro. En este momento, la función ISAKMP utiliza el protocolo de gestión de claves criptográficas de Oakley para proteger los mensajes ISAKMP intercambiados entre direccionadores, en preparación para un intercambio de datos seguro.
- Public Key Infrastructure (Infraestructura de claves pública) (PKI) es una disposición efectuada por la Autoridad de certificación (CA) que distribuye y verifica claves para usuarios.
- El certificado es un área de datos que enlaza el ID codificado (signatura digital) de cada usuario de red con su clave pública/privada.
- La signatura digital es un área de datos que contiene el ID codificado de un usuario, que pasa a formar parte de un certificado.

Authentication Header

Authentication Header (AH) de IP proporciona integridad sin conexión (es decir, por paquete) y autentificación de origen de datos para datagramas IP. También ofrece protección contra la reproducción. La integridad de datos se asegura mediante la suma de comprobación generada por un código de autentificación de mensaje (por ejemplo, MD5); la autentificación del origen de datos se asegura incluyendo una clave compartida secreta en los datos que se deben autentificar; y la protección de reproducción se proporciona utilizando un campo de número de secuencia dentro de la cabecera AH. En el vocabulario de IPSec, estas tres funciones diferenciadas se agrupan y se denominan simplemente autentificación de nombre.

AH autentifica tanta cantidad del datagrama IP como es posible. Algunos campos de la cabecera IP cambian por el camino y el receptor no puede predecir su valor. Estos campos se llaman mutables y no están protegidos por AH. Los campos IPv4 mutables son:

- Tipo de servicio
- Distintivos
- Desplazamiento de fragmentos
- Tiempo de vida (TTL)
- Suma de comprobación de cabecera

AH se identifica por el número de protocolo 51, asignado por IANA. La cabecera de protocolo (IPv4, IPv6 o Extensión) que precede inmediatamente a la cabecera AH contiene este valor en su campo de protocolo (Protocol) (IPv4) o cabecera siguiente (Next Header) (IPv6, Extensión).

El proceso AH sólo se aplica a paquetes IP no fragmentados. Sin embargo, un paquete IP en el que se ha aplicado AH puede ser fragmentado por direccionadores intermedios. En este caso, el destino primero vuelve a ensamblar el paquete y luego le aplica el proceso AH. Si un paquete IP que parece ser un fragmento (el campo de desplazamiento es diferente de cero o se establece el bit Más fragmentos) se entra en el proceso AH, se elimina. Esto impide el llamado

ataque de fragmentos de solapamiento, que utiliza incorrectamente el algoritmo de reemsamblaje de fragmentos para crear paquetes falsificados y forzarlos a través de un cortafuegos.

Los paquetes que han fallado la autentificación se eliminan y no se entregan nunca a las capas superiores. Esta modalidad de operación reduce mucho las posibilidades de rechazo satisfactorio de ataques de servicio, que pretenden bloquear las comunicaciones de un sistema principal o pasarela inundándolas con paquetes falsos.

AH se puede utilizar en dos modalidades: modalidad de transporte y modalidad de túnel. La modalidad de transporte la utilizan los sistemas principales en lugar de las pasarelas. Las pasarelas ni siquiera son necesarias para soportar la modalidad de transporte. La modalidad de transporte necesita menos actividad general de proceso, pero los campos mutables no se autentifican.

Cuando se necesite la protección de los campos IPv4, se deberán utilizar los túneles. La carga útil del paquete IP se considera inmutable y está siempre protegida por AH.

La modalidad de túnel se utiliza siempre que uno de los extremos de una SA es una pasarela. De este modo, entre dos cortafuegos se utiliza siempre la modalidad de túnel. Aunque las pasarelas sólo se necesitan para soportar la modalidad de túnel, normalmente también soportan la modalidad de transporte. Esta modalidad está permitida cuando la pasarela actúa como sistema principal, por ejemplo en casos en los que el tráfico está destinado a sí mismo. Los mandatos SNMP o las peticiones de eco ICMP son ejemplos de ello.

En modalidad de túnel, las direcciones IP de las cabeceras externas no necesitan ser las mismas que las direcciones de las cabeceras internas. Por ejemplo, dos pasarelas de seguridad pueden operar un túnel AH que se utiliza para autentificar todo el tráfico entre las redes que conectan. Ésta es una modalidad de operación muy típica. Los sistemas principales no son necesarios para soportar la modalidad de túnel, pero normalmente la soportan.

La modalidad de túnel ofrece protección total del datagrama IP encapsulado y la posibilidad de utilizar direcciones privadas. Sin embargo, hay una actividad general de proceso adicional asociada con esta modalidad.

Nota: La especificación AH original en RFC 1825 no lista la modalidad de túnel como un requisito. Debido a ello, hay implementaciones IPSec basadas en dicho RFC que no soportan AH en modalidad de túnel. Esto tiene implicaciones en la posibilidad de implementar determinados escenarios.

IP Encapsulating Security Payload

Encapsulating Security Payload (ESP) de IP proporciona confidencialidad (cifrado) de datos,integridad sin conexión (es decir, por paquete), autentificación de origen de datos y protección contra reproducción. ESP siempre proporciona confidencialidad de datos y también puede proporcionar opcionalmente autentificación de origen de datos, comprobación de integridad de datos y protección contra reproducción. Si compara ESP con AH, comprobará que sólo ESP proporciona cifrado, mientras que los dos pueden proporcionar autentificación, comprobación de integridad y protección contra reproducción.

Cuando ESP se utiliza para proporcionar la función de autentificación, utiliza los mismos algoritmos usados por el protocolo AH. Sin embargo, el alcance es diferente.

Combinación de los protocolos

Tanto ESP como AH pueden aplicarse solos, en combinación con el otro o incluso anidados dentro de otra instancia de sí mismos. Con estas combinaciones, se puede proporcionar autentificación y/o cifrado entre una pareja de sistemas principales que se comunican, entre una pareja de cortafuegos que se comunican o entre un sistema principal y un cortafuegos.

Internet Key Exchange (IKE)

Una SA contiene toda la información pertinente que los sistemas que se comunican necesitan para ejecutar los protocolos IPSec, por ejemplo AH o ESP. Por ejemplo, una SA identificará el algoritmo criptográfico a utilizar, la información de claves y las identidades de las partes participantes. ISAKMP define una infraestructura estandarizada para soportar la negociación de las SA, la generación inicial de todas las claves criptográficas y la renovación subsiguiente de dichas claves. Oakley es el protocolo de gestión de claves obligatorio que es necesario utilizar dentro de la infraestructura ISAKMP. ISAKMP soporta la negociación automatizada de las SA y la generación y renovación automatizadas de las claves criptográficas. La posibilidad de efectuar estas funciones con ninguna o muy poca configuración de máquinas será un elemento crítico a medida que una VPN aumenta de tamaño.

El intercambio seguro de claves es el factor más crítico al establecer un entorno de comunicaciones seguro. Si la clave está comprometida, la autentificación y el cifrado son inútiles por muy fuertes que sean. Dado que los procedimientos ISAKMP se encargan de la inicialización de las claves, tienen que ser capaces de ejecutarse a través de enlaces donde no se supone ninguna seguridad. Es decir, se utilizan para ejecutar una rutina de carga en los protocolos IPSec. Por lo tanto, los protocolos ISAKMP utilizan las operaciones más complejas y que usan más intensivamente el procesador del conjunto de protocolos IPSec.

ISAKMP necesita que todos los intercambios de información se cifren y autentifiquen. Nadie puede escuchar furtivamente el material de claves y el material de claves sólo se intercambiará entre partes autentificadas.

Escenarios de cliente de VPN

Esta sección describe tres de los escenarios de negocios más probables que se adaptan bien a la implementación de una solución VPN:

- Red de conexión de sucursales
- Red de proveedores/business partners
- Red de acceso remoto

Las secciones siguientes proporcionan una breve visión general de cada uno de estos escenarios.

Red de conexión de sucursales

El escenario de sucursales conecta de forma segura dos intranets fiables dentro de la organización. El foco de seguridad se centra ahora en proteger la intranet de la compañía frente a intrusos externos y en proteger los datos de la compañía mientras fluyen a través de la Internet pública. Ésta difiere de la red de

proveedores/business partners que se describe a continuación, donde el foco está puesto en permitir a los proveedores/business partners acceder a los datos de la intranet corporativa.

Supongamos que las oficinas centrales corporativas desean minimizar los costes producidos por la comunicación con sus propias sucursales. En la actualidad, la compañía puede utilizar líneas conmutadas y/o alquiladas, pero desea explorar otras opciones para transmitir los datos confidenciales internos que sean menos caras, más seguras y accesibles globalmente. Aprovechando la Internet, se pueden establecer fácilmente las VPN de conexión de sucursales para satisfacer las necesidades de la compañía.

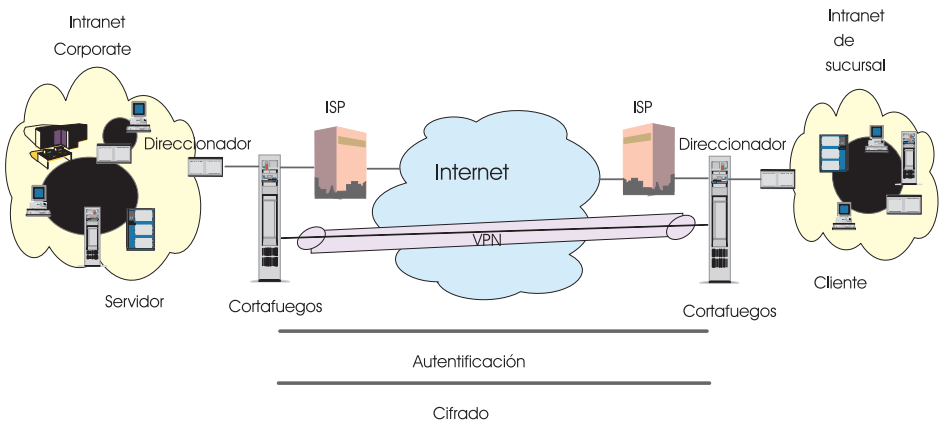


Figura 57. Red de conexión de sucursales

Como se muestra en la Figura 57, un modo de implementar esta conexión VPN entre las oficinas principales corporativas y una de sus sucursales consiste en que la compañía compre el acceso a Internet a un ISP, por ejemplo IBM Global Services. Se colocarían en el límite de cada una de las intranets direccionadores o cortafuegos IBM eNetwork con funciones de cortafuegos integradas o, en algunos casos, un servidor IBM con posibilidad de IPSec para proteger el tráfico corporativo de los piratas informáticos de Internet. Con este escenario, los clientes y servidores no necesitan soportar la tecnología IPSec, dado que los direccionadores (o cortafuegos) habilitados para IPSec proporcionarían la autentificación y el cifrado necesarios de los paquetes de datos. Con este planteamiento, se escondería cualquier información confidencial de los usuarios de Internet no fiables, con el direccionador o el cortafuegos rechazando el acceso a los posibles asaltantes.

Con el establecimiento de las VPN de conexión de sucursales, las oficinas centrales corporativas podrán comunicarse de forma segura y efectiva de costes con sus sucursales, tanto si éstas están ubicadas localmente como si están lejos. Mediante la tecnología VPN, cada sucursal puede también ampliar el alcance de su intranet existente para incorporar otras intranets de bifurcación, creando una red corporativa ampliada para toda la empresa.

Esta compañía también puede ampliar fácilmente este entorno recién creado para incluir a sus business partners, proveedores y usuarios remotos mediante el uso de tecnología IPSec abierta.

Red de proveedores/business partners

Las compañías líderes de la industria son aquéllas que pueden comunicarse de forma segura y no costosa con sus business partners, subsidiarias y proveedores. Muchas compañías han elegido implementar líneas conmutadas y/o comprar líneas alquiladas para lograr esta interacción. Pero normalmente esto es caro y el alcance geográfico puede ser limitado. La tecnología VPN ofrece una alternativa para que las compañías construyan una red corporativa ampliada privada y efectiva de costes con cobertura mundial, aprovechando la Internet u otra red pública.

Suponga que es usted el proveedor principal de piezas de un fabricante. Puesto que es crítico que tenga las piezas y las cantidades específicas en el momento exacto necesario para la empresa de fabricación, necesita estar siempre al corriente del estado de inventario y de las planificaciones de producción del fabricante. Quizá en la actualidad está manejando esta interacción manualmente y encuentra que este método requiere mucho tiempo, es caro y quizá incluso impreciso. Le gustaría encontrar un modo más fácil, más rápido y más efectivo para comunicarse. Sin embargo, dada la confidencialidad y la naturaleza sensible al tiempo de esta información, el fabricante no desea publicar estos datos en su página Web corporativa o distribuir esta información mensualmente a través de un informe externo.

Para solucionar estos problemas, el proveedor de piezas y el fabricante pueden implementar una VPN, como se muestra en la Figura 58. Se puede crear una VPN entre una estación de trabajo cliente, en la intranet del proveedor de piezas o directamente en el servidor que reside en la intranet del fabricante. Los clientes pueden autentificarse a sí mismos en el direccionador o el cortafuegos que protege la intranet del fabricante, directamente en el servidor del fabricante (validando que son quienes dicen que son) o utilizando ambas opciones en función de la política de seguridad. Entonces se puede establecer un túnel, cifrando todos los paquetes de datos del cliente, a través de Internet, al servidor necesario.

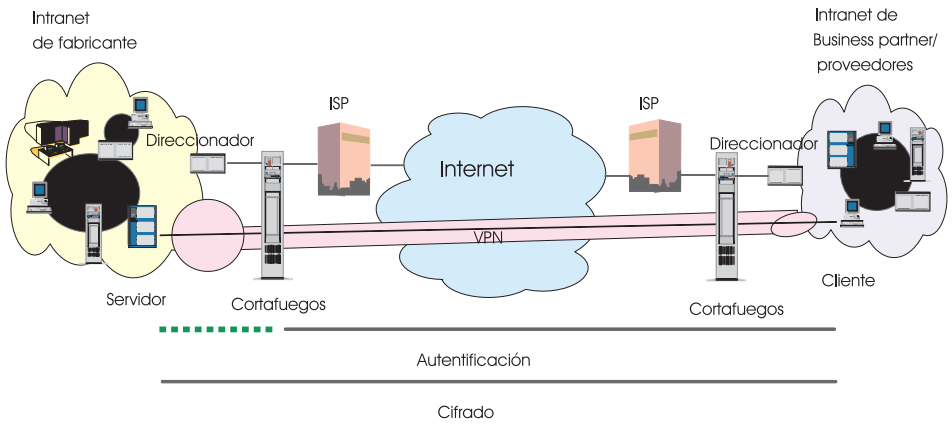


Figura 58. Red de proveedores/business partners

Un modo de implementar este escenario consiste en que las compañías compren el acceso a Internet a un ISP, por ejemplo IBM Global Services. Entonces, dada la falta de seguridad de Internet, se puede utilizar un direccionador habilitado para IPSec, un cortafuegos de IBM eNetwork o un servidor de IBM con posibilidad de IPSec según sea necesario para proteger las intranets frente a los intrusos. Si se desea una protección de extremo a extremo, las máquinas cliente y servidor también necesitarán estar habilitadas para IPSec.

Mediante la implementación de esta tecnología VPN, el fabricante podrá ampliar fácilmente el alcance de la intranet corporativa existente para incluir a uno o más proveedores de piezas (esencialmente creando una red corporativa ampliada) al mismo tiempo que disfrutará de las ventajas de efectividad de costes de utilizar la Internet como red troncal. Ahora con la flexibilidad de la tecnología IPSec abierta, la posibilidad de este fabricante de incorporar más proveedores externos es ilimitada.

Al implementar una VPN, se debe establecer un conjunto de criterios de configuración de seguridad. Decisiones tales como, por ejemplo, los algoritmos de seguridad que debe utilizar cada sistema habilitado para IPSec y el momento en que deben renovarse las claves, son todas ellas aspectos de la gestión de política. En lo que concierne a la tecnología de claves, casi todos los protocolos de seguridad actualmente comunes de hoy en día empiezan utilizando la criptografía de clave pública. Se asigna a cada usuario una clave pública exclusiva. Los certificados, en forma de signaturas digitales, validan la autenticidad de la identidad y la clave de cifrado.

Estos certificados pueden almacenarse en una base de datos de claves públicas, por ejemplo un DNS seguro, a la que se puede acceder a través de un protocolo simple, por ejemplo LDAP.

Red de acceso remoto

Un usuario remoto, que está en su casa o de viaje, desea poder comunicarse de forma segura y efectiva de costes con la intranet corporativa.

Aunque mucha gente utiliza todavía números de teléfono de larga distancia y gratuitos, este coste puede minimizarse mucho aprovechando la Internet. Por ejemplo, está en casa o de viaje, pero necesita un archivo confidencial que se encuentra en un servidor de la intranet. Mediante la obtención de acceso a Internet en forma de conexión de marcación a un ISP, por ejemplo IBM Global Services, podrá comunicarse con el servidor de la intranet y acceder al archivo necesario.

Un modo de implementar este escenario consiste en utilizar un cliente remoto habilitado para IPSec de VPN eNetwork y un direccionador o cortafuegos, como se muestra en la Figura 59 en la página 283. El cliente accede a Internet a través de la marcación en un ISP y, a continuación, establece un túnel autentificado y cifrado entre él y el direccionador o cortafuegos en el límite de la intranet.

Mediante la aplicación de la autentificación IPSec entre el cliente remoto y el direccionador o cortafuegos, puede proteger la intranet contra paquetes IP no deseados y posiblemente maliciosos. Y mediante el cifrado del tráfico que fluye entre el sistema principal remoto y el direccionador o cortafuegos, puede impedir que los intrusos accedan furtivamente a la información.

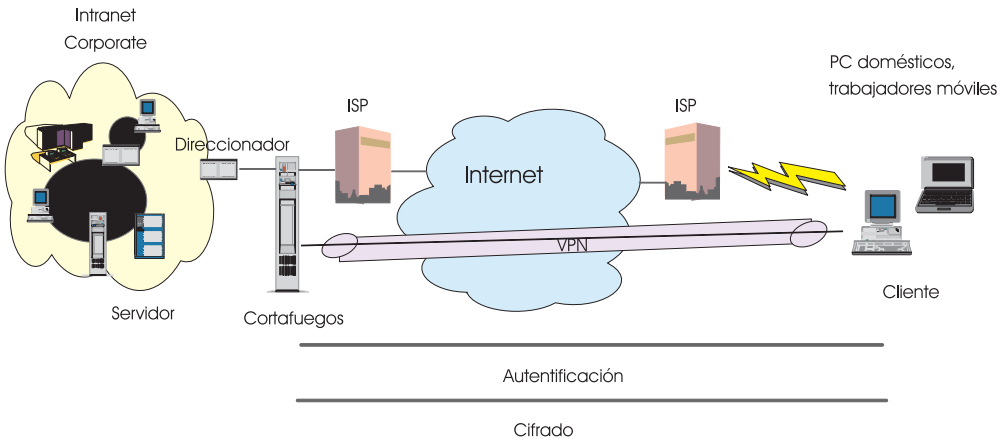


Figura 59. Red de acceso remoto

Los tres escenarios descritos en esta sección son la base para los ejemplos de implementación y configuración de IPSec descritos en este manual. El capítulo siguiente proporciona procedimientos paso a paso para configurar túneles IPSec con direccionadores de IBM.

Redes basadas en política

Las redes basadas en política es un arquitectura mediante la cual los dispositivos de red determinan si se debe aplicar una acción distinta del direccionamiento al tráfico recibido. Por ejemplo, ¿debe protegerse el tráfico mediante la Seguridad IP? o ¿tiene el tráfico requisitos especiales de Calidad de servicio (QoS)? Para que los dispositivos de red puedan tomar decisiones basadas en la política, es necesario que estén configurados para ello. La configuración de múltiples dispositivos es difícil de escalar a una red grande. La gestión de estas diversas configuraciones puede facilitarse desarrollando un método de almacenamiento, recuperación y distribución de objetos de configuración comunes. El método aceptado de almacenamiento, búsqueda y compartimiento de datos de configuración está en una base de datos de políticas.

Para desarrollar una política, se deben definir primero los requisitos, por ejemplo la seguridad y el rendimiento del tráfico. A continuación se proporciona un ejemplo de requisito de manejo de tráfico: *El tráfico que va entre una sucursal a través de Internet a la oficina corporativa debe estar protegido*. Este requisito se utiliza para definir lo que se conoce como ***política***. Para el requisito mencionado anteriormente, el dispositivo de red debe poder identificar cuáles de los paquetes que recibe proceden de la sucursal y están destinados a la oficina corporativa. Se crea un ***perfil*** basado en atributos, por ejemplo las direcciones IP de origen y destino o los protocolos, que deben compararse con los paquetes recibidos. Si los atributos del paquete coinciden con los atributos del perfil, se maneja el paquete de un modo prescrito por una definición de ***acción***. Como es de suponer, las acciones definen cuestiones tales como el cifrado y los métodos QoS.

Todas las políticas, los perfiles y las acciones pueden almacenarse en una base de datos. Mediante la utilización de una base de datos, determinados perfiles y acciones pueden volverse a utilizar y combinar de modos diferentes para crear múltiples políticas sin crear individualmente cada política en la configuración de dispositivo. La gestión de cambios se facilita mediante la posibilidad de efectuar un solo cambio en un objeto que se propagará a cualquier política que utilice dicho

objeto. Por ejemplo, múltiples túneles VPN pueden utilizar un método de cifrado común. Si se deseara cambiar el método de cifrado para todos los túneles, sólo sería necesario efectuar un cambio.

Cuatro protocolos podrán utilizar la base de datos de políticas. Estos protocolos son unos con datos repetitivos — repetitivos dentro de un dispositivo y posiblemente en toda la red. Se soportan los protocolos siguientes:

- RSVP
- DiffServ
- IKE
- IPSec

Cada política tiene un perfil de tráfico y un periodo de disponibilidad. Puede especificar que dicha política sólo se aplique al tráfico que llega y sale por interfaces específicas. Sólo es necesario identificar a los usuarios si va a especificar la acción IKE.

Una acción IPSec puede especificar una acción de eliminación, de pase o de seguridad. Si la acción es eliminar, todos los paquetes que coincidan con esta política se eliminarán. Si la acción es pasar sin seguridad, todos los paquetes pasarán en texto claro. Por otro lado, si la acción es pasar con seguridad, todos los paquetes se protegerán por medio de una SA especificada por esta acción. La acción IPSec también contiene las direcciones IP de los puntos finales del túnel para el túnel IPSec y las SA IKE.

Políticas definidas manualmente

Una opción para entrar políticas en la base de datos consiste en configurar manualmente cada dispositivo. En los direccionadores IBM, se utiliza la interfaz de la línea de mandatos (talk 6) o el programa de configuración para añadir objetos tales como políticas, perfiles, periodos de validez, acciones IPSec y otros objetos relacionados con la seguridad y el rendimiento. Como se ha mencionado anteriormente, algunos de estos objetos pueden volverse a utilizar con políticas diferentes lo cual reduce la cantidad de configuración manual. Esto puede ser aceptable e incluso deseable en una red pequeña, pero este método no funciona bien en redes grandes.

Políticas de un servidor LDAP

Una solución alternativa para configurar cada dispositivo de red consiste en entrar todas las políticas en un servidor central y distribuir las políticas a los dispositivos. El IETF ha propuesto que el servidor central sea un servidor LDAP y que cada dispositivo de red sea un cliente LDAP. Por ahora, es suficiente entender que el servidor LDAP puede almacenar y distribuir políticas. En la Figura 60 en la página 285, las políticas del lado derecho las distribuye el Servidor LDAP.

Para obtener una descripción adicional sobre este tema, apunte el navegador Web en la dirección siguiente:

`http://www.networking.ibm.com/support/networkutility/downloads`

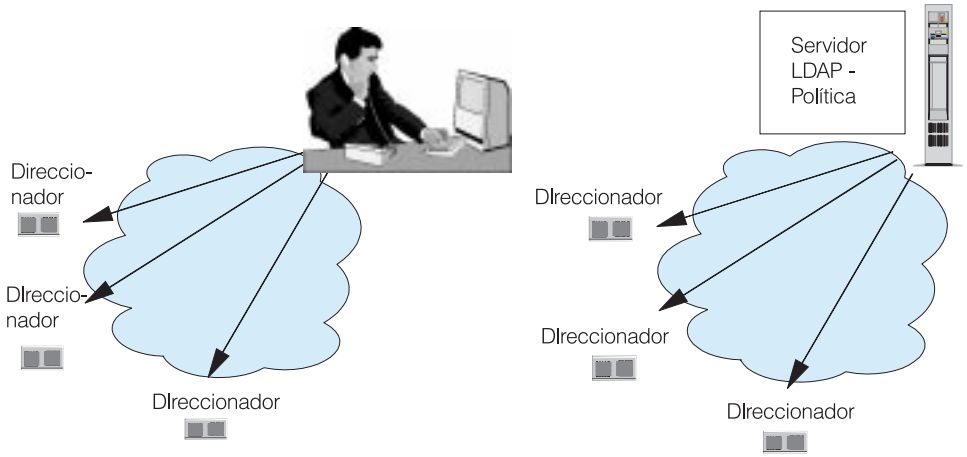


Figura 60. Distribución de política manual y mediante Servidor LDAP

IKE

Las direcciones IKE conciernen a los túneles manuales para IPSec. Los túneles manuales requieren la configuración manual difícil de claves y características de SA.

IKE, anteriormente conocido como ISAKMP/Oakley Key Resolution, define una infraestructura estandarizada para soportar la negociación automatizada de una SA, la generación inicial de todas las claves criptográficas y las renovaciones subsiguientes de dichas claves. Se utilizan las SA negociadas y los materiales de clave para proteger los intercambios IKE y también otras funciones de seguridad, por ejemplo AH y ESP. El intercambio seguro de claves es el factor más crítico al establecer un entorno de comunicaciones seguro. Dado que IKE se encarga de la inicialización de claves, debe ser capaz de ser utilizado a través de enlaces donde no se puede suponer ninguna seguridad. Los protocolos IKE utilizan las operaciones más complejas y que usan más intensivamente el procesador del conjunto de protocolos IPSec.

IKE necesita que todos los intercambios de información estén cifrados y autentificados. También se ha diseñado para proteger frente a varios peligros conocidos públicamente:

- **Rechazo de servicio:** Los mensajes se construyen con cookies exclusivos que se pueden utilizar para identificar y rechazar rápidamente mensajes no válidos sin necesidad de ejecutar operaciones criptográficas que utilizan intensamente el procesador.
- **Man-in-the-middle:** Se proporciona protección frente a los ataques comunes, por ejemplo la supresión de mensajes, las modificaciones de mensajes, la redundancia de mensajes al remitente, la reproducción de mensajes antiguos y el redireccionamiento de mensajes a destinatarios no propuestos.
- **Perfect Forward Secrecy (PFS):** El compromiso de claves anteriores no proporciona ninguna pista útil resultante del descifrado de otra clave tanto si se ha producido antes como después de la clave comprometida.

Certificados digitales y de claves precompartidas IKE

IKE tiene dos fases. En la fase I, las operaciones criptográficas son las que utilizan más intensamente el procesador, dado que esta fase está diseñada para intercambiar un ″secreto maestro″ cuando no hay seguridad en el lugar. El secreto maestro se utiliza para derivar las claves que se utilizarán para proteger el tráfico

de los usuarios. La fase I sólo atañe al establecimiento del conjunto de protecciones para los propios mensajes IKE; no establece ninguna SA de claves para proteger datos de usuario. Las operaciones de la fase I sólo necesitan efectuarse a veces y se puede utilizar una sola negociación de fase I para soportar múltiples intercambios de la fase II. La Figura 61 muestra los mensajes intercambiados en la Fase I. Estos 6 mensajes muestran los intercambios entre dos parejas en modalidad Principal.

Modalidad principal:

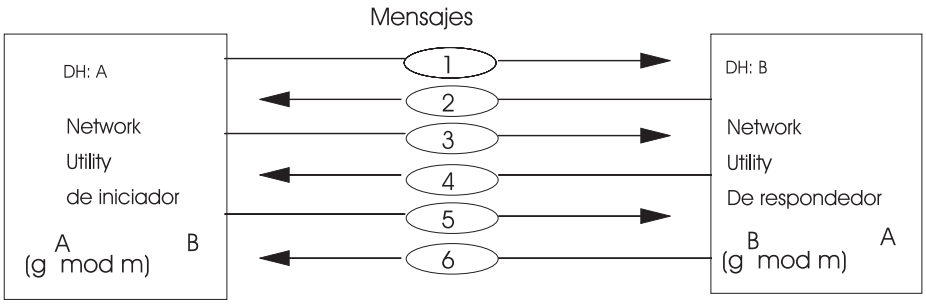


Figura 61. Intercambio de mensajes de Fase I en modalidad Principal de IKE

El igual IKE que desea establecer un túnel ISAKMP envía el mensaje 1. El primer mensaje está compuesto por una cabecera IP estándar y una cabecera UDP. Todos los mensajes ISAKMP se transportan en un paquete UDP con el puerto de destino 500. La carga útil de UDP está compuesta por una cabecera ISAKMP, una carga útil SA y una o más cargas útiles de propuestas y transformaciones.

El mensaje 2 contiene la única propuesta y transformación que el respondedor desea aceptar.

El mensaje 3 y el mensaje 4 intercambian información de la que finalmente se derivarán las claves criptográficas. Toda la información se intercambia abiertamente. Los mensajes contienen una carga útil de intercambio de claves y la carga útil nonce. La carga útil de intercambio de claves contiene el valor público Diffie-Hellman (DH). El exponente es el valor privado DH que siempre se mantiene secreto. La carga útil nonce lleva un gran número aleatorio que se genera de acuerdo con directrices matemáticas muy estrictas. Esta carga útil se utiliza para garantizar que existe la conexión y para proteger frente a ataques de reproducción.

Ambos dispositivos IKE tienen ahora los valores públicos DH del otro y sus propias claves. Pueden efectuar el cálculo DH para generar un secreto compartido. El secreto compartido es el valor público DH a la potencia de la clave privada. En la Figura 61, los valores DH privados son A y B. En este caso, el secreto compartido es un número igual en ambos direccionadores que se ha obtenido utilizando los valores DH A y B. Los direccionadores ya se han puesto de acuerdo con el valor de *g* en los mensajes 1 y 2.

A partir de este punto, las claves pueden generarse con la información que ya se ha intercambiado y establecido. Ahora ambos direccionadores conocen:

- Dos valores nonce, N-i y N-r
- Su propio valor DH privado
- El valor DH público de su asociado, pk-i y pk-r
- Los cookies de iniciador y respondedor

- El algoritmo hash acordado
- El secreto compartido — el resultado del cálculo DH

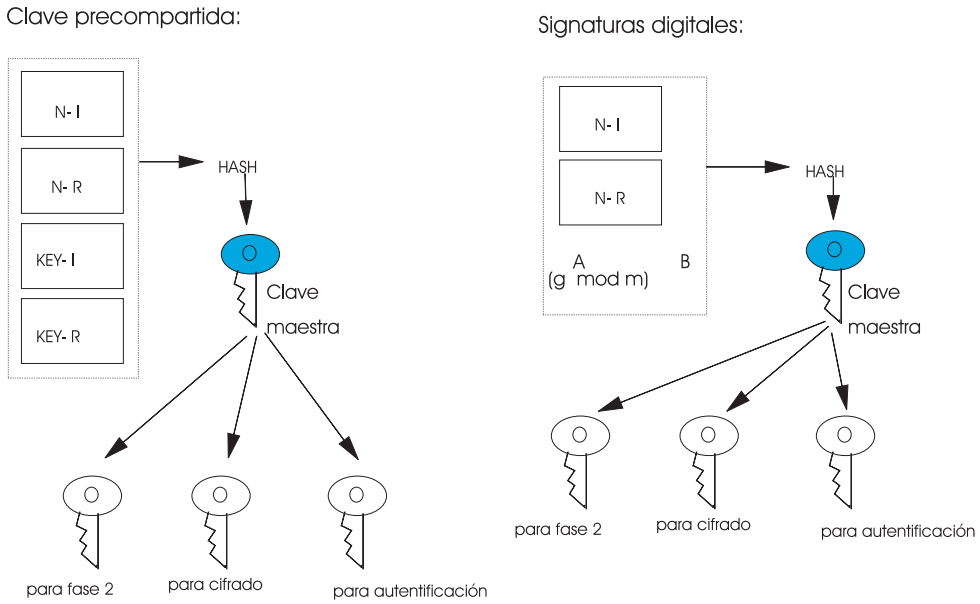


Figura 62. Generación de las claves

Como puede verse en la Figura 62, ambos dispositivos generan ahora una clave maestra, a la que se denomina SKEYID. Éste es el material de clave para el que se obtendrán las claves criptográficas reales. El método para generar las claves maestras depende del mensaje de autentificación acordado en el mensaje 2. Las opciones son:

Claves precompartidas
La clave maestra se obtiene a partir del hash de la clave precompartida con el nonce del iniciador (N-I) y el nonce del respondedor (N-R).

Signatura digital
La clave del maestro se obtiene a partir del hash del secreto compartido (resultado del cálculo DH) con el nonce del iniciador (N-I) y el nonce del respondedor (N-R).

La finalidad del mensaje 5 es permitir al respondedor autentificar al iniciador y el mensaje 6 permite al iniciador autentificar al respondedor. El formato de los mensajes depende de si los iguales IKE han acordado efectuar la autentificación a través de claves precompartidas o signaturas digitales.

En este momento, los mensajes de la fase I se completan en la modalidad principal. Cada igual se ha autentificado a sí mismo a su igual, ambos han acordado las características de la SA ISAKMP y han obtenido el mismo conjunto de material de clave.

Modalidad agresiva:
El otro planteamiento en la fase I es la modalidad agresiva. La modalidad agresiva utiliza menos intensivamente el procesador, con sólo 3 intercambios de mensajes en lugar de seis. Sin embargo, la modalidad agresiva es menos segura.

El mensaje 1 de la modalidad agresiva es similar al mensaje 1 de la modalidad principal en que ofrece al igual la opción de las SA ISAKMP. También incluye la carga útil de intercambio de claves, la carga útil nonce y las cargas útiles de identidad. Éstas se hubieran enviado en los mensajes 3 y 5 en modalidad principal. Esto significa que para la modalidad agresiva, la identidad del iniciador se envía en texto claro, a diferencia de la modalidad principal donde se envía cifrada.

El mensaje 2 en modalidad agresiva es el respondedor que indica cuál de las SA ISAKMP desea aceptar. En la respuesta, también incluye las cargas útiles que hubieran estado presentes en el mensaje 2, mensaje 4 y mensaje 6 de la modalidad principal.

Esto significa que la identidad del respondedor, su certificado y signatura se envía en texto claro, si la autentificación es a través de signaturas digitales. Si la autentificación es a través de claves precompartidas, la identidad y las cargas útiles de hash se transportan en texto claro. Recuerde que en el mensaje 6 de la modalidad principal, el material de autentificación se hubiera cifrado antes de enviarse.

El mensaje 3, que está cifrado, se envía para permitir al respondedor autentificar al iniciador. El iniciador envía la carga útil de hash (claves precompartidas) o la carga útil de certificado y signatura (modalidad de signatura digital) al respondedor. El contenido de las cargas útiles se describe en la descripción de modalidad principal. El respondedor utilizará entonces la información proporcionada para autentificar al iniciador como se describe para el mensaje 5 en modalidad principal.

Los intercambios de fase II negocian las SA y las claves que se utilizarán para proteger los intercambios de datos de usuario. Los mensajes IKE de la fase II están protegidos por la SA IKE generada en la fase I. Las negociaciones de la fase II se producen generalmente con más frecuencia que las de la fase I, normalmente una vez cada pocos minutos, mientras que las de la fase I pueden estar tan espaciadas como una vez al día.

En la fase II, el intercambio de mensajes empieza con ofertas del iniciador. En el mensaje 1, como puede verse en la Figura 63 en la página 289, el iniciador ofrece algunas opciones e información para calcular la clave compartida. Éstos son valores nonce de iniciador, DH público (pk-i), que son un número aleatorio grande (N-i). Toda esta información se transfiere en formato cifrado.

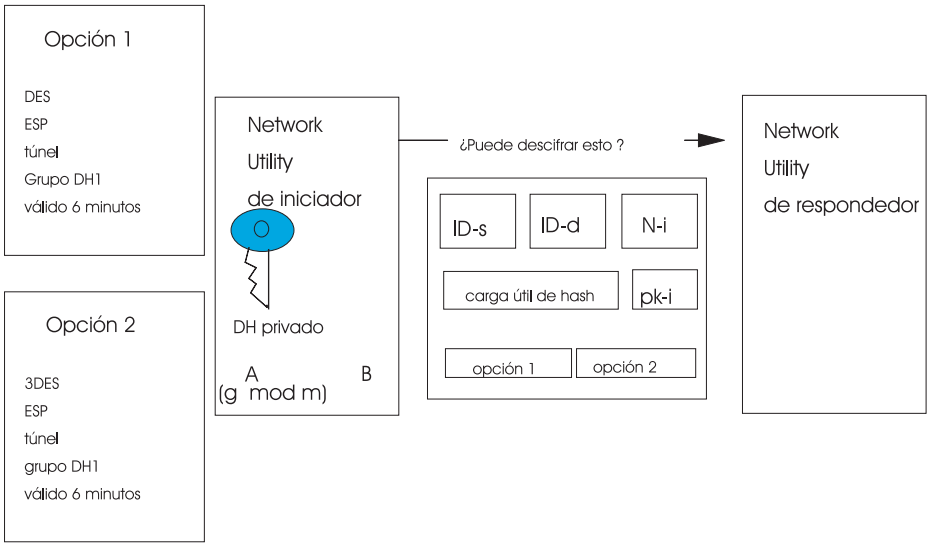


Figura 63. Mensaje 1 de la fase II

En el mensaje 2, el respondedor proporciona la información similar (N-r, pk-r), al iniciador además de éstos. Selecciona una de las opciones que se le han proporcionado a sí mismo.

Ahora cada Network Utility conoce lo siguiente acerca de los demás:

- Las nonces de los otros, N-I y N-R
- Las claves públicas de los demás (es decir, valores DH públicos)
- El índice de parámetros de seguridad (SPI): valor arbitrario de 32 bits que identifica de forma exclusiva una de las asociaciones de seguridad (de entrada o de salida).
- Los protocolos acordados
- El SKEYID_d calculado en la fase 1. Se trata del hash de la clave maestra, los dos cookies y el secreto DH compartido.

El cálculo DH se efectúa para generar el secreto compartido de la fase 2. El material de clave para el tráfico que va del respondedor al iniciador es el de SKEYID_d, el secreto compartido, protocolo, SPI del iniciador y dos nonces.

Todo el material de claves necesario no se ha intercambiado. El mensaje 3 prueba que la conexión está activa.

Protocolos de túneles

Consulte la publicación *Nways Multiprotocol Access Services Using and Configurating Features* para obtener una explicación de los protocolos siguientes.

Layer 2 Tunneling

El L2TP (Layer 2 Tunneling Protocol) (Protocolo de túneles de la capa 2) es el protocolo de pista del estándar IETF para el tráfico PPP (Point-to-Point Protocol) (Protocolo de punto a punto) de túneles a través de una red IP. L2TP utiliza un transporte UDP para los mensajes de definición de túnel y para transportar datos PPP entre puntos finales. L2TP es una arquitectura de cliente-servidor con un

cliente denominado LAC (L2TP Access Concentrator) (Concentrador de acceso L2TP) y el servidor denominado LNS (L2TP Network Server) (Servidor de red L2TP).

Layer 2 Forwarding

El L2F (Layer 2 Forwarding) (Reenvío de la capa 2) es un protocolo de túneles desarrollado por Cisco Systems, Inc. Proporciona las mismas soluciones que L2TP. Cuando el IETF desarrolló el L2TP, volvió a utilizar parte del L2F de Cisco y del PPTP de Microsoft. Los direccionadores IBM implementan L2F para interoperar con los direccionadores Cisco. Entre los direccionadores IBM, se utiliza L2TP porque es un estándar IETF.

L2F define dos dispositivos—un NAS y una pasarela de inicio.

Point-to-Point Tunneling Protocol

El PPTP (Point-to-Point Tunneling Protocol) (Protocolo de túneles de punto a punto) tiene el mismo propósito que L2TP: pasar paquetes PPP a través de una red IP. L2TP fue desarrollado por IETF y se basa en gran parte en PPTP y L2F (el equivalente de Cisco). Para establecer un túnel con un dispositivo Microsoft, es necesario que los direccionadores soporten el PPTP.

El PPTP es una arquitectura de cliente-servidor con un cliente denominado concentrador de acceso a red PPTP (PAC) y el servidor denominado servidor de red PPTP (PNS). De acuerdo con la arquitectura, el PAC es normalmente una estación de trabajo y el PNS, un servidor.

Túneles voluntarios con PPTP

Los túneles voluntarios son un modelo iniciado por el cliente. El cliente/PAC marca en el NAS, obtiene una dirección IP y establece el acceso a red normal. Después, abre otra sesión de marcación que establece el túnel PPTP. Existen dos escenarios en los que se pueden utilizar direccionadores IBM con un PPTP de túneles voluntarios. El direccionador IBM puede terminar el túnel o iniciar el túnel. Si termina el túnel, el cliente que inicia el túnel debe tener capacidad para PPTP y puede utilizar un dispositivo NT o Windows o cualquier otro dispositivo que soporte PPTP. En el segundo escenario, un direccionador puede establecer un túnel de retorno a un dispositivo PPTP, por ejemplo un servidor NT.

Túneles obligatorios con L2TP

Los túneles obligatorios son un modelo iniciado por el direccionador. En este escenario, el cliente no tiene conocimiento de L2TP. El cliente marca en el LAC y el LAC inicia el túnel de regreso L2TP al LNS. En este caso, el LAC envía una petición de llamada de entrada al LNS. Dado que el cliente y el LAC ya han negociado la autentificación parcial y LCP, el LAC ha pasado esta información al LNS en lo que se denomina autentificación de proxy. Después del establecimiento de llamada, el LNS completa la autentificación de PPP y la fase de red con el cliente a través del túnel recién formado.

Soporte de anotación cronológica de sucesos (ELS) de VPN

Los cuatro subsistemas siguientes le ayudarán a depurar y determinar el estado de la configuración VPN.

Subsistema L2

El Subsistema L2 contiene los Mensajes ELS para todos los protocolos de túneles de la capa 2 incluyendo L2F, L2TP y PPTP. Este subsistema muestra información acerca del establecimiento y terminación de túneles y llamadas. También muestra información acerca de los paquetes recibidos y transmitidos a través de los túneles L2. También se visualizan mensajes de error resultantes de una negociación anómala del túnel.

Subsistema PLCY

Los mensajes ELS para el Subsistema PLCY informan acerca del estado de la renovación de la base de datos de políticas, indican cuántas reglas se han cargado en la base de datos y proporcionan información acerca de errores que pueden haberse producido cuando se estaba creando la base de datos de políticas. Puede consultar la información de paquetes para conocer las consultas de la base de datos de políticas, qué reglas y acciones se han producido como resultado de estas consultas y los errores u otra información pertinente a las negociaciones que incluyen la base de datos de políticas.

Subsistema IPSP

El Subsistema IPSP contiene mensajes para el módulo IPSec del direccionador. El subsistema IPSP muestra información acerca del cifrado y descifrado de paquetes, los algoritmos que se están utilizando y los mensajes de error resultantes de paquetes eliminados debido a anomalías.

Subsistema IKE

El Subsistema IKE muestra información acerca de las negociaciones de la fase I y fase II que finalmente configuran un Túnel IPSec seguro entre dos sistemas principales o pasarelas de seguridad. Se visualizarán los errores resultantes de negociaciones anómalas debido a la discrepancia de claves precompartidas, discrepancias de propuestas de seguridad o errores de política.

Capítulo 20. Ejemplos de redes privadas virtuales

En este capítulo, encontrará los ejemplos siguientes que muestran soluciones básicas de VPN:

- VPN IPSec de direccionador a direccionador utilizando claves precompartidas
- VPN de direccionador a direccionador utilizando certificados digitales
- Túnel PPTP voluntario con terminación de direccionador de IBM
- Túnel PPTP voluntario iniciado por Network Utility de IBM
- Túnel L2TP voluntario iniciado por Network Utility de IBM
- Túnel L2TP terminado en un LNS de Network Utility de IBM

VPN IPSec de direccionador a direccionador utilizando claves precompartidas

Este ejemplo utiliza IPSec con la generación automática de claves y claves precompartidas. En la Figura 64, se crea un túnel seguro de pasarela a pasarela. Este túnel autentificará y cifrará el tráfico de sistemas principales específicos y excluirá todo el resto de tráfico. El perfil describe exactamente a qué sistemas principales en cada extremo del túnel se les permite pasar datos a través del túnel. La política puede permitir un solo sistema principal en cada extremo, una o múltiples subredes en cada extremo o cualquier combinación de las dos opciones. La limitación de túneles de pasarela a pasarela consiste en que no se produce autentificación o cifrado en la LAN. Esta solución no proporciona seguridad en la LAN.

La red utilizada para este ejemplo (Figura 64) consta de dos segmentos de Red en Anillo conectados por dos direccionadores IBM 2210. En un escenario real, el enlace serie entre los direccionadores puede ser cualquier red de área amplia (WAN) privada o pública.

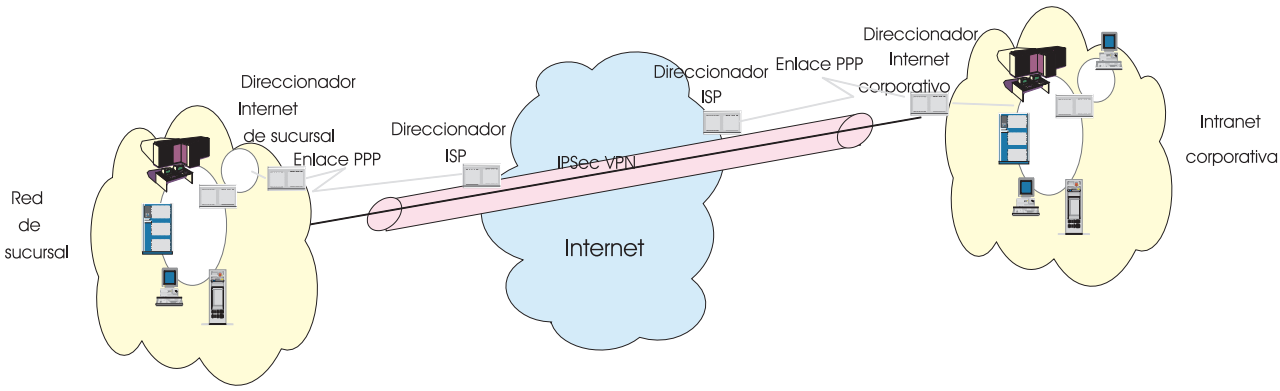


Figura 64. Red física utilizada para las configuraciones de ejemplo

En la Figura 65 en la página 294, el túnel debe autentificar y cifrar todo el tráfico entre la Subred 9.24.106.0 (a través del direccionador de bifurcación VPNRTR2 y el direccionador corporativo VPNRTR1) y la Subred 192.168.141.32. Ningún otro tráfico de ninguna otra subred puede atravesar el enlace entre los dos direccionadores. La autentificación garantiza que se configure un túnel entre los puntos finales correctos y el cifrado impide que los datos se interpreten mientras cruzan la WAN.

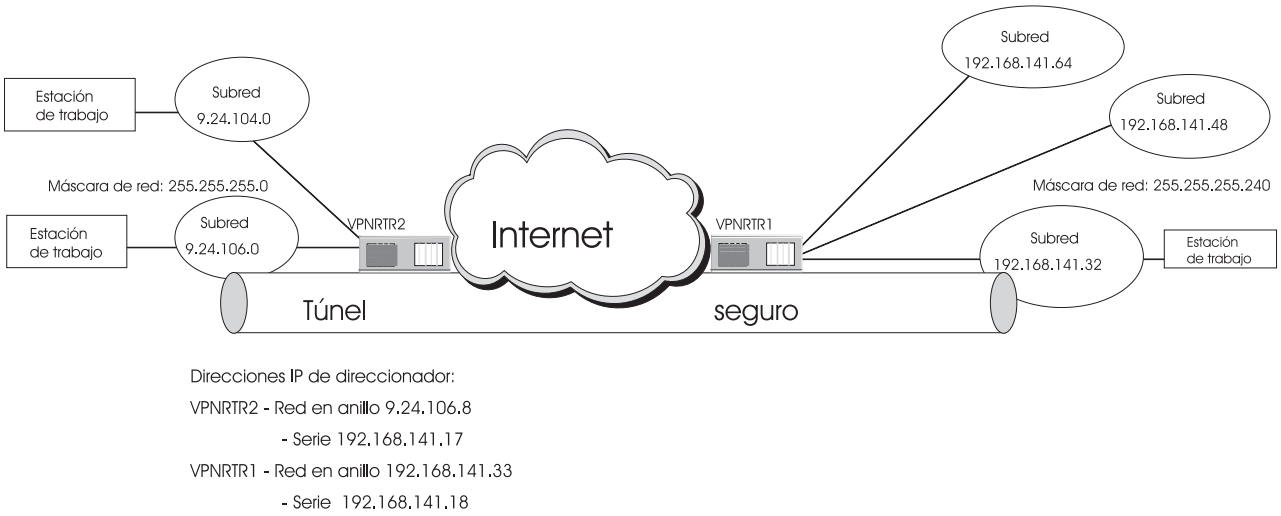


Figura 65. Red de ejemplo utilizada para IPSec con claves precompartidas

Crear una política para el túnel IPSec para VPNRTR1

Siga estos pasos para configurar el direccionador:

1. Habilitar la Seguridad IP
2. Crear la clave precompartida
3. Añadir una política
4. Añadir un perfil
5. Añadir un periodo de validez
6. Añadir una acción IPSec
7. Añadir una propuesta IPSec
8. Añadir una transformación ESP
9. Añadir una acción ISAKMP
10. Añadir una propuesta ISAKMP

Habilitar la Seguridad IP

Desde la interfaz de la línea de mandatos de Talk 6, habilite la Seguridad IP a nivel del sistema.

Tabla 78. Habilitar la Seguridad IP

```
VPNRTR1  *TALK 6
Gateway user configuration
VPNRTR1 Config>feature ipsec
IP Security feature user configuration
IPsec config>ipv4
VPNRTR1 IPV4-IPsec config>ENABLE IPSEC
It is necessary to restart the router for IPsec to be active.
VPNRTR1 IPV4-IPsec config>EXIT
VPNRTR1 IPsec config>EXIT
```

Crear la clave precompartida

Se debe configurar una clave precompartida para cada usuario remoto. Por esta razón, las claves precompartidas no son muy escalables. Sin embargo, las claves precompartidas se renuevan con regularidad, lo que les da ventaja respecto al método de túnel manual.

Para configurar las claves se utiliza el mandato **Add User** de Talk 6.

Tabla 79. Añadir el usuario PPP

```
VPNRTR1 Config>FEATURE Policy
IP Network Policy configuration VPNRTR1 Policy config>ADD USER
Choose from the following ways to identify a user:      1
        1: IP Address
        2: Fully Qualified Domain Name
        3: User Fully Qualified Domain Name
        4: Key ID (Any string)
Enter your choice(1-4) [1]? 1
Enter the IP Address that distinguishes this user
 [0.0.0.0]? 192.168.141.17                          2
Group to include this user in []?
Authenticate user with 1:pre-shared key or 2: Public Certificate [1]? 1
Mode to enter key (1=ASCII, 2=HEX) [1]? 1
Enter the Pre-Shared Key (an even number of 2-128 ascii chars):
Enter the Pre-Shared Key again (3 characters) in ascii:       3


Here is the User Information you specified...

Name      = 192.168.141.17
Type      = IPV4 Addr
        Group     =
        Auth Mode =Pre-Shared Key
        Key(Ascii)=key                                  3
Is this correct? [Yes]:
```

1. El direccionador necesita saber cómo reconocer el igual IKE remoto y la clave precompartida.
2. En este ejemplo, el identificador elegido era la dirección IP (IP Address). Ésta debe ser la dirección del punto final de túnel del direccionador remoto — en este ejemplo, la dirección IP de la interfaz WAN de VPNRTR2.
3. La clave debe entrarse dos veces para validarla y debe ser exactamente la misma para cada direccionador de los puntos finales del túnel. En este ejemplo, se utiliza la palabra **key**. Puede utilizar cualquier clave con un máximo de 128 caracteres. Sin embargo, debe entrar exactamente la misma clave dos veces en cada direccionador. El modo más fácil para hacerlo consiste en escribir la clave en un editor de texto y luego cortar y pegar la clave en el campo de entrada de los indicadores de Talk 6.

Añadir la política

Una política es la infraestructura para describir cómo debe manejarse el tráfico que entra o sale del direccionador. Sin control de acceso, el direccionador sólo toma decisiones de direccionamiento. Mediante la utilización de la política, el direccionador toma decisiones tales como, por ejemplo, pasar el paquete a través de la interfaz, determinar si es necesario autentificar el paquete y si es necesario cifrar o descifrar el paquete. La política une otros objetos. Este ejemplo utiliza primero el mandato **Add Policy**. Éste es probablemente el modo más fácil de crear la primera política, dado que le solicita que entre toda la información necesaria en el orden correcto.

Si una política crea un túnel de seguridad, sólo se cifrarán y reenviarán los paquetes que coincidan con el perfil. Otros paquetes que no coincidan con el perfil se pasarán en texto claro a no ser que otra política los desactive explícitamente. Cuando existe más de una política en un direccionador, las políticas se evalúan de acuerdo con el número de prioridad.

Consulte la Figura 66 para ver cómo se evalúa un paquete de entrada con múltiples políticas. Si el paquete coincide con el perfil para la Política núm. 1, se envía a IPSec para procesarse. Si el paquete no coincide con el perfil para la Política núm. 1, se evalúa con el perfil para la Política núm. 2. Este proceso continúa hasta que se evalúa el paquete de entrada con todas las políticas. Si el paquete no coincidiera con ningún perfil, se enviaría en texto claro al protocolo de direccionamiento para procesarse.

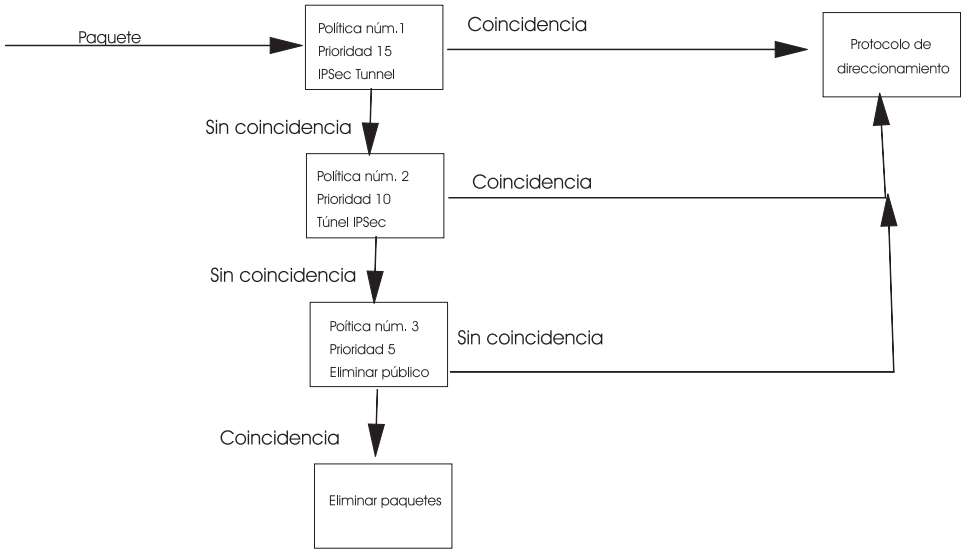


Figura 66. Efecto de múltiples políticas

Tabla 80. Crear una política nueva

```
VPNRTR1 Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? ike-pre-32-106
Enter the priority of this policy (This number is used to determine
the policy to enforce in the event of policy conflicts) [5]? 15              1
List of Profiles:
        0: New Profile                  2
```

1. La prioridad de la política especifica el orden en que se evaluarán múltiples políticas. Las políticas con un número más alto se evalúan antes que las políticas con un número más bajo. Consulte la Figura 66 para ver el flujo de evaluación de paquetes cuando se definen múltiples políticas.
2. Después de añadir una política, deberá crear un perfil para asociarlo con la política. Dado que no se ha creado ningún perfil en este direccionador, se solicita que se cree un perfil nuevo.

Añadir el perfil

El perfil describe los criterios utilizados para determinar si una política debe actuar en un paquete. Estos criterios incluyen la dirección de origen y destino, el protocolo, el tipo de puerto y el byte de Servicios diferenciados (DS/TOS).

Tabla 81. Añadir el perfil

```
List of Profiles:
        0: New Profile
Enter a Name (1-29 characters) for this Profile []? 32-106        1
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?        2
Enter IPV4 Source Address [192.168.141.32]?
Enter IPV4 Source Mask [255.255.255.240]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [9.24.106.0]?
Enter IPV4 Destination Mask [255.255.255.0]?

Protocol IDs:
     1)  TCP
     2)  UDP
     3)  All Protocols
     4)  Specify Range

Select the protocol to filter on (1-4) [3]?         3
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?        4
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]: YES         5
Enter local identification to send to remote
     1)  Local Tunnel Endpoint Address
     2)  Fully Qualified Domain Name
     3)  User Fully Qualified Domain Name
     4)  Key ID (any string)
Select the Identification type (1-4) [1]?
Any user within profile definition allowed access? [Yes]:
Limit this profile to specific interface(s)? [No]:


...continued on next screen
```

1. Aquí se utiliza el nombre descriptivo 106-32.
2. En este ejemplo, cualquier sistema principal de una subred podría acceder a cualquier sistema principal de la otra subred.
3. Puede configurar el perfil para permitir sólo determinados protocolos y determinados puertos si desea limitar los servicios de forma adicional. Por ejemplo, puede permitir sólo Telnet y no FTP permitiendo sólo el puerto 23 de TCP.
4. El byte DS está relacionado con QoS o la prioridad. Puede seleccionar el tráfico que coincide con el perfil por nivel de prioridad.
5. Este paso de configuración de ID locales y remotos para ISAKMP es opcional a no ser que el igual deba identificarle con algún elemento más que sea distinto de la dirección IP.

Tabla 82. Confirmar el perfil

```
Here is the Profile you specified...


Profile Name    = 32->106
        sAddr:Mask= 192.168.141.32: 255.255.255.240 sPort=    0 : 65535
        dAddr:Mask= 9.24.106.0 : 255.255.255.0   dPort=    0 : 65535
        proto     =              0 : 255
        TOS       =            x00 : x00
        Remote Grp=All Users
Is this correct? [Yes]:
List of Profiles:
        0: New Profile
        1: 32->106

Enter number of the profile for this policy [1]? 1
```

Añadir el periodo de validez

El periodo de validez es el periodo de tiempo durante el cual es válida la política. Puede configurar el periodo de validez para especificar una duración para la validez de la política o especificar los meses del año, los días de la semana y las horas del día durante los cuales la política es válida. Esta flexibilidad permite al administrador de red especificar cuándo es válida una política. Por ejemplo, los requisitos pueden ser ″todo el tiempo″ o ″sólo este año durante enero y febrero″ o ″sólo de lunes a viernes de 9 AM a 5 PM″. Estos requisitos pueden convertirse en valores de configuración utilizando el mandato **Add Validity Period**.

Tabla 83. Añadir el periodo de validez

```
List of Validity Periods:              1
        0: New Validity Period

Enter number of the validity period for this policy [0]?
Enter a Name (1-29 characters) for this Policy Valid Profile []? always
Enter the lifetime of this policy. Please input the
information in the following format:
               yyyymmddhhmmss:yyyymmddhhmmss OR '*' denotes forever.
 [*]? *
During which months should policies containing this profile
be valid.  Please input any sequence of months by typing in
the first three letters of each month with a space in between
each entry, or type ALL to signify year round.
 [ALL]?
During which days should policies containing this profile
be valid.  Please input any sequence of days by typing in
the first three letters of each day with a space in between
each entry, or type ALL to signify all week
 [ALL]?
Enter the starting time (hh:mm:ss or * denotes all day)
 [*]?


Here is the Policy Validity Profile you specified...


Validity Name   = always                       2
        Duration  = Forever
        Months    = ALL
        Days      = ALL
        Hours     = All Day
Is this correct? [Yes]:
List of validity periods:
      0: New Validity Period
      1: always
Enter number of the validity period for this policy [1]?
```

1. Dado que está creando una política nueva, se le solicita que cree un periodo de validez. En algunos casos, puede volver a usar un periodo de validez que se ha creado anteriormente. En ejemplos posteriores de este capítulo verá que se utiliza un periodo de validez existente. Este concepto es válido para todos los objetos de la base de datos de políticas. Cuando sea apropiado, se puede volver a usar cualquier objeto.
2. El periodo de validez de nuestro ejemplo se ha configurado para estar en vigor en todo momento.

Añadir la acción IPSec

Además de un perfil y de un periodo de validez, una política debe asociarse también con una acción IPSec, un IPsec manual o una acción DiffServ. En este escenario, se configura una acción IPSec.

Una acción IPSec puede especificar una acción de eliminación, de pase o de seguridad. Si la acción es eliminar, todos los paquetes que coincidan con el perfil utilizado por esta política se eliminarán. Si la acción es pasar sin seguridad, todos los paquetes se pasarán en texto claro. Si la acción es pasar con seguridad, todos los paquetes se protegerán por medio de la SA especificada por esta acción. La acción IPSec también contiene las direcciones IP de los puntos finales del túnel IPSec y las SA IKE.

Tabla 84. Añadir la acción IPSec

```
Should this policy enforce an IPSEC action? [No]: y
IPSEC Actions:
        0: New IPSEC Action

Enter the Number of the IPSEC Action [0]?
Enter a Name (1-29 characters) for this IPsec Action []? tunnel_vpnrtr1-vpnrtr2
List of IPsec Security Action types:
     1)  Block (block connection)
     2)  Permit

Select the Security Action type (1-2) [2]?
Should the traffic flow into a secure tunnel or in the clear:
     1) Clear
     2) Secure Tunnel
 [2]?
Enter Tunnel Start Point IPV4 Address
 [192.168.141.18]?
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
 [0.0.0.0]? 192.168.141.17
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:        1
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
Security Association Refresh Threshold, in percent (1-100) [85]?
Options for DF Bit in outer header (tunnel mode):           2
     1)  Copy
     2)  Set
     3)  Clear
Enter choice (1-3) [1]?
Enable Replay prevention (1=enable, 2=disable) [2]?          3
Do you want to negotiate the security association at
system initialization(Y-N)? [No]: y          4
```

1. Entonces se le solicitará si el túnel IPSec negociado desemboca en otro túnel. Esto está relacionado con la característica de túnel a túnel que se enviaba primero en la V3.2 del código. En la Figura 67 se muestra un escenario de túnel en túnel:

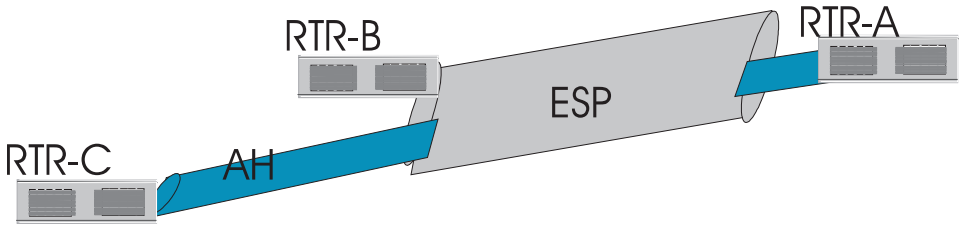


Figura 67. Túnel en un túnel

Todo el tráfico entre RTR-A y RTR-C debe autentificarse, pero todo el tráfico entre RTR-A y RTR-B debe cifrarse. La diferencia de túnel en túnel consiste en que los túneles empiezan en el mismo punto pero terminan en puntos diferentes. Para este ejemplo, la respuesta es no.

2. Al crear la cabecera IPSec, muchos de los campos de la cabecera IP se copian de la cabecera del paquete que se está protegiendo. Puede controlar cómo se establece el campo **don't fragment** (no fragmentar). Puede copiar del paquete original, establecer el bit DF o, si está activado en el paquete original, desactivarlo. El establecimiento del bit DF tiene implicaciones para IPSec. Examine el diagrama más abajo.

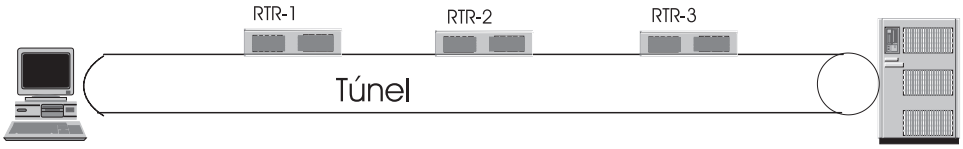


Figura 68. Interpretación del bit DF

El tráfico fluye del dispositivo de la izquierda al dispositivo de la derecha. RTR-2 necesita fragmentar el paquete pero no puede hacerlo porque se ha establecido el bit DF. RTR-2 generará un mensaje indicando que el paquete ICMP es demasiado grande y lo enviará al remitente del paquete, RTR-1. Entonces RTR-1 necesita informar al remitente que el paquete es demasiado grande. Esto puede producir problemas para RTR-1 porque (a) puede que el paquete ICMP no contenga una parte suficiente del paquete original para poder determinar quién es el remitente o (b) puede que la dirección IP esté cifrada. Si RTR-1 no puede determinar quién es el remitente, almacenará información de túnel y esperará a que llegue otro paquete para ese túnel. Cuando llegue ese paquete, RTR-1 generará, si es necesario, el mensaje que indica que el paquete ICMP es demasiado grande. Por consiguiente, considere cuidadosamente el valor del bit DF.

En este ejemplo, hemos establecido el bit DF en copy (copiar) (el valor por omisión).

3. **Enable replay prevention** (Habilitar prevención de reproducción) define si deben comprobarse los números de secuencia en los paquetes recibidos.
4. Este parámetro controla si se debe crear esta SA al arrancar el sistema. Si se especifica **no**, se indica que esta SA sólo deberá negociarse cuando se reciban paquetes que coincidan con la política.

A continuación de este paso, se nos solicita que seleccionemos una propuesta IPSec. Dado que no existe ninguna propuesta anterior, la única opción es crear una nueva.

Añadir una propuesta IPSec

La propuesta IPSec contiene la información acerca de la transformación ESP y/o AH que se debe proponer o con la que se debe efectuar la comprobación durante las negociaciones ISAKMP de la fase 2. Consulte el apartado “IKE” en la página 285 para obtener una explicación de las negociaciones de la fase 2. Si necesita pfs (perfect forward secrecy) (secreto de reenvío perfecto), la propuesta IPSec identifica el grupo DH (Diffie-Hellman) que se debe utilizar. Las transformaciones a las que hace referencia la propuesta IPSec se envían o se comprueban con el orden en que se han especificado. La primera transformación ESP o AH de la lista debe ser la que sea más apropiada para utilizar. Si hay más de una transformación en la lista, se compara cada una con la lista de transformaciones del igual para encontrar una coincidencia. Si ninguna de las transformaciones configuradas coincide con la lista del igual, falla la negociación. La propuesta IPSec puede listar una combinación de transformaciones AH y ESP, pero las únicas combinaciones válidas son:

- Lista de AH solamente (modalidad de túnel o transporte)
- Lista de ESP solamente (modalidad de túnel o transporte)
- Lista de AH (modalidad de transporte) y lista de ESP (modalidad de túnel)
  - AH (modalidad de transporte) + ESP (modalidad de transporte) define la modalidad de transporte

– AH (modalidad de túnel o transporte) + ESP (modalidad de túnel o transporte) define la modalidad de túnel

Tabla 85. Adición de la propuesta IPSec

```
You must choose the proposals to be sent/checked against during phase 2
negotiations.  Proposals should be entered in order of priority.

List of IPSEC Proposals:         1
        0: New Proposal

Enter the Number of the IPSEC Proposal [0]?
Enter a Name (1-29 characters) for this IPsec Proposal []? esp-prop1
Does this proposal require Perfect Forward Secrecy?(Y-N)? [No]:
Do you wish to enter any AH transforms for this proposal? [No]:
Do you wish to enter any ESP transforms for this proposal? [No]: y         2
```

1. Puesto que ha especificado una acción IPSec, se le solicita que cree una propuesta nueva.
2. Escriba **y** para entrar una transformación ESP y se le solicitará que añada la transformación.

Añadir una transformación IPSec

Los atributos de la transformación IPSec contienen información acerca de los parámetros de cifrado y autentificación de IPSec y también especifican la frecuencia con la que se renuevan las claves. La transformación es AH (sólo autentificación) o ESP (cifrado y/o autentificación) y puede configurarse para operar en modalidad de túnel o de transporte.

Tabla 86. Añadir la transformación IPSec

```
List of ESP Transforms:
        0: New Transform

Enter the Number of the ESP transform [0]?
Enter a Name (1-29 characters) for this IPsec Transform []? esp-trans1
List of Protocol IDs:
     1)  IPSEC AH
     2)  IPSEC ESP

Select the Protocol ID (1-2) [1]? 2
List of Encapsulation Modes:
     1)  Tunnel                              1
     2)  Transport

Select the Encapsulation Mode(1-2) [1]?
List of IPsec Authentication Algorithms:          2
0)  None
     1)  HMAC-MD5
     2)  HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [2]?
List of ESP Cipher Algorithms:
     1)  ESP DES
     2)  ESP 3DES
     3)  ESP CDMF
     4)  ESP NULL

Select the ESP Cipher Algorithm (1-4) [1]?           3
Security Association Lifesize, in kilobytes (1024-65535) [50000]?           4
Security Association Lifetime, in seconds (120-65535) [3600]?


Here is the IPSec transform you specified...


Transform Name  = esp-trans1
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =DES
Is this correct? [Yes]: y
List of ESP Transforms:
        0: New Transform
        1: esp-trans1

Enter the Number of the ESP transform [1]?
Do you wish to add another ESP transform to this proposal? [Yes]: n
```

1. La modalidad de transporte es una SA definida entre dos estaciones finales. La modalidad de túnel se utiliza cuando uno de los dispositivos como mínimo es una pasarela de seguridad (por ejemplo, un direccionador). Hemos seleccionado la modalidad de túnel dado que nuestra SA está entre dos direccionadores.
2. Éstos son los métodos de autentificación. HMAC_SHA es más seguro que HMAC_MD5.
3. Seleccione el método de cifrado. Tenga en cuenta que ESP 3DES no está permitido fuera de EE.UU.
4. Establezca el tiempo de vida/tamaño natural (lifetime/lifesize) de la SA. Cuando caduque la SA, IKE realizará otro cálculo de fase II para renovar las claves. Se ha establecido el valor por omisión de 3600 segundos. Esto significa que alguien que pueda interceptar uno de los paquetes sólo tendría 1 hora para descifrar el código. En una ocasión, un grupo de estudiantes universitarios demostraron que el cifrado DES solo puede descifrarse en 22 horas.

Después de añadir la transformación IPSec, se le solicitará que confirme la propuesta IPSec.

Tabla 87. Confirmar la propuesta IPSec

```
Here is the IPSec proposal you specified...


Name  = esp-prop1
        Pfs   = N
        ESP Transforms:
                esp-trans1
Is this correct? [Yes]: y
List of IPSEC Proposals:
        0: New Proposal
        1: esp-prop1

Enter the Number of the IPSEC Proposal [1]?
Are there any more Proposal definitions for this IPSEC Action? [No]:
```

Después de crear la transformación y la propuesta IPSec, podemos finalizar la acción IPSec. Se nos proporciona una pantalla de confirmación y se nos solicita que seleccionemos la acción que se debe asociar con la política.

Tabla 88. Confirmar la acción IPSec

```
Here is the IPSEC Action you specified...

IPSECAction Name = tunnel_vpnrtr1-vpnrtr2
        Tunnel Start:End         = 192.168.141.18 : 192.168.141.17
        Tunnel In Tunnel         =              No
        Min Percent of SA Life   =              75
        Refresh Threshold        =              85 %
        Autostart                =             Yes
        DF Bit                   =            COPY
        Replay Prevention        =        Disabled
        IPSEC Proposals:
                esp-prop1
Is this correct? [Yes]:
IPSEC Actions:
        0: New IPSEC Action
        1: tunnel_vpnrtr1-vpnrtr2

Enter the Number of the IPSEC Action [1]?
```

Añadir la acción ISAKMP

Dado que se ha especificado una acción IPSec segura, se le solicitará automáticamente que cree una acción ISAKMP. En la mayoría de los casos, es suficiente una acción ISAKMP y una propuesta ISAKMP para todas las políticas de seguridad. Los algoritmos y los métodos que elija serán probablemente parámetros estratégicos para toda la empresa. Por ejemplo, su compañía tomará una decisión basándose en requisitos de seguridad corporativos, por ejemplo elegir entre maximizar niveles de cifrado o encontrar un equilibrio entre la confidencialidad y el rendimiento. Como con cualquier diseño de seguridad, la configuración original debe comprobarse y supervisarse para asegurar que está soportando correctamente sus intenciones. La acción ISAKMP especifica la información de gestión clave para la fase I. Consulte el apartado “IKE” en la página 285 para obtener una explicación de las negociaciones de la fase I y fase II.

Tabla 89. Añadir la acción ISAKMP

```
ISAKMP Actions:
        0: New ISAKMP Action

Enter the Number of the ISAKMP Action [0]?
Enter a Name (1-29 characters) for this ISAKMP Action []? ike-1

List of ISAKMP Exchange Modes:            1
     1)  Main
     2)  Aggressive

Enter Exchange Mode (1-2) [1]?
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
ISAKMP Connection Lifesize, in kilobytes (100-65535) [5000]?        2
ISAKMP Connection Lifetime, in seconds (120-65535) [30000]?
Do you want to negotiate the security association at
system initialization(Y-N)? [Yes]:           3
```

1. Las modalidades de intercambio están relacionadas con el nivel de seguridad durante las negociaciones de la fase 1. La modalidad agresiva es más rápida puesto que tiene un número menor de mensajes intercambiados pero es menos segura porque se envía la identidad del iniciador en texto claro. Se selecciona que la acción se produzca en modalidad principal.
2. Connection Lifesize (Tamaño natural de conexión) y Connection Lifetime (Tiempo de vida de conexión) controlan cuándo se negociará una nueva SA. Esta renovación de claves puede durar varios segundos, de modo que cuanto menores sean los números, mayor será la frecuencia con la que se producirá una renovación. Como sucede con muchas opciones relacionadas con la seguridad, se necesita un buen equilibrio entre el rendimiento y los requisitos de seguridad.
3. Hemos seleccionado negociar la SA en la inicialización con el fin de mejorar el rendimiento de las transacciones iniciales que se produce en el túnel.

Añadir la propuesta ISAKMP

La propuesta ISAKMP especifica los atributos de cifrado y autentificación de la SA de la fase I. También especifica qué grupo DH se debe utilizar para generar las claves y la vida de la seguridad de la fase I.

Tabla 90. Añadir la propuesta ISAKMP (Pantalla 1 de 2)

```
You must choose the proposals to be sent/checked against during phase 1
negotiations.  Proposals should be entered in order of priority.
List of ISAKMP Proposals:
        0: New Proposal

Enter the Number of the ISAKMP Proposal [0]? 0
Enter a Name (1-29 characters) for this ISAKMP Proposal []? ike-prop1

List of Authentication Methods:
     1)  Pre-Shared Key
     2)  RSA SIG

Select the authentication method (1-2) [1]? 1

List of Hashing Algorithms:
     1)  MD5
     2)  SHA

Select the hashing algorithm(1-2) [1]? 1

List of Cipher Algorithms:
     1)  DES
     2)  3DES

Select the Cipher Algorithm (1-2) [1]? 1

...continued
```

Tabla 91. Añadir la propuesta ISAKMP (Pantalla 2 de 2)

```
Security Association Lifesize, in kilobytes (100-65535) [1000]?
Security Association Lifetime, in seconds (120-65535) [15000]?

List of Diffie Hellman Groups:
     1)  Diffie Hellman Group 1
     2)  Diffie Hellman Group 2

Select the Diffie Hellman Group ID from this proposal (1-2) [1]?        1


Here is the ISAKMP Proposal you specified...

Name = ike-prop1
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = MD5
        Encr Algo  = DES CBC
Is this correct? [Yes]:
List of ISAKMP Proposals:
        0: New Proposal
        1: ike-prop1

Enter the Number of the ISAKMP Proposal [1]?
Are there any more Proposal definitions for this ISAKMP Action? [No]:
```

1. Seleccione 1 para las claves precompartidas. Si quisiéramos utilizar certificados para la autentificación, habríamos seleccionado RSA-SIG.

Una vez que se han creado todos los objetos necesarios para una política de túnel segura, se presenta un resumen de la política. La política definida — ike-pre-32-106 — tiene una prioridad de 15 y definirá un túnel seguro entre la subred 192.168.141.32 y la subred 9.24.106.0. La acción IPSec especifica un túnel

seguro que estará siempre en vigor tal como especifica el periodo de validez. Los paquetes a los que se permite entrar en el túnel los determina el perfil que describe las dos subredes. Los métodos de autentificación y cifrado se especifican en la acción ISAKMP y la propuesta ISAKMP.

Tabla 92. Confirmar la acción ISAKMP

```
Here is the ISAKMP Action you specified...


ISAKMP Name     = ike-1
        Mode                    =            Main
        Min Percent of SA Life  =              75
        Conn LifeSize:LifeTime  =            5000 : 30000
        Autostart               =             Yes
        ISAKMP Proposals:
                ike-prop1
Is this correct? [Yes]: y
ISAKMP Actions:
        0: New ISAKMP Action
        1: ike-1

Enter the Number of the ISAKMP Action [1]?
```

Confirmar la política

Después de confirmar la acción y la política ISAKMP, puede que desee configurar una acción DiffServ. En ese caso, se presentará un resumen de la política para su confirmación.

Tabla 93. Confirmar la política

```
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?

Here is the Policy you specified...


Policy Name     = ike-pre-32-106
        State:Priority =Enabled    : 15
        Profile        =32-106
        Valid Period   =always
        IPSEC Action   =tunnel_vpnrtr1-vpnrtr2
        ISAKMP Action  =ike-1
Is this correct? [Yes]:   Y
```

Esta política evaluará todos los paquetes que entren en el direccionador y reenviará aquellos paquetes que coincidan con el perfil a IPSec para cifrarlos. Si no se crean políticas adicionales, todos los paquetes que no coincidan con el perfil se direccionarán en texto claro a la interfaz apropiada.

Sin embargo, para este escenario, sólo debe cruzar la VPN el tráfico entre las dos subredes. Para que esto se lleve a cabo, se tendrá que crear una política para eliminar todo el tráfico que no venga de una de las dos subredes especificadas.

Crear una política en VPNRTR1 para eliminar tráfico público

Éstos son los pasos para crear la política para eliminar el tráfico público que no procede de una de las subredes especificadas en la política de túnel IPSec. Los pasos para configurar esta política son similares a los de la política de túnel excepto en que hay menos pasos:

1. Añadir la política
2. Añadir el perfil

3. Especificar las interfaces
4. Añadir el periodo de validez
5. Añadir la acción de seguridad IP
6. Confirmar la política

Añadir la política

Tabla 94. Añadir política para eliminar tráfico público

```
VPNRTR1 Config>FEATURE Policy
IP Network Policy configuration
VPNRTR1 Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? dropAllPublicTraffic
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?          1
```

1. En la política anterior, se ha asignado una prioridad de 15. La próxima vez, se asignará una prioridad de 5. Por consiguiente, los paquetes de entrada se evaluarán primero con el perfil de la política de túnel. Si no coinciden con ese perfil, se evaluarán con este perfil. Entonces el resultado será que todos los paquetes que no cumplan con el perfil de túnel coincidirán con este perfil y, por consiguiente, se eliminarán.

Añadir el perfil

Este perfil está diseñado para que coincida con todo el tráfico.

Tabla 95. Añadir política para que coincida con todo el tráfico

```
List of Profiles:
        0: New Profile
        1: 32->106

Enter number of the profile for this policy [1]? 0
Enter a Name (1-29 characters) for this Profile []? allPublicTraffic
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]?
Enter IPV4 Source Mask [0.0.0.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [0.0.0.0]?
Enter IPV4 Destination Mask [0.0.0.0]?

Protocol IDs:
     1)  TCP
     2)  UDP
     3)  All Protocols
     4)  Specify Range

Select the protocol to filter on (1-4) [3]?
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]:
```

Especificar las parejas de interfaces

Puesto que no se han definido direcciones IP de origen y destino, se deberá especificar a qué interfaces se aplica la política.

Tabla 96. Definir interfaces para bloquear el tráfico público

```
The Source and/or Destination Address information you specified
includes all addresses.  You must specify an Interface Pair
with this profile to further qualify what traffic you wish to filter
to this policy.
Limit this profile to specific interface(s)? [No]: yes
Interface Pair Groups:
        0: New Ifc Pair
Number of Ifc Pair Group [1]? 0
Enter a Group Name (1-29 characters) for this Interface Pair []? inOutPublic
Ingress Interface IP Address (255.255.255.255 = any ingress)
 [255.255.255.255]?
Egress Interface IP Address (255.255.255.255 = any egress)
 [255.255.255.255]? 192.168.141.18
Interface Pair Groups:
        0: New Ifc Pair
        1) Group Name: inOutPublic
                  In:Out=255.255.255.255 : 192.168.141.18
```

Tabla 97. Verificar interfaces especificadas

```
Number of Ifc Pair Group [1]? 0
Enter a Group Name (1-29 characters)for this Interface Pair []?inOutPublic
Ingress Interface IP Address (255.255.255.255 = any ingress)
 [255.255.255.255]? 192.168.141.18
Egress Interface IP Address (255.255.255.255 = any egress)
 [255.255.255.255]?
Interface Pair Groups:
        0: New Ifc Pair
        1) Group Name: inOutPublic
                  In:Out=255.255.255.255 : 192.168.141.18
                  In:Out= 192.168.141.18 : 255.255.255.255

Number of Ifc Pair Group [1]? 1


Here is the Profile you specified...


Profile Name    = allPublicTraffic
        sAddr:Mask=        0.0.0.0 : 0.0.0.0   sPort=    0 : 65535        1
        dAddr:Mask=        0.0.0.0 : 0.0.0.0   dPort=    0 : 65535        2
        proto     =              0 : 255
        TOS       =            x00 : x00              3
        Remote Grp=All Users
        1.  In:Out=255.255.255.255 : 192.168.141.18
        2.  In:Out= 192.168.141.18 : 255.255.255.255
Is this correct? [Yes]:
```

1. Todo ceros indica que el tráfico procedente de cualquier origen coincide con el perfil.
2. Todo ceros indica que el tráfico con cualquier destino coincide con el perfil.
3. Si se deja el TOS por omisión en x00 indica que el tráfico a cualquier nivel de prioridad coincidirá con el perfil.

Añadir el periodo de validez

Una vez que se han especificado las interfaces, se deberá seleccionar el perfil y el periodo de validez. No es necesario crear un periodo de validez nuevo puesto que se puede utilizar la descripción **always** anterior configurada.

Tabla 98. Volver a usar el periodo de validez ALWAYS

```
List of Profiles:
        0: New Profile
        1: 32->106
        2: allPublicTraffic

Enter number of the profile for this policy [1]? 2
List of Validity Periods:
        0: New Validity Period
        1: always

Enter number of the validity period for this policy [1]? 1
```

Añadir la acción IPSec

Describa una acción de seguridad para eliminar todo el tráfico que coincide con el perfil **allPublicTraffic**. El hecho de que esta política se establezca en una prioridad más baja que la política de túnel hará que entre el tráfico correcto en el túnel y que se elimine todo el resto de tráfico. En otras palabras, se comprueba cada paquete de entrada, primero con el perfil de túnel y, por último, con el perfil público.

Tabla 99. Añadir la acción IPSec para eliminar el tráfico público

```
Should this policy enforce an IPSEC action? [No]: yes
IPSEC Actions:
        0: New IPSEC Action
        1: tun-32->106

Enter the Number of the IPSEC Action [1]? 0
Enter a Name (1-29 characters) for this IPsec Action []? dropTraffic
List of IPsec Security Action types:
     1)  Block (block connection)
     2)  Permit

Select the Security Action type (1-2) [2]? 1


Here is the IPSec Action you specified...


IPSECAction Name = dropTraffic
        Action   = Drop
Is this correct? [Yes]: yes
IPSEC Actions:
        0: New IPSEC Action
        1: tun-32->106
        2: dropTraffic

Enter the Number of the IPSEC Action [1]? 2
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]? 1
```

Confirmar que la política es correcta

Confirme la política entrando **Yes**.

Tabla 100. Confirmar la política para eliminar tráfico

```
Here is the Policy you specified...


Policy Name     = dropAllPublicTraffic
        State:Priority =Enabled    : 1
        Profile        =allPublicTraffic
        Valid Period   =always
        IPSEC Action   =dropTraffic
Is this correct? [Yes]:   Y
```

Esto completa la configuración en VPNRTR1. Asegúrese de hacer una copia de la configuración en IBD, el programa de configuración o de enviarla a un servidor TFTP.

Crear una política para el túnel IPSec para VPNRTR2

Consulte la Figura 65 en la página 294 para ver el diagrama de red y las direcciones IP para este ejemplo. Éstos son los pasos para configurar el direccionador:

1. Habilitar la seguridad IP
2. Crear la clave precompartida
3. Añadir una política
4. Añadir un perfil
5. Añadir un periodo de validez
6. Añadir una acción IPSec
7. Añadir una propuesta IPSec
8. Añadir una transformación ESP

Los pasos para crear la política VPNRTR2 son los mismos que los utilizados para VPNRTR1 con las diferencias siguientes:

- El perfil para la política de túnel VPNRTR2 invierte la sAddr:Mask y la dAddr:Mask utilizadas con VPNRTR1.
- El perfil para la política de eliminación VPNRTR2 invierte las interfaces especificadas.
- La acción IPSec para VPNRTR2 invierte los puntos Tunnel Start:End.
- El usuario definido para VPNRTR2 es el punto final de túnel de VPNRTR1.

Nota: Asegúrese de que la clave precompartida sea idéntica en ambos direccionadores. Un modo fácil de comprobarlo consiste en cortar y pegar las claves. Asimismo, tenga en cuenta que si la clave entrada tiene una longitud mayor que la anchura de caracteres de la pantalla de sesión Telnet, puede que no vea la clave entera cuando se presenta la pantalla de confirmación.

La Tabla 101 en la página 312 muestra la salida del mandato **list all** de Talk 6 después de completar la configuración de VPNRTR2. Los valores que son diferentes de los de la política VPNRTR1 se anotan debajo de cada figura.

Tabla 101. Listar todos los objetos de la base de datos de políticas para VPNRTR2

```
VPNRTR2 Policy config>LIST ALL

Configured Policies....

Policy Name     = ike-pre-106->32              1
        State:Priority =Enabled    : 15
        Profile        =106->32                2
        Valid Period   =always
        IPSEC Action   =ike-1
        ISAKMP Action  =ike-1

Policy Name     = dropAllPublicTraffic
        State:Priority =Enabled    : 5
        Profile        =allPublicTraffic
        Valid Period   =always
        IPSEC Action   =dropTraffic

Configured Profiles....

Profile Name    = 106->32      3
        sAddr:Mask=     9.24.106.0 : 255.255.255.0   sPort=     0 : 65535
        dAddr:Mask= 192.168.141.32 : 255.255.255.240 dPort=    0 : 65535
        proto     =              0 : 255
        TOS       =            x00 : x00
```

1. El nombre de la política sólo es para tener una referencia. Utilice un nombre significativo.
2. Utilice un nombre significativo para el perfil.
3. Las direcciones de perfil son las contrarias del direccionador del punto final opuesto del túnel.

Tabla 102. Listar objetos de la base de datos de políticas para VPNRTR2 (Pantalla 1 de 4)

```
Remote Grp=All Users

Profile Name    = allPublicTraffic
        sAddr:Mask=        0.0.0.0 : 0.0.0.0         sPort=    0 : 65535
        dAddr:Mask=        0.0.0.0 : 0.0.0.0         dPort=    0 : 65535
        proto     =              0 : 255
        TOS       =            x00 : x00
        Remote Grp=All Users
        1.  In:Out=255.255.255.255 : 192.168.141.17       1
        2.  In:Out= 192.168.141.17 : 255.255.255.255

Configured Validity Periods

Validity Name   = always
        Duration  = Forever
        Months    = ALL
        Days      = ALL
        Hours     = All Day

Configured DiffServ Actions....
No DiffServ Actions configured
```

1. La dirección del puerto WAN.

Tabla 103. Listar objetos de la base de datos de políticas para VPNRTR2 (Pantalla 2 de 4)

```
Configured IPSEC Actions....

IPSECAction Name = ike-1
        Tunnel Start:End         = 192.168.141.17 : 192.168.141.18          1
        Tunnel In Tunnel         =              No
        Min Percent of SA Life   =              75
        Refresh Threshold        =              85 %
        Autostart                =              No
        DF Bit                   =            COPY
        Replay Prevention        =        Disabled
        IPSEC Proposals:
                esp-prop1

IPSECAction Name = dropTraffic
        Action   = Drop

Configured IPSEC Proposals....

Name  = esp-prop1
        Pfs   = N
        ESP Transforms:
                esp-trans1
```

1. Recuerde, para la acción IPSec de este direccionador, los puntos inicial y final de túnel deben ser exactamente los contrarios de los del direccionador del punto final opuesto.

Tabla 104. Listar objetos de la base de datos de políticas para VPNRTR2 (Pantalla 3 de 4)

```
Configured IPSEC Transforms....

Transform Name  = esp-trans1
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =DES

Configured ISAKMP Actions....

ISAKMP Name     = ike-1
        Mode                     =            Main
        Min Percent of SA Life   =              75
        Conn LifeSize:LifeTime   =            5000 : 30000
        Autostart                =             Yes
        ISAKMP Proposals:
                ike-prop1
```

Tabla 105. Listar objetos de la base de datos de políticas para VPNRTR2 (Pantalla 4 de 4)

```
Configured ISAKMP Proposals....
Name = ike-prop1
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = MD5
        Encr Algo  = DES CBC

Configured Policy Users....
Name      = 192.168.141.18         1
Type      = IPV4 Addr
        Group     =
        Auth Mode =Pre-Shared Key
        Key(Ascii)=key
Configured Manual IPSEC Tunnels....

                            IPv4 Tunnels
-------------------------------------------------------------------------------

   ID         Name        Local IPv4 Addr  Rem IPv4 Addr    Mode    State
 ------  --------------  --------------  --------------  -----  --------
VPNRTR2 Policy config>
```

1. El usuario de política configurado para VPNRTR2 será la dirección IP de VPNRTR1.

Crear una política en VPNRTR2 para eliminar tráfico público

Éstos son los pasos para crear la política para eliminar el tráfico público que no procede de una de las subredes especificadas en la política de túnel IPSec.

Nota: Para obtener instrucciones exactas paso a paso, consulte el apartado “Crear una política en VPNRTR1 para eliminar tráfico público” en la página 307. La única diferencia está en el paso **Especificar las interfaces** donde la dirección de interfaz será la dirección IP del puerto WAN para VPNRTR2.

1. Añadir la política
2. Añadir el perfil
3. Especificar las interfaces
4. Añadir el periodo de validez
5. Añadir la acción de seguridad IP
6. Confirmar la política

Supervisión y resolución de problemas de las políticas

La base de datos de políticas toma la política y genera las reglas que son necesarias para IPSec. La política ha definido que sea necesario que el tráfico que va de x.x.x.x a x.x.x.x esté protegido utilizando el túnel *nombretúnel*. En el pasado, también era necesario que los filtros de paquetes estuvieran configurados para confirmar que el tráfico de x.x.x.x a x.x.x.x se había protegido mediante el túnel *nombretúnel*. La característica de política crea este filtro. Si desea conocer qué políticas se han generado, vaya a la característica de política desde talk 5 y entre **list policy generated**. El direccionador listará todas las políticas que ha definido. Seleccione el número apropiado y el direccionador le indicará qué reglas se han generado para dicha política.

Tabla 106. Listar la política generada

```
VPNRTR2 *TALK 6
VPNRTR2 Config>FEATURE Policy
IP Network Policy configuration
VPNRTR2 Policy console>LIST POLICY GENERATED
1: (Enabled,Valid)      dropAllPublicTraffic
2: (Enabled,Valid)      ike-pki-106-32
Number of Policy to display [0]? 2
Rules generated for policy ike-pki-106-32:
Rule 1.  ike-pki-106-32.p1in
Rule 2.  ike-pki-106-32.p1out
Rule 3.  ike-pki-106-32.p2in
Rule 4.  ike-pki-106-32.traffic
Rule 5.  ike-pki-106-32.inBoundTunnel
```

Si desea saber cuáles son estas reglas, existen dos mandatos: uno le proporciona un resumen y otro le proporciona los detalles. **List rule basic** le proporciona la información básica acerca de una regla — la prioridad, cómo se ha generado y cómo se ha utilizado.

Tabla 107. Listar regla básica (List Rule Basic)

```
VPNRTR2 Policy console>LIST RULE BASIC
1: (Enabled,Valid)      ike-pki-106-32.p2in
2: (Enabled,Valid)      ike-pki-106-32.p1out
3: (Enabled,Valid)      ike-pki-106-32.p1in
4: (Enabled,Valid)      ike-pki-106-32.traffic
5: (Enabled,Valid)      ike-pki-106-32.inBoundTunnel
11: (Enabled,Valid)     dropAllPublicTraffic
Number of Rule to display (0 for All) [0]? 1
Policy Name: ike-pki-106-32.p2in
Loaded from: Local
State:       Enabled and Valid
Priority:    94
Hits:        0
Profile:     106->32.p2in
Validity:    always
IPSEC:       ike-1
```

List rule complete le muestra los detalles de la regla. Esta regla se utiliza para confirmar que el tráfico de 192.168.141.18 a 192.168.141.17 se ha protegido utilizando la definición de túnel correcta.

Tabla 108. Listar regla completa (List Rule Complete)

```
VPNRTR2 Policy console>LIST RULE COMPLETE
1: (Enabled,Valid)      ike-pki-106-32.p2in
2: (Enabled,Valid)      ike-pki-106-32.p1out
3: (Enabled,Valid)      ike-pki-106-32.p1in
4: (Enabled,Valid)      ike-pki-106-32.traffic
5: (Enabled,Valid)      ike-pki-106-32.inBoundTunnel
11: (Enabled,Valid)     dropAllPublicTraffic
Number of Rule to display (0 for All) [0]? 1
Policy name:                            ike-pki-106-32.p2in
Policy Loaded from:                     Local Configuration
Policy state:                           Enabled and Valid
Policy Priority:                        94

Profile Name    = 106->32.p2in
        sAddr:End = 192.168.141.18 : 192.168.141.18  sPort=  500 : 500
        dAddr:End = 192.168.141.17 : 192.168.141.17  dPort=  500 : 500
        proto     =             17 : 17
        TOS       =            x00 : x00
        Remote Grp=All Users

Validity Name   = always
        Duration  = Forever
        Months    = ALL
        Days      = ALL
        Hours     = All Day

IPSECAction Name = ike-1
        Tunnel Start:End         = 192.168.141.17 : 192.168.141.18
        Tunnel In Tunnel         =              No
        Min Percent of SA Life   =              75
        Refresh Threshold        =              85 %
        Autostart                =              No
        DF Bit                   =            COPY
        Replay Prevention        =        Disabled
        IPSEC Proposals:
        ----------------
        1:Name = esp-prop1
                Pfs  = N
                ESP Transforms:
                --------------
                1:Name = esp-trans1
                        Mode     = Tunnel
                        LifeSize = 50000
                        LifeTime = 3600
                        Authent  = SHA          Encr =DES
VPNRTR2 Policy console>
```

Otros mandatos útiles:

- >TALK 5
- >+FEATURE IPSec
- IPSec>IKE
- VPNRTR2 IKE>LIST TUNNEL
- VPNRTR2 IKE>LIST ALL
- VPNRTR2 IKE>STATS

VPN de direccionador a direccionador utilizando certificados digitales

Si va a realizar la autentificación utilizando certificados digitales necesitará tener una autoridad de certificación (CA). Esto es normalmente un paquete de software que se ejecuta en un PC o una plataforma UNIX. Tenga en cuenta que en este release sólo se soporta una CA, de modo que todos los certificados para la red entera tiene que emitirlos la misma instancia del paquete de software. Muchas compañías venden software CA — por ejemplo, Entrust Technologies, Inc. y VeriSign.

Para obtener un certificado, el direccionador debe tener una clave privada y una pública. Éstas se generan cuando se emite la petición de certificado desde talk 5. Una vez generadas las claves, el direccionador forma un paquete de petición de certificado. Éste contiene la clave pública del direccionador y un identificador. Entonces se envía la petición a un servidor TFTP que se ejecuta en algún lugar de la red. A continuación se debe pasar la petición de certificado a la CA y ésta debe leerla y procesarla. La CA emitirá el certificado. El certificado contiene la clave pública del direccionador, el identificador enviado por el direccionador y un periodo de validez. El certificado está firmado con la clave privada de la CA.

El direccionador debe entonces recuperar este certificado, a través de TFTP o LDAP. Cuando el direccionador baje el certificado, la clave privada que es el asociado de la clave pública del certificado debe estar aún en la memoria en ejecución del direccionador. El certificado de bajada es inútil si el direccionador ha perdido la clave privada coincidente. Esto significa que desde el momento en que emite la petición de certificado hasta el momento en que se baja el certificado, no deberá reiniciar ni volver a cargar el direccionador, borrar la antememoria o emitir una nueva petición de certificado. Cualquiera de estas operaciones destruirá la clave privada. Las claves y el certificado deben guardarse tan pronto como se ha recuperado el certificado.

El direccionador también necesita tener una copia del certificado de la CA. Cuando el direccionador verifica el certificado de un igual, debe confirmar que el certificado del igual ha sido firmado con la clave privada de la CA. Para poder realizar dicha acción, debe tener el certificado de la CA que contiene la clave pública de la CA. Cada direccionador que realice IKE debe bajar el certificado de la CA utilizando TFTP o LDAP. Este certificado también debe guardarse.

Este ejemplo explica cómo configurar direccionadores de IBM para seguridad IP con negociaciones de clave automáticas utilizando signaturas digitales para proporcionar autentificación. El túnel va de direccionador a direccionador. Este túnel autentificará y cifrará el tráfico de sistemas principales específicos y excluirá todo el tráfico restante. El ***perfil*** describe exactamente a qué sistemas principales en cada extremo del túnel se les permite pasar datos a través del túnel. La ***política*** puede permitir a un solo sistema principal en cada extremo, a una o varias subredes de cada extremo o cualquier combinación de las dos opciones. La limitación del túnel de direccionador a direccionador es que no se produce ninguna autentificación o ningún cifrado en la LAN. Esta solución no proporciona seguridad en la LAN.

Consulte la Figura 64 en la página 293 para ver la conectividad de red física. Consulte la Figura 65 en la página 294 para ver el diagrama de red lógica y el direccionamiento IP. Se proporcionarán documentación y capturas de pantalla sólo para los parámetros que son diferentes de los del ejemplo del apartado “VPN IPSec de direccionador a direccionador utilizando claves precompartidas” en la página 293.

Nota: En este caso no es necesario definir un usuario. El certificado digital proporcionará la autentificación.

Crear una política para el túnel IPSec para VPNRTR1

Los pasos para este ejemplo serán muy similares a los descritos en el apartado “Crear una política para el túnel IPSec para VPNRTR1” en la página 294. Para crear esta configuración, empiece con el paso titulado **Enable IPSecurity** (Habilitar seguridad IP) y continúe exactamente con los pasos hasta el final del paso titulado **Add ISAKMP Action** (Añadir acción ISAKMP). El paso siguiente, **Add ISAKMP Proposal** (Añadir propuesta ISAKMP), será diferente.

Los pasos siguientes son iguales que los del ejemplo de claves precompartidas proporcionado en el apartado “Crear una política para el túnel IPSec para VPNRTR1” en la página 294, excepto cuando se indique en los mismos. Cuando utilice este método, no utilice el mandato **Add User** para crear un usuario y las claves. Al crear el perfil, puede configurarlo igual que en el ejemplo anterior, pero asegúrese de tener en cuenta la nota.

1. Habilitar la seguridad IP
2. Añadir una política
3. Añadir un perfil

   Nota: Al añadir el perfil, se le solicita que configure los ID para ISAKMP. Deberá realizar esta acción para que el otro igual pueda identificarle. El método elegido aquí debe coincidir con el tipo **subject-alt-name** y la información entrada en el mandato **CERT-REQ** mostrado en la Tabla 111 en la página 320. La información también debe coincidir con la que se envía a la Autoridad de certificación que se muestra en la Figura 70 en la página 322.
4. Añadir un periodo de validez
5. Añadir una acción IPSec
6. Añadir una propuesta IPSec
7. Añadir una transformación ESP
8. Añadir una acción ISAKMP

Los pasos siguientes serán diferentes de los del ejemplo de claves precompartidas. Empezará por añadir una nueva propuesta ISAKMP para especificar el método de autentificación RSA SIG. RSA SIG es un término para los certificados digitales. A continuación, solicitará y cargará un certificado de direccionador y un certificado de CA.

1. Añadir una propuesta ISAKMP
2. Configurar el servidor TFTP para cargar certificados
3. Solicitar un certificado de direccionador
4. Cargar el certificado de direccionador
5. Guardar el certificado de direccionador
6. Obtener un certificado CA
7. Cargar el certificado CA
8. Guardar el certificado CA

Añadir una propuesta ISAKMP

La propuesta ISAKMP especifica los atributos de cifrado y autentificación de la SA de la fase I. También especifica qué grupo Diffie-Hellman se debe utilizar para generar las claves y la vida de la seguridad de la fase I.

Tabla 109. Añadir la propuesta ISAKMP para certificados digitales

```
VPNRTR1 Policy config>ADD ISAKMP-PROPOSAL
Enter a Name (1-29 characters) for this ISAKMP Proposal []? cert1      1

List of Authentication Methods:         2
     1)  Pre-Shared Key
     2)  RSA SIG

Select the authentication method (1-2) [1]? 2

List of Hashing Algorithms:
     1)  MD5
     2)  SHA

Select the hashing algorithm(1-2) [1]?

List of Cipher Algorithms:
     1)  DES
     2)  3DES

Select the Cipher Algorithm (1-2) [1]?
Security Association Lifesize, in kilobytes (100-65535) [1000]?
Security Association Lifetime, in seconds (120-65535) [15000]?

List of Diffie Hellman Groups:
     1)  Diffie Hellman Group 1
     2)  Diffie Hellman Group 2

Select the Diffie Hellman Group ID from this proposal (1-2) [1]?


Here is the ISAKMP Proposal you specified...

Name = cert1
        AuthMethod = RSA SIG
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = MD5
        Encr Algo  = DES CBC
Is this correct? [Yes]:
```

1. Se dará un nombre a la propuesta ISAKMP.
2. Especifíquelo para utilizar certificados digitales.

Configurar el servidor TFTP para cargar certificados

El mandato **Load Certificate** necesita que se haya definido anteriormente un servidor TFTP. Utilice el mandato **Add Server** para asignar un nombre y una dirección IP. Es una buena idea comprobar la conectividad entre el direccionador y el servidor TFTP antes de intentar la operación de carga del certificado.

Tabla 110. Añadir la descripción de servidor TFTP para cargar certificados

```
VPNRTR1 Config>FEATURE IPSec
IP Security feature user configuration
VPNRTR1 IPsec config>PKI
VPNRTR1 PKI config>ADD SERVER
Name ? (max 65 chars) []? TFTPServer
Enter server IP Address []? 9.24.106.146
Transport type (Choices: TFTP/LDAP)  [TFTP]?
VPNRTR1 PKI config>EXIT
```

Solicitar un certificado de direccionador

Antes de solicitar un certificado, es importante asegurarse de que el reloj del direccionador en el que se cargará el certificado indica una hora próxima pero no

posterior a la del reloj del sistema CA. Consulte el “Capítulo 19. Redes privadas virtuales” en la página 275 para obtener una explicación de las Autoridades de certificación. Cuando una CA emite un certificado, en éste se realizará una indicación de la hora con un periodo válido expresado como hora y fecha de inicio y de finalización. La hora del direccionador debe ser posterior a la hora de inicio del certificado y anterior a la hora de finalización. Si el certificado lo está emitiendo un sistema principal que no está bajo su control, el único modo de poder saber la indicación de la hora del certificado consiste en solicitarla e intentar cargarla en el direccionador. Si la hora para el direccionador está fuera del periodo de validez, se visualizará el mensaje siguiente en la anotación cronológica ELS.

```
PKI.009 Validity check: failed Current date 1999/3/5, Time 9:38.21.
Cert valid date: 1999/3/5 10:14:38 -- 1999/6/5 10:14:38
```

Este mensaje le informa de que la hora del direccionador es anterior a la hora válida del certificado. Si ocurre esto, compruebe la hora del direccionador utilizando el mandato de T 6 **time list** para visualizar la hora y el mandato **time set** para ajustar la hora.

El mandato **CERT-REQ** se utiliza para crear una petición de certificado que se enviará a la CA.

Tabla 111. Solicitar el certificado

```
VPNRTR1  *TALK 5
VPNRTR1 +FEATURE IPSec
VPNRTR1 IPSP>PKI
VPNRTR1 PKI Console>CERT-REQ
Enter the following part for the subject name
   Country Name(Max 16 characters) []? us
   Organization Name(Max 32 characters) []? cert
   Organization Unit Name(Max 32 characters) []?
   Common Name(Max 32 characters) []? VPNRTR1        1
Key modulus size (512|768|1024)
 [512]?
Certificate subject-alt-name type:     2
   1--IPv4 Address
   2--User FQDN
   3--FQDN
Select choice [1]?
Enter an IPv4 addr) []? 192.168.141.18       3
Generating a key pair. This may take some time. Please wait ...
Cert Request format: 1--DER;2--PEM      4
 [1]? 2
PKCS10 message successfully generated
Enter tftp server IP Address []? 9.24.106.146
Remote file name (max 63 chars) [/tmp/tftp_pkcs10_file]? test.req
Memory transfer starting.
.Memory transfer completed - successfully.
Certificate request TFTP to remote host sucessfully.     5
Generated private key stored into cache
Please download router certificate and save
both router certificate and its private key ASAP.
VPNRTR1 PKI Console>
```

1. Este nombre debe coincidir con el nombre real de sistema de direccionador configurado.
2. El tipo debe coincidir con el tipo de ID especificado en el perfil.
3. Ésta debe ser la dirección de punto final de túnel local. La dirección IP de la interfaz serie está directamente en Internet.
4. El formato de la petición de certificado debe coincidir con el formato que utiliza la CA para crear el certificado. DER es formato digital y PEM es formato ASCII.

5. Ahora la petición de certificado está en el servidor TFTP como test.req.

Obtención de los certificados de la CA

La petición de certificado debe enviarse al servidor CA que verificará la petición y emitirá un certificado. El certificado contiene la clave pública del direccionador y la información entrada. La CA firma el certificado con una clave privada y éste se convierte en información digital fiable.

Abra el documento *test.req* en Word Pad como se muestra en la Figura 69.

Figura 69. Petición de certificado creada por el direccionador

Para este ejemplo, se ha utilizado Entrust Technologies aunque puede utilizar cualquier Autoridad de certificación. Los pasos para obtener el certificado pueden ser diferentes de los pasos listados aquí.

Recuerde que cuando efectúe una operación de cortar y pegar, sólo deberá cortar y pegar la cabecera, el pie y los caracteres del medio. La cabecera debe empezar por guiones y el pie debe finalizar con guiones.

En la ubicación Web de la compañía, seleccione **Request a VPN Certificate**. Rellene el formulario de declaración de limitación de responsabilidad y pulse en **PROCEED**. En el formulario siguiente, desplácese hacia abajo hasta el área de entrada como se muestra en la Tabla 111 en la página 320, y rellene el nombre común (que, en este ejemplo, es VPNRTR1). Deseleccione el recuadro etiquetado **Encode certificate in PKCS7 certificates only message**. Entre el nombre alternativo que debe coincidir con la referencia 2 de la Tabla 111 en la página 320 para la que hemos entrado 192.168.141.18. Suprima el texto entrado previamente en el área de cortar y pegar. Utilizando Word Pad, abra el archivo *test.req* y corte y pegue la petición de certificado en la ventana proporcionada en la página Web. El certificado se pega sin retornos de carro.

Figura 70. Rellenar el formulario de petición de certificado

Un certificado se devolverá en el navegador Web como se muestra en la Figura 71.

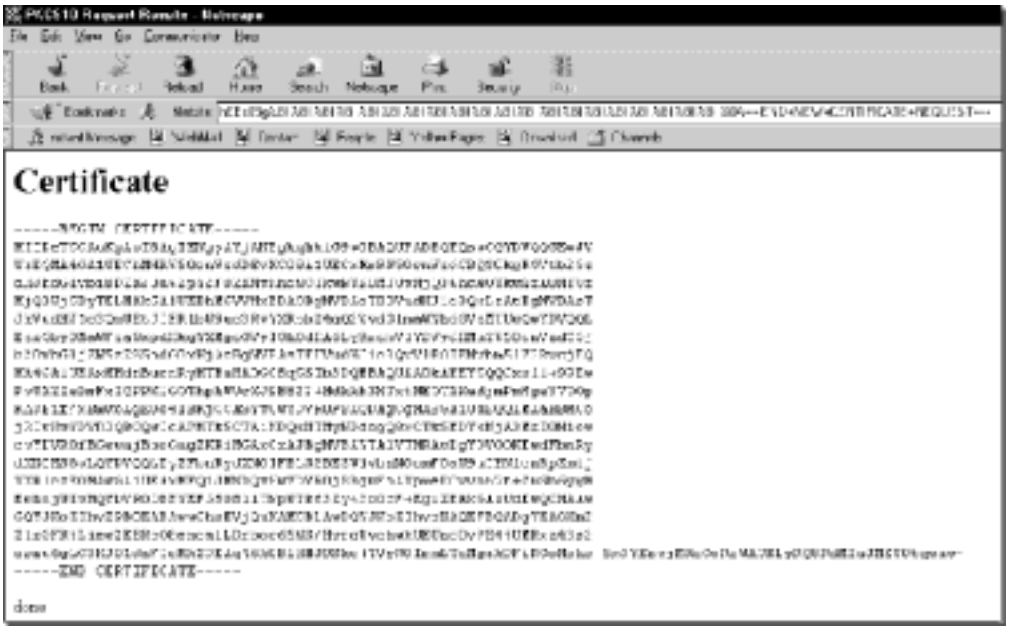


Figura 71. El certificado de direccionador se devuelve al navegador

Corte y pegue el certificado en un nuevo documento de texto en Word Pad. Suprima los espacios al final de la primera, penúltima y última línea. Guarde el certificado en el Directorio de subida de servidor TFTP. Para este ejemplo, el archivo de certificado se ha denominado *cert.txt*.

Cargar certificado de direccionador

Ahora el certificado debe recuperarse a través de LDAP o TFTP. El escenario siguiente utiliza TFTP para recuperar el certificado. Tal como se muestra en la Tabla 112, utilice el mandato **Load Certificate** para recuperar el certificado del direccionador. Tome la opción por omisión para el tipo de certificado dado que está recuperando el certificado del direccionador. Entonces se le preguntará si el certificado está en formato digital (opción 1) o en formato ASCII (opción 2). Seleccione la opción 2. A continuación se le solicitará el nombre de servidor. Éste es el nombre del servidor TFTP que ha añadido desde talk 6. Finalmente, se le solicitará el nombre del archivo en el servidor. Entonces el direccionador recuperará el certificado y lo almacenará en la memoria de ejecución.

Tabla 112. Cargar el certificado de direccionador

```
VPNRTR1 PKI Console>LOAD CERTIFICATE
Enter the type of the certificate:
Choices:  1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]?
Encoding format:
Choices: 1-DER 2-PEM
Enter (1-2): [1]? 2
Server info name []? TFTPServer
Remote file name on tftp server (max 63 chars) [/tmp/default_file]? cert.txt

Attempting to load certificate file. Please wait ...
Memory transfer starting.
.Memory transfer completed - succesfully.
Router Certificate  loaded into run-time cache
VPNRTR1 PKI Console>
```

Guardar el certificado de direccionador

Guarde inmediatamente el certificado y las claves asociadas. Tendrá que repetir el proceso de certificado si no guarda el certificado y se reinicia el direccionador. Se le solicitará que indique qué certificado está guardando, qué nombre desea ponerle y si desea que este certificado se cargue en la memoria del direccionador cuando éste se inicie.

Tabla 113. Guardar el certificado de direccionador

```
VPNRTR1 PKI Console>CERT-SAVE
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]?
SRAM Name for certificate and private key []? r1cert.txt
Load as default router certificate at initialization? [No]: y
Both Router Certificate and private key saved into SRAM successfully
VPNRTR1 PKI Console>
```

Obtener un certificado CA

El direccionador tiene ahora sus claves privada y pública, que se han generado justo antes de que se emitiera la petición de certificado. Acaba de recuperar el certificado del direccionador. Ahora necesita el certificado de la CA para poder verificar la validez de un certificado del igual IKE. Una parte de la confirmación de la validez consiste en comprobar que la CA ha firmado el certificado del igual, por consiguiente se necesita el certificado de la CA. El certificado del igual debe estar firmado por la misma CA porque no existe ningún mecanismo que pueda utilizarse para comprobar un certificado emitido por otra CA.

A continuación, se ha seleccionado **Retrieve PEM Encoded Certificate** en la ubicación Web Entrust. Como se muestra en la Figura 72 en la página 324, se ha

devuelto un certificado CA al navegador. Para esta prueba en concreto, no se ha enviado ninguna cabecera o ningún pie de página con el certificado CA.

Figura 72. El certificado CA se devuelve al navegador Web

Para este ejemplo, se ha pegado el texto que hay a continuación de ″CA Certificate″ en un nuevo documento de texto de Word Pad. No se ha enviado ninguna cabecera o ningún pie de página con el certificado CA. (Esto puede variar en función de cómo se obtenga el certificado CA). Para que el direccionador de este ejemplo acepte el certificado, se han tenido que pegar en el documento la cabecera y el pie de página del certificado de direccionador que ya se había recibido y se ha pegado el texto de certificado CA entre el texto de cabecera y el de pie de página como se muestra en la Figura 73 en la página 325.

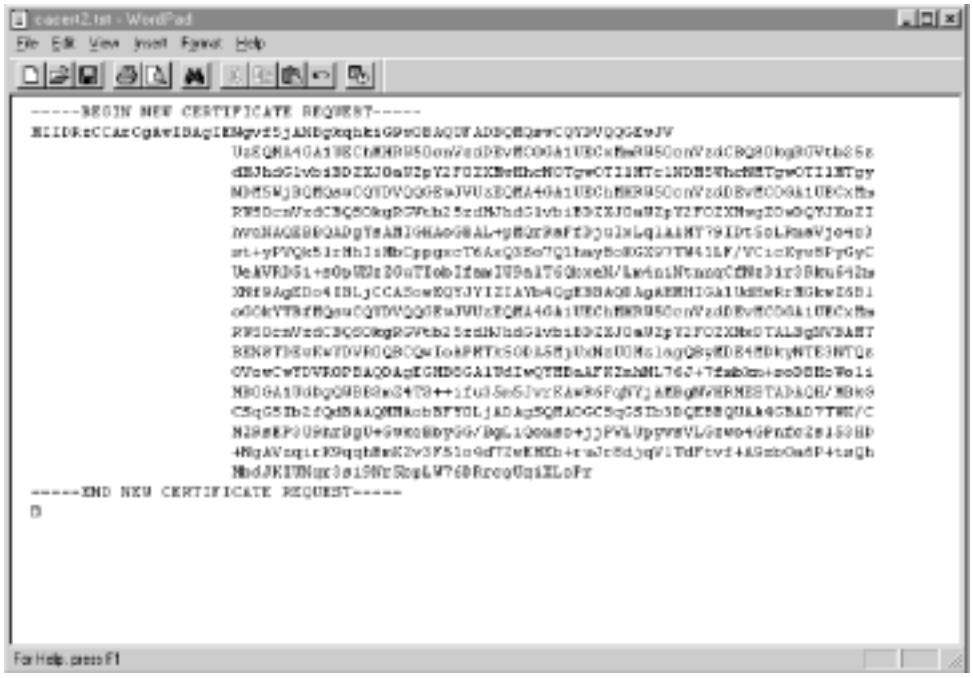


Figura 73. Añadir la cabecera y el pie de página en el certificado CA

Guarde el certificado como un documento en el directorio de subida de servidor TFTP. Para este ejemplo, el archivo se ha denominado *cert.txt*.

Cargar el certificado CA

El certificado de la CA también se puede cargar a través TFTP utilizando el mandato **Load Certificate** y seleccionando la opción 1 como tipo de certificado.

Tabla 114. Cargar el certificado raíz en antememoria

```
VPNRTR1 PKI Console>LOAD CERTIFICATE
Enter the type of the certificate:
Choices:  1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]? 1
Encoding format:
Choices: 1-DER 2-PEM
Enter (1-2): [1]? 2
Server info name []? TFTPServer
Remote file name on tftp server (max 63 chars) [/tmp/default_file]? cacert.txt

Attempting to load certificate file. Please wait ...
Memory transfer starting.
.Memory transfer completed - successfully.
Root CA Certificate  loaded into run-time cache
VPNRTR1 PKI Console>
```

Guardar el certificado CA

Tabla 115. Guardar el certificado raíz en la configuración del direccionador

```
VPNRTR1 PKI Console>CERT-SAVE
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]? 1
SRAM Name to store Root Certificate? []? cacert
Load as default root certificate at initialization? [No]: y
Root Certificate saved into SRAM successfully.
VPNRTR1 PKI Console>
```

Una vez que haya guardado el certificado CA, habrá completado la configuración de la política de túnel VPNRTR1.

Crear una política en VPNRTR1 para eliminar tráfico público

Los pasos para configurar esta política son exactamente los mismos que los del ejemplo mostrado en el apartado “Crear una política en VPNRTR1 para eliminar tráfico público” en la página 307:

1. Añadir la política
2. Añadir el perfil
3. Especificar las interfaces
4. Añadir el periodo de validez
5. Añadir la acción de seguridad IP
6. Confirmar la política

Esto completa la configuración de VPNRTR1. Guarde copias de la configuración para no tener que volver a repetirla.

Crear una política para el túnel IPSec para VPNRTR2

Para crear el túnel de Seguridad IP, siga estos pasos:

1. Habilitar la seguridad IP
2. Añadir una política
3. Añadir un perfil
4. Añadir un periodo de validez
5. Añadir una acción IPSec
6. Añadir una propuesta IPSec
7. Añadir una transformación ESP
8. Añadir una acción ISAKMP
9. Añadir una propuesta ISAKMP
10. Configurar el servidor TFTP para cargar certificados
11. Solicitar un certificado de direccionador
12. Cargar el certificado de direccionador
13. Guardar el certificado de direccionador
14. Obtener un certificado CA
15. Cargar el certificado CA
16. Guardar el certificado CA

Los pasos anteriores son los mismos que los mostrados en el apartado “Crear una política para el túnel IPSec para VPNRTR1” en la página 318 con las diferencias siguientes:

- El perfil para la política de túnel VPNRTR2 invierte la sAddr:Mask y la dAddr:Mask utilizadas con VPNRTR1.
- La acción IPSec para VPNRTR2 invierte los puntos Tunnel Start:End.

Crear una política en VPNRTR2 para eliminar tráfico público

Los pasos para crear esta política son los mismos que los del apartado “Crear una política en VPNRTR2 para eliminar tráfico público” en la página 314.

Supervisión/Resolución de problemas desde talk 5

Las operaciones de supervisión y las estadísticas para este ejemplo son iguales que para el ejemplo de claves precompartidas. Consulte el apartado “Supervisión y resolución de problemas de las políticas” en la página 314.

Túnel PPTP voluntario con terminación de direccionador de IBM

Consulte el apartado “Point-to-Point Tunneling Protocol” en la página 290 para obtener información adicional acerca de PPTP.

Los direccionadores de IBM soportan PPTP a fin de proporcionar interoperabilidad con dispositivos Microsoft Windows que sólo soportan PPTP. Microsoft ha anunciado su intención de implementar L2TP en NT 5.0.

La Figura 74 en la página 328 es un ejemplo de una VPN de acceso remoto utilizando el túnel voluntario PPTP. El direccionador de IBM se configurará como el punto final de un túnel PPTP. El cliente, un cliente DUN (Dial-Up Networking) de Windows/98, Windows/95 o Windows NT llamará en el direccionador ISP. El cliente establecerá una conexión PPP y se le proporcionará una dirección IP en la subred 9.24.104.0. Llegado este momento, el cliente tiene conectividad IP a cualquier parte de la nube IP de Internet incluyendo la interfaz WAN del direccionador corporativo de Internet. El cliente establecerá entonces un túnel en 192.168.141.18, que es la dirección IP del direccionador corporativo de Internet. El ID de usuario y la contraseña para el túnel PPTP es *sg245281* y la dirección IP es 192.168.141.38. Éstos los asigna el direccionador corporativo. Una vez establecido el túnel, la conectividad es la misma que tendría si hubiera llamado directamente en un Servidor de acceso remoto de la LAN corporativa.

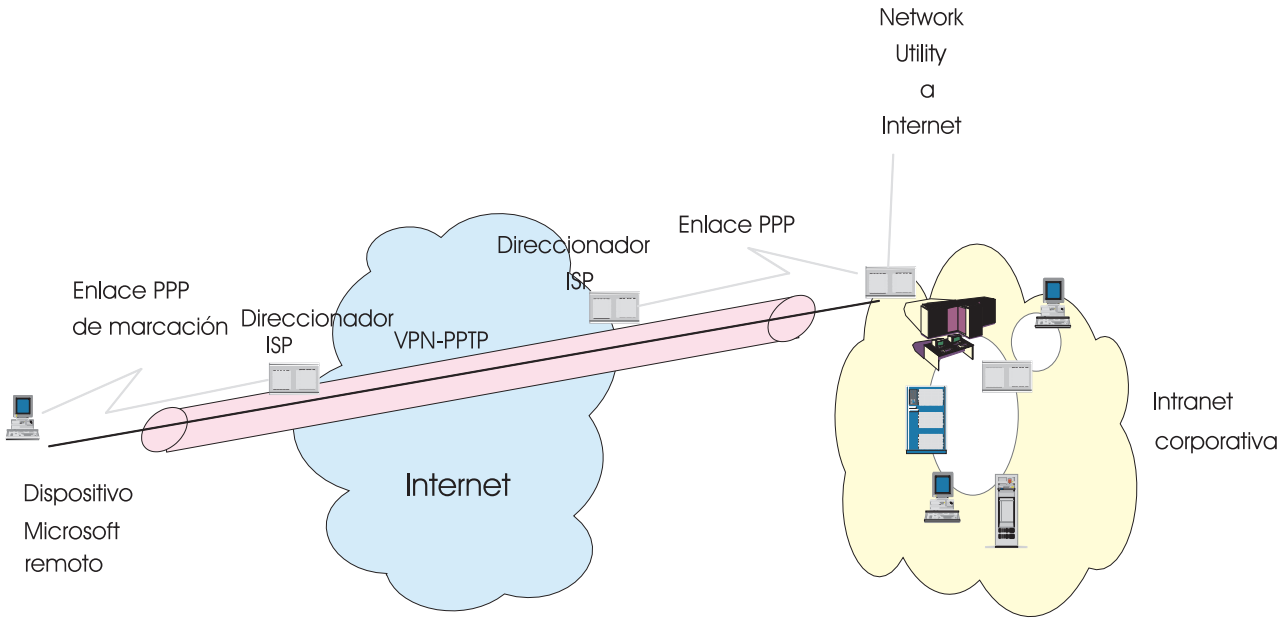


Figura 74. Túnel PPTP de estación de trabajo a pasarela

Configuración del Network Utility

Antes de realizar los pasos siguientes, asegúrese de que el Network Utility tiene configuradas las interfaces adecuadas. Configure también IP para que la interfaz PPP tenga una ruta estática o dinámica a Internet. La interfaz de Intranet no deberá anunciarse en Internet. Consulte la Figura 75 en la página 329 para conocer el direccionamiento IP de la red que se ha utilizado para este ejemplo.

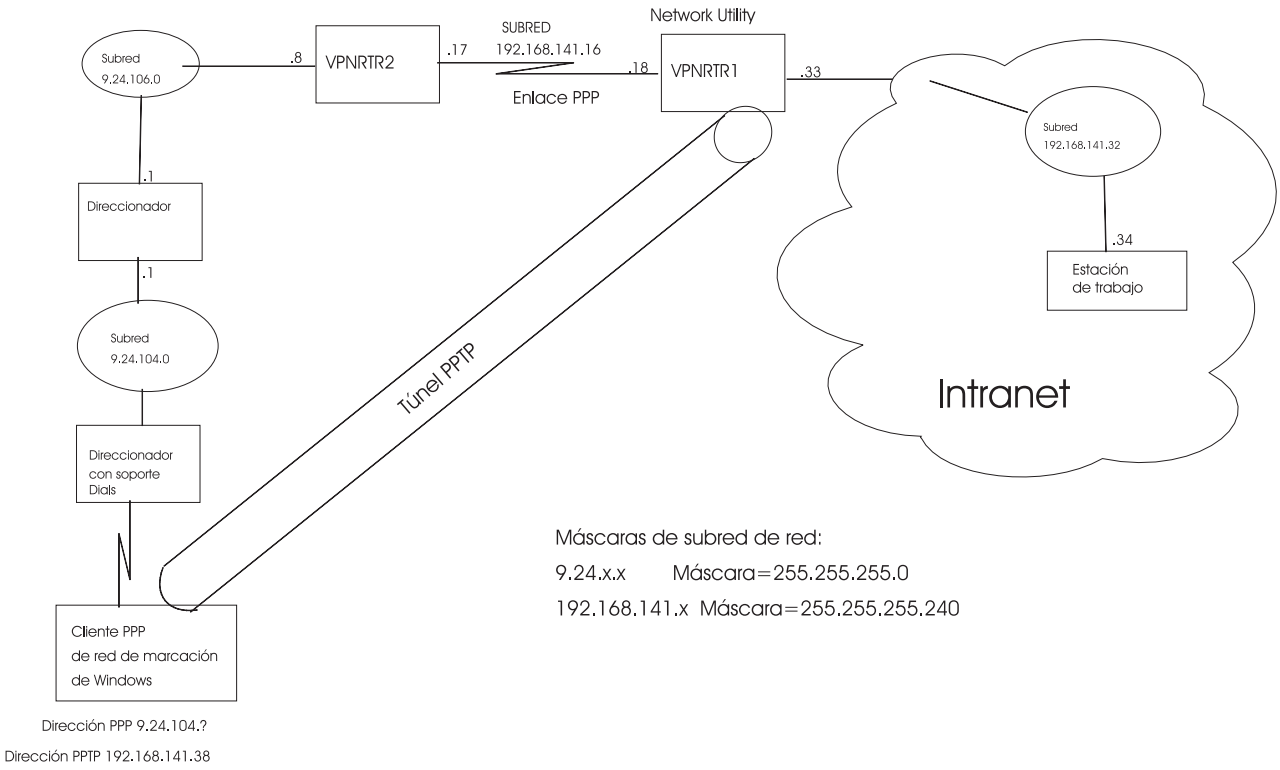


Figura 75. Esquema de direccionamiento IP

Para configurar el direccionador corporativo de Internet como se ilustra en la Figura 74 en la página 328, siga estos pasos:

- Habilitar PPTP
- Añadir redes L2
- Habilitar mschap y mppe
- Añadir USUARIO PPP
- Habilitar el direccionamiento de subred arp
- Configurar el cliente DUN (Dial-UP Networking)

Habilitar PPTP

Tabla 116. Habilitar PPTP

```
VPNRTR1  *TALK 6
VPNRTR2 Config>FEATURE Layer-2-Tunneling
VPNRTR2 Layer-2-Tunneling Config>ENABLE PPTP

 Restart system for changes to take effect.
```

Añadir redes de capa 2

Añada el número de Redes de capa 2 necesario para soportar el número máximo de conexiones simultáneas. En este ejemplo, se añaden 3 redes. No necesita habilitar IPX o puentes transparentes.

Tabla 117. Añadir una red de capa 2

```
VPNRTR1 *TALK 6
VPNRTR2 Config>FEATURE Layer-2-Tunneling
VPNRTR2 Layer-2-Tunneling Config>ADD L2-NETS
Additional L2 nets:  [0]? 3       1
Add unnumbered IP addresses for each L2 net? [Yes]:
Adding device as interface 6
Defaulting Data-link protocol to PPP
Adding device as interface 7
Defaulting Data-link protocol to PPP
Adding device as interface 8
Defaulting Data-link protocol to PPP
Enable IPX on L2T interfaces?(Yes or [No]):
Enable transparent bridging on L2T interfaces?(Yes or [No]):
Bridge configuration was not changed.

Restart router for changes to take affect.
VPNRTR2 Layer-2-Tunneling Config>
```

1. Añada el número de redes para igualar el número máximo planificado de clientes PPTP conectados simultáneamente.

Habilitar mschap y mppe

Los clientes PPTP DUN (Dial-UP Networking) Windows de Microsoft utilizan MPPE para efectuar el cifrado. Este protocolo necesita estar habilitado en la L2Net (Red de capa 2). Las L2Net configuradas como de entrada desde cualquiera (el valor por omisión) toman sus valores por omisión PPP de una plantilla de la característica de capa. El mandato **encapsulator** le lleva a un indicador desde donde se pueden ajustar todos los valores por omisión PPP.

Para utilizar MPPE, deberá habilitar MS-CHAP. Al habilitar MPPE, se le preguntará si MPPE está operando en modalidad obligatoria u opcional. Si está operando en modalidad obligatoria, deberá negociar MPPE. La modalidad obligatoria fuerza al direccionador a volver a negociar MPPE cada vez que se solicita una conexión nueva, incluso cuando el remitente ha establecido anteriormente MPPE entre él y el direccionador. Si MPPE está operando en modalidad opcional, no está obligado a negociar MPPE. La modalidad opcional hace que el direccionador mantenga MPPE entre él mismo y el remitente después de la negociación inicial y no vuelve a negociar MPPE para cada nueva conexión. A continuación se le preguntará si las claves tienen estado o no tienen estado. Si las claves no tienen estado, la clave cambiará cada vez que se envíe un paquete, mientras que si tiene estado la clave sólo se generará cuando se hayan enviado 255 paquetes. Las claves sin estado se recomiendan para redes disipativas y se deberán utilizar para las conexiones PPTP. El direccionador sabrá si el cliente está utilizando la modalidad sin estado o con estado dado que parte de la cabecera MPPE indica si se han renovado las claves.

Microsoft también tiene su propio algoritmo de compresión, MPPC. MPPE se negocia como una opción MPPC. Si desea efectuar compresión y está utilizando MPPE, deberá utilizar MPPC. En este caso, no puede utilizar el algoritmo Stac-LZS que normalmente está disponible para enlaces PPP. Si elige no utilizar MPPC, el código de direccionador habilita parcialmente la función para permitir negociar MPPE. Si elige utilizar MPPE y MPPC, éstos se descodifican de un solo paso dado que estos protocolos comparten la misma cabecera PPP.

Tabla 118. Habilitar MSCHAP y MPPE

```
VPNRTR1 Layer-2-Tunneling Config>ENCAPSULATOR
Point-to-Point user configuration
VPNRTR1 PPP-L2T Config>ENABLE MSCHAP
Rechallenge Interval in seconds (0=NONE)  [0]?
Enabling MSCHAP
VPNRTR1 PPP-L2T Config>ENABLE MPPE
mandatory or optional [optional]?
stateful or stateless [stateful]? stateless      1
Enabling encryption

** Note ** : To view the MPPE configuration, please enter a 'list ccp'
             command since MPPE is negotiated within the CCP protocol.
VPNRTR1 PPP-L2T Config>
```

1. Si las claves no tienen estado, la clave cambiará cada vez que se envíe un paquete, mientras que si tienen estado la clave sólo se generará cuando se hayan enviado 255 paquetes. Las claves sin estado se recomiendan para redes disipativas y se deberán utilizar para las conexiones PPTP.

Añadir usuario PPP

Para este ejemplo, se configuran dos usuarios para que se prueben al menos dos conexiones simultáneas. Se le ha asignado a cada usuario una dirección IP estática. Éste es el modo más simple pero también el menos flexible y menos escalable de asignar direcciones IP a clientes PPP. Existen otros métodos de asignación de direcciones IP que consisten en utilizar una agrupación de direcciones IP o en utilizar servicios DHCP.

Primero se añade el usuario llamado *sg245281*. La entrada de contraseña no aparecerá en la pantalla.

Tabla 119. Añadir el usuario PPP

```
VPNRTR2 Config>ADD PPP-USER
Enter name:  []? sg245281
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
Number of days before account expires [0-1000] [0]?
Number of grace logins allowed after an expiration [0-100] [0]?
IP address: [0.0.0.0]? 192.168.141.38       1
Enter hostname: []?
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Will user be able to dial-out ? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No]
Disable user ? (Yes, No): [No]

     PPP user name: sg245281
   User IP address: 192.168.141.38
     Netroute Mask: 255.255.255.255
          Hostname:       Virtual Conn: disabled
      Time alotted: Box Default
     Callback type: disabled
          Dial-out: disabled
        Encryption: disabled
            Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
    Account Expiry:    Password Expiry:
Is information correct? (Yes, No, Quit): [Yes]

User 'sg245281' has been added
VPNRTR2 Config>
```

1. Dirección IP asignada manualmente al cliente PPTP

Añada otro usuario ppp llamado *vendedor* utilizando los mismos parámetros y luego liste todos los usuarios ppp.

Tabla 120. Listar usuarios PPP

```
VPNRTR2 Config>LIST PPP-USERS addr
List  (Name, Verb, User, Addr, VCon, Call, Time, Dial, Encr): [User] addr

PPP user name      User IP address     Netroute Mask       Hostname
-----------------  ------------------  ------------------  ---------------
vendedor           192.168.141.39      255.255.255.255     <no definido>
sg245281           192.168.141.38      255.255.255.255           <no definido>
2 PPP records displayed.
```

Habilitar direccionamiento de subred arp

El direccionamiento de subred arp se denomina también proxy arp. Si un sistema principal de la red corporativa transmite un datagrama a un sistema principal PPTP que tiene una dirección IP en la misma subred, el remitente no enviará el datagrama a la ruta por omisión, sino que esperará ver una entrada en su propia antememoria ARP. Si no existe ninguna entrada en la antememoria ARP, el remitente enviará difusiones ARP directamente al IP de destino. Dado que la dirección IP de destino (el cliente PPTP remoto) no está en la red física, no responderá nunca. El direccionamiento de subred arp permite al direccionador local

responder a la difusión ARP en nombre del cliente remoto. Entonces el direccionador copia el datagrama y éste se reenvía a través de Internet.

Tabla 121. Habilitar direccionamiento de subred arp

```
VPNRTR2 Config>PROTOCOL
Protocol name or number [IP]?
Internet protocol user configuration
VPNRTR1 IP config>ENABLE ARP-SUBNET-ROUTING
VPNRTR1 IP config>
```

Configurar el cliente DUN

Para establecer una conexión PPTP utilizando una plataforma Microsoft, necesita dos sesiones DUN — una en Internet — el direccionador de ISP — y otra en el Network Utility. Primero arrancará la conexión de llamada PPP que establece la conexión Internet y luego arrancará la conexión PPTP para crear el túnel al Network Utility. La interfaz PPP del IBM Network Utility debe ser accesible en Internet.

Nota: Deberá tener instalado DUN 1.2 o posterior. Para ver si tiene la Versión 1.2 o posterior, abra una ventana **Make a New Connection** en la carpeta DUN. Compruebe si el Adaptador Microsoft VPN está en la ventana desplegable **Select a Device**.

Para configurar el cliente Microsoft PPTP, siga estos pasos:

- Añada un cliente DUN. Configúrelo para utilizar su módem para llamar en el direccionador ISP.
- Añada un segundo cliente DUN. Configúrelo para utilizar el adaptador VPN para conectar con la dirección IP de la interfaz WAN del direccionador corporativo. Al pulsar en **Make a New Connection**, se le solicitarán detalles acerca del adaptador. Deberá utilizar el adaptador Microsoft VPN. La pantalla siguiente le solicitará el nombre de sistema principal o la dirección IP. En este recuadro, entre la dirección IP del direccionador de IBM que se puede alcanzar a través de la nube IP. Al arrancar dicha conexión DUN, ésta le solicitará un id de usuario y una contraseña que deben coincidir con los detalles configurados con el mandato **add ppp-user** en la configuración de direccionador que se muestra en el apartado “Configuración del Network Utility” en la página 328.

Al utilizar el usuario ppp definido manualmente, deberá tener una dirección IP estática para cada usuario configurado manualmente.

Puede definir un usuario ppp/una dirección ip para cada usuario y especificar en DUN que se utilice la dirección IP asignada por el servidor. De lo contrario, puede tener un usuario ppp y especificar en DUN que se utilice la dirección IP estática asignada localmente.

En el cliente DUN bajo los valores **Properties/Server Type/TCP/IP**, puede especificar si se debe utilizar o no la ruta por omisión en la red remota. Lo que especifique aquí dependerá de si el cliente PPTP está accediendo sólo a recursos de la subred remota o de si necesita tener también conectividad a otras redes.

Supervisión

Para verificar que la configuración es correcta, puede efectuar las pruebas ping siguientes. En primer lugar, inicie el enlace PPP en el cliente DUN y haga ping en la interfaz de Internet del Network Utility. La operación ping debe ser satisfactoria. A continuación, intente hacer ping en la interfaz de Intranet. La operación ping debe

fallar. Ahora inicie el túnel PPTP arrancando la definición DUN de PPTP. Ahora deberá poder hacer ping en todos los sistemas principales de la Intranet.

Desde el indicador de Talk 5, emita el mandato **NETWORK 6** y, a continuación, el mandato **LIST ALL** para ver información exhaustiva acerca de la conexión PPP. Lo más útil para la resolución de problemas son las estadísticas, el id de usuario y la dirección IP de la conexión.

Utilice el mandato **CALL STATE** como se muestra en la Tabla 122. Antes de que emitiéramos el mandato **CALL STATE**, hemos establecido sesiones con nuestros dos usuarios ppp.

Tabla 122. Visualizar sesiones de la capa 2

```
VPNRTR1 Layer-2-Tunneling Console> CALL STATE
CallID │ Serial # │ Net #  │    State    │ Time Since Chg │ PeerID │ TunnelID
 55285 │        0 │      8 │ Established │     0:37:10    │      0 │     6084
 38142 │        0 │      7 │ Established │     0: 4:35    │      0 │    24721
VPNRTR1 Layer-2-Tunneling Console>
```

Para supervisar y solucionar problemas, utilice los mandatos siguientes:

- Consola de túnel de la capa 2 VPNRTR1> **TUNNEL TRANSPORT**
- Emita el mandato **TALK 2** después de configurar ELS con **DISPLAY SUBSYSTEM L2 ALL ALL**

En la Tabla 123, la salida del mandato **TALK 2** muestra las dos redes PPP con el id de llamada (CallID) que coincide con la información.

Tabla 123. Salida de Talk 2 con suceso establecido para visualizar subsistema L2

```
00:41:55   L2.024: PPTP PAYLOAD SEND 38 bytes, net=7, callid=38142
00:41:55   L2.041: SND PPTP:F=3081,L=54,Tid=0,Cid=0,NS=115,NR=117,O=0
00:41:55   L2.040: RCV PPTP:F=3081,L=38,Tid=24721,Cid=38142,NS=118,NR=115,O=0
00:41:55   L2.022: PPTP PAYLOAD RCVD 38 bytes, net 7, callid=38142
00:42:00   L2.024: PPTP PAYLOAD SEND 38 bytes, net=8, callid=55285
00:42:00   L2.041: SND PPTP:F=3081,L=54,Tid=0,Cid=0,NS=264,NR=274,O=0
00:42:00   L2.040: RCV PPTP:F=3081,L=38,Tid=6084,Cid=55285,NS=275,NR=264,O=0
00:42:00   L2.022: PPTP PAYLOAD RCVD 38 bytes, net 8, callid=55285
00:42:03   L2.084: PPTP Tunnel 6084/0 EVENT Rcv-ECHO,state=Established
```

Consulte la Tabla 124 para ver un listado parcial del mandato **LIST ALL**.

Tabla 124. Salida parcial del mandato List All

```
VPNRTR1 +NETWORK 8
Point-to-Point Console
       VPNRTR1 PPP 8>LIST ALL

Interface Statistic        In                      Out
-------------------        --                      ---
Packets:                   81                      70
Octets:                    3316                    2581
..
.Remote Username:           sg245281
.
..IPCP Option                Local                   Remote
-----------                -----                   ------
IP Address                 0.0.0.0                 192.168.141.38
Compression Slots          None                    None
```

Túnel PPTP voluntario iniciado por Network Utility de IBM

Este ejemplo, que se ilustra en la Figura 76, es un escenario PPTP donde el direccionador de IBM inicia un túnel PPTP con un RAS (Remote Access Server) (Servidor de acceso remoto) que funciona bajo NT de Microsoft y que es su igual PPTP. El servidor NT tiene dos adaptadores — uno con una dirección IP a la que puede conectarse a través de la nube IP y otro en la red privada. El sistema principal NT no tiene configurado ningún protocolo de direccionamiento dinámico, pero tiene posibilidad de reenvío IP.

El escenario proporcionará conectividad para los sistemas principales IP en la bifurcación a los sistemas principales en una sola subred dentro de la red corporativa. El RAS NT está ubicado en lo que a veces se denomina DMZ. Es accesible desde Internet y no está protegido por el cortafuegos corporativo. El propio RAS se convierte en cortafuegos para la subred corporativa a la que se accederá a través de Internet.

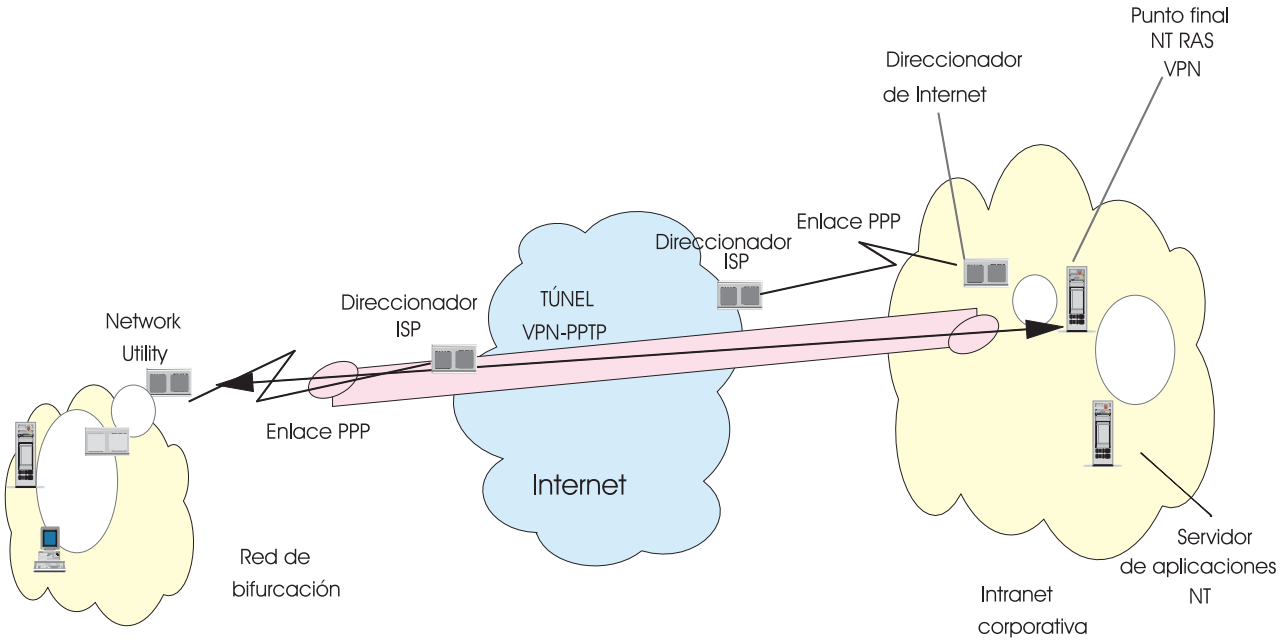


Figura 76. Túnel PPTP iniciado por direccionador de IBM

La red de laboratorio utilizada para este ejemplo consta de un enlace PPP y tres segmentos de Red en Anillo conectados por dos direccionadores IBM 2210 y una Estación de trabajo NT. Hemos denominado a los direccionadores VPNRTR1 y VPNRTR2. Los direccionadores del laboratorio están conectados con un enlace PPP a 56 Kbps. En un escenario real, el enlace entre los direccionadores puede ser cualquier WAN privada o pública.

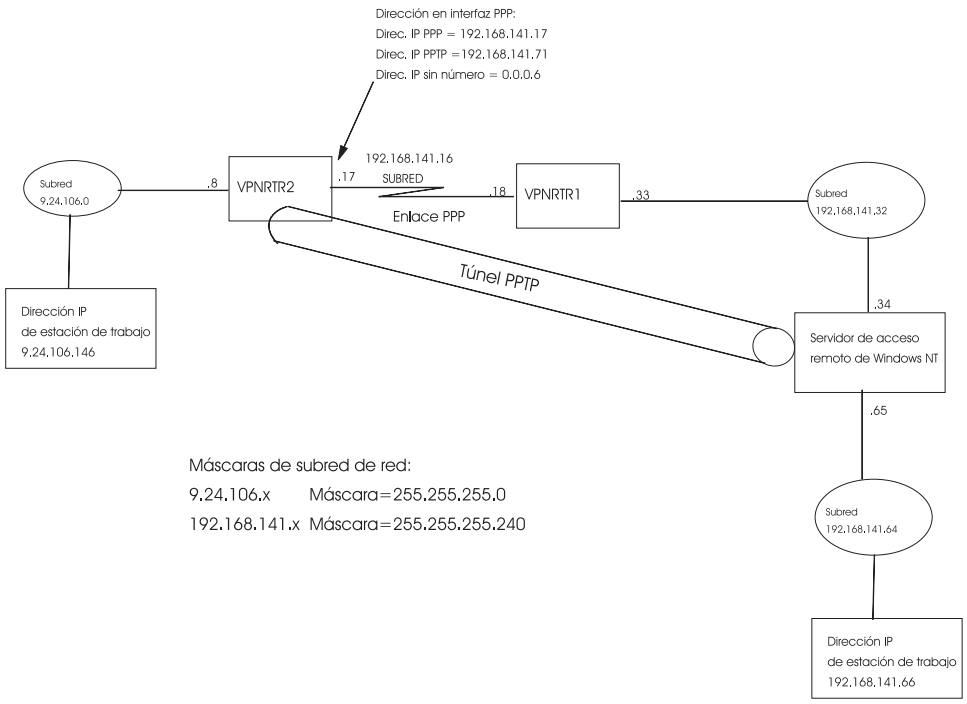


Figura 77. Direccionamiento IP de red de laboratorio

Se establece un túnel PPTP cuando un dispositivo de la red de bifurcación 9.24.106.0 tiene datos para enviar a la red IP LAN corporativa 192.168.141.64. La red 192.168.141.64 no está anunciada en la nube IP. Los sistemas principales de la red corporativa son direcciones privadas y la nube IP es una red de ISP.

VPNRTR2, que representa el Direccionador Internet de bifurcación como se muestra en la Figura 76 en la página 335, se configurará con una ruta estática que especifica el tráfico destinado a la red 192.168.141.64 y deberá direccionarse a través de la interfaz virtual. Cuando se reciban datos en la interfaz, el direccionador establecerá un túnel PPTP. El direccionador examinará la L2Net y la definición de túnel para localizar la dirección IP del igual PPTP, 192.168.141.34, que se ilustra como el RAS (Servidor de acceso remoto) NT y el Punto final de VPN. El direccionador establecerá una conexión TCP con esta dirección a través de Internet. Después de que NT haya aceptado la conexión PPTP, el direccionador de bifurcación negociará los parámetros PPP para su L2Net. El servidor NT devolverá una dirección IP de una agrupación de direcciones configuradas para dicha interfaz PPTP. La dirección IP tiene que estar en la misma subred que la interfaz LAN corporativa. L2Net debe configurarse para recibir su dirección IP a través de IPCP.

Configurar el direccionador de bifurcación

A continuación se indican los pasos básicos para configurar el direccionador de bifurcación:

- Habilitar PPTP
- Añadir el perfil de túnel
- Configurar las definiciones para el direccionamiento IP y la autentificación
- Configurar la Conversión de dirección de red
- Crear filtros de paquetes

Habilite PPTP en el direccionador y añada la interfaz virtual. Cuando se reciba tráfico en esta interfaz, el direccionador iniciará el túnel PPTP.

Tabla 125. Añadir las redes de la capa 2

```
VPNRTR2 *TALK 6

VPNRTR2 Config>FEATURE Layer-2-Tunneling
VPNRTR2 Layer-2-Tunneling Config>ENABLE PPTP

 Restart system for changes to take effect.
VPNRTR2 Layer-2-Tunneling Config>
Layer-2-Tunneling Config>add l2-nets
Additional L2 nets: [0]? 1
Add unnumbered IP addresses for each L2 net? [Yes]:
Adding device as interface 6         1
Defaulting data-link protocol to PPP
Enable IPX on L2T interfaces?(Yes or [No]):
Enable transparent bridging on L2T interfaces?(Yes or
[No]):
Bridge configuration was not changed.
Restart router for changes to take affect.
Layer-2-Tunneling Config>exit
VPNRTR2 Config>
```

1. Dado que hemos especificado que se añadiera la dirección IP sin número, se asigna 0.0.0.6 porque L2Net es la interfaz 6. Como se muestra en la Tabla 126, puede utilizar el mandato **list addr** en el indicador de mandatos IP Config> para verificar la dirección. Esta dirección se utilizará como parámetro para el mandato **enable dynamic** como se muestra en la Tabla 130 en la página 339.

Tabla 126. Listar direcciones para verificar la dirección IP de la interfaz PPTP

```
VPNRTR2 Config>PROTOCOL IP
VPNRTR2 IP config>LIST ADDRESSES
IP addresses for each interface:
   intf     0                                    IP disabled on this interface
   intf     1  192.168.141.17   255.255.255.240  Local wire broadcast, fill 1
   intf     2                                    IP disabled on this interface
   intf     3                                    IP disabled on this interface
   intf     4                                    IP disabled on this interface
   intf     5  9.24.106.8       255.255.255.0    Local wire broadcast, fill 1
   intf     6  0.0.0.6          0.0.0.0          Local wire broadcast, fill 1
                                                 DYNAMIC-ADDRESS Enabled
VPNRTR2 Config>EXIT
```

El paso siguiente es definir el punto final del túnel PPTP. Se utiliza el mandato **add tunnel-profile** para definir el túnel. El nombre que se le solicita es el nombre del PPTP remoto. Esto es sólo para realizar la identificación local. No se envía durante los intercambios PPTP. Se le solicita la dirección de punto final de servidor de túnel — la cual está en la dirección del servidor NT con el que puede comunicarse a través de la nube IP.

Tabla 127. Añadir el túnel

```
VPNRTR2 Config>ADD TUNNEL-PROFILE
Enter name:  []? NT
Tunneling Protocol?  (PPTP, L2F, L2TP): [L2TP] PPTP
Tunnel-Server endpoint address: [0.0.0.0]? 192.168.141.34

       Tunnel name: NT
          TunnType: PPTP
          Endpoint: 192.168.141.34

Tunnel 'NT' has been added
```

El siguiente paso es unir nuestra interfaz virtual con el igual llamado NT. Por omisión, todas las redes de la capa 2 (L2Net) son de entrada desde cualquier dispositivo. Esto debe cambiarse para que sean de salida. Entonces se le solicitará el nombre del dispositivo remoto. Esto significa que cuando se direccione tráfico a nuestra interfaz virtual, la interfaz 6, el direccionador establecerá un túnel hacia un igual llamado ″NT″. Examinará la definición de túnel ″NT″ y descubrirá que se trata de un túnel PPTP en 192.168.141.34.

El direccionador consultará la tabla de direccionamiento para determinar cómo llegar a dicha dirección, lo cual en este ejemplo será a través de 192.168.141.17. Es necesario que el direccionador se configure a través de un protocolo de direccionamiento estático o de direccionamiento dinámico para saber cómo se accede a 192.168.141.34.

Tabla 128. Configurar la interfaz virtual

```
VPNRTR2 Config>NETWORK 6
Session configuration
VPNRTR2 L2T config:   6>SET CONNECTION-DIRECTION OUTBOUND     1
Enter remote tunnel hostname:  []? NT
VPNRTR2 L2T config:   6>
```

Cuando una L2Net pasa a ser de salida en lugar de ser de entrada, se pueden configurar los valores por omisión PPP en dicha L2Net. Puede acceder al indicador de configuración PPP utilizando el mandato **encapsulator**. En este ejemplo, el direccionador está configurado para enviar el nombre rtr-1 cuando se le solicite. Esta L2Net está destinada a recibir su dirección IP del sistema NT. Ésta se enviará durante las negociaciones IPCP y será necesario configurar el direccionador para solicitar al sistema NT la dirección IP. Esta acción puede realizarse utilizando el mandato **set ipcp** y respondiendo sí (yes) a la pregunta ″Request an IP address″ (solicitar una dirección IP).

Tabla 129. Configurar L2net para enviar nombre y habilitar interfaz para recibir dirección IP a través de IPCP

```
VPNRTR2 Config>NETWORK 6
Session configuration
VPNRTR2 L2T config:   6>ENCAPSULATOR
Point-to-Point user configuration
VPNRTR2 PPP 6 Config>SET NAME
Enter Local Name:  []? rtr-1
Password:rtr-1            1
Enter password again:rtr-1
PPP Local Name = rtr-1


VPNRTR2 PPP 6 Config>
VPNRTR2 PPP 6 Config>SET IPCP
IP COMPRESSION [no]:
Request an IP address [no]: yes      2
Interface remote IP address to offer if requested (0.0.0.0 for none) [0.0.0.0]?

VPNRTR2 PPP 6 Config>EXIT
VPNRTR2 L2T config:   6>EXIT
VPNRTR2 Config>
```

1. La contraseña no aparecerá en la pantalla. Aquí se muestra sólo a modo ilustrativo. Este nombre y esta contraseña deben coincidir con el Usuario y la Contraseña definidos en el Servidor de acceso remoto NT bajo la función de gestión de usuarios (User Manager).
2. Responda sí (yes) para que NT envíe una dirección IP para L2Net.

Para que la L2net de direccionador reciba una dirección IP del punto final de túnel NT, debemos habilitar la dirección IP para IP dinámico. Esto permitirá a NT enviar una dirección de una agrupación de direcciones preconfiguradas a través de IPCP.

Tabla 130. Configurar IP en la L2Net

```
VPNRTR2 Config>PROTOCOL IP
Internet protocol user configuration
VPNRTR2 IP config>ENABLE DYNAMIC-ADDRESS
Interface address []? 0.0.0.6   1
VPNRTR2 IP config>
```

1. Entre la dirección IP asignada por el mandato **add l2-nets** como se muestra en la Tabla 125 en la página 337.

Se deberá añadir una ruta estática a la subred corporativa puesto que no se utilizan protocolos de direccionamiento dinámico en el sistema principal RAS NT.

Tabla 131. Añadir una ruta estática a la red privada

```
VPNRTR2 IP config>ADD ROUTE
IP destination []? 192.168.141.64       1
Address mask [255.255.255.0]? 255.255.255.240
Via gateway 1 at []? 0.0.0.6
Cost [1]?
Via gateway 2 at []?
VPNRTR2 IP config>EXIT
VPNRTR2 Config>
```

1. Ésta es la máscara de dirección y de subred de la red donde está ubicado el RAS NT.

Dado que el direccionador va a aparecer como un solo usuario en la red corporativa y la red corporativa no tiene conocimiento de la red de bifurcación, necesitamos utilizar la NAPT (Network Address and Port Translation) (Conversión de puerto y dirección de red). La NAPT es una mejora de la NAT, que se enviaba originalmente en los direccionadores de IBM de la V3.1. Se habilita y configura desde la característica NAT.

Tabla 132. Configurar NAT

```
VPNRTR2 Config>FEATURE NAT
Network Address Translation (NAT) user configuration
VPNRTR2 NAT config>ENABLE NAT

Complete! NAT set to ENABLED.
VPNRTR2 NAT config>
```

El paso siguiente es definir en qué dirección queremos los paquetes convertidos. Esto se realiza utilizando el mandato **reserve**. Cuando se le solicite si la dirección se obtendrá a través de IPCP, la respuesta debe ser sí (yes). La interfaz es 6, la L2Net. Entonces el direccionador solicita un nombre de agrupación. Éste se utiliza como referencia cuando definimos las direcciones que deben convertirse. El direccionador también le indica que necesita configurar filtros de paquetes IP para pasar los paquetes a la característica NAT para convertirlos. Ésta es la primera vez que el direccionador le recuerda que debe configurar filtros de paquetes IP.

Tabla 133. Definir cómo deben convertirse las direcciones de LAN

```
VPNRTR2 NAT config>RESERVE
Dynamically allocate address via IPCP? [No]: yes
Network number to get dynamic address. [0]? 6
Reserve Pool name..................... []? dyn-nat

Complete! NAT Reserve Pool defined.

NOTE: The associated TRANSLATE RANGE for this RESERVE POOL
      must still be configured.
      It must have a pool name of: dyn-nat

NOTE: You must have a corresponding INBOUND IP Access Control rule
      applied to your designated NAT interface.
      The rule should include the following information:
          Type=IN (include + NAT)
          DESTINATION_Addr=0.0.0.0
          DESTINATION_Mask=0.0.0.0

VPNRTR2 NAT config>
```

El paso siguiente es definir qué direcciones deben convertirse. El mandato indica, ″Convertir todos los paquetes con una dirección de origen en la red 9.24.106.0 para que tengan una dirección en la agrupación dyn-nat″. En el paso anterior, hemos definido que la agrupación dyn-nat es la dirección recibida por IPCP en la interfaz 6. El direccionador le recuerda que necesita configurar filtros para que los paquetes pasen a NAT/NAPT para su conversión.

Tabla 134. Definir qué direcciones de LAN deben convertirse

```
VPNRTR2 NAT config>TRANSLATE
Base (private) IP address to translate [0.0.0.0]? 9.24.106.0
Translate Range mask.................. [255.255.255.0]?
Associated Reserve Pool name.......... [dyn-nat]?

Complete! NAT Translate Range defined.

NOTE: The associated RESERVE POOL for this TRANSLATE RANGE has been found.

NOTE: You must have a corresponding OUTBOUND IP Access Control rule
      applied to your designated NAT interface.
      The rule should include the following information:
          Type=IN (include + NAT)
          SOURCE_Addr=9.24.106.0
          SOURCE_Mask=255.255.255.0
VPNRTR2 NAT config>EXIT
VPNRTR2 Config>
```

Ahora necesitamos crear los filtros de paquete IP. La Tabla 135 en la página 341 muestra que se habilita el control de acceso y, a continuación, se crean los filtros conectados a la L2Net y se denominan out-6 e in-6.

Tabla 135. Añadir filtros de paquetes

```
VPNRTR2 Config>PROTOCOL IP
Internet protocol user configuration
VPNRTR2 IP config>SET ACCESS-CONTROL ON
VPNRTR2 IP config>

VPNRTR2 IP config>ADD PACKET-FILTER
Packet-filter name []? out-6
Filter incoming or outgoing traffic? [IN]? out
Which interface is this filter for [0]? 6

VPNRTR2 IP config>ADD PACKET-FILTER
Packet-filter name []? in-6
Filter incoming or outgoing traffic? [IN]?
Which interface is this filter for [0]? 6
VPNRTR2 IP config>
```

Una vez que se han creado los filtros de paquetes, utilice el mandato **update packet-filter** para definir los filtros. La finalidad del filtro out-6 es dirigir todos los paquetes que proceden de la subred 9.24.106.0 y están destinados a Internet a la función NAT (Network Address Translation) (Conversión de dirección de red).

Tabla 136. Actualizar el filtro de paquetes de salida

```
VPNRTR2 IP config>UPDATE PACKET-FILTER
Packet-filter name []? out-6
VPNRTR2 Packet-filter 'out-6' Config>ADD ACCESS-CONTROL
Access Control type [E]? N      1
Internet source [0.0.0.0]? 9.24.106.0
Source mask [255.255.255.0]?
Internet destination [0.0.0.0]?
Destination mask [0.0.0.0]?
Starting protocol number ([0] for all protocols) [0]?
Starting DESTINATION port number ([0] for all ports) [0]?
Starting SOURCE port number ([0] for all ports) [0]?
Filter on ICMP Type ([-1] for all types) [-1]?
TOS/Precedence filter mask (00-FF - [0] for none) [0]?
TOS/Precedence modification mask (00-FF - [0] for none) [0]?
Enable logging? [No]:
VPNRTR2 Packet-filter 'out-6' Config>exit
```

1. El tipo N especifica que el datagrama debe enviarse a la función NAT.

La finalidad del filtro in-6 es dirigir todos los paquetes que proceden de la Internet y están destinados a la subred 9.24.106.0 a la función NAT.

Tabla 137. Actualizar el filtro de paquetes de entrada

```
VPNRTR2 IP config>UPDATE PACKET-FILTER
Packet-filter name []? in-6
VPNRTR2 Packet-filter 'in-6' Config>ADD ACCESS-CONTROL
Access Control type [E]? N
Internet source [0.0.0.0]?
Source mask [0.0.0.0]?
Internet destination [0.0.0.0]?
Destination mask [0.0.0.0]?
Starting protocol number ([0] for all protocols) [0]?
Starting DESTINATION port number ([0] for all ports) [0]?
Starting SOURCE port number ([0] for all ports) [0]?
Filter on ICMP Type ([-1] for all types) [-1]?
TOS/Precedence filter mask (00-FF - [0] for none) [0]?
TOS/Precedence modification mask (00-FF - [0] for none) [0]?
Enable logging? [No]:
VPNRTR2 Packet-filter 'in-6' Config>exit
VPNRTR2 IP config>EXIT
VPNRTR2 Config>
```

Esto completa la configuración del direccionador de bifurcación. Como siempre, es una buena idea guardar la configuración en el programa de configuración o en un servidor TFTP.

Configurar servidor de acceso remoto NT

Para configurar el Servidor de acceso remoto NT, siga estos pasos:

- IP en la Red en Anillo accesible por Internet = 192.168.141.34 / 255.255.255.240
- IP en ethernet = 192.168.141.65 / 255.255.255.240
- Añada el protocolo PPTP con un mínimo de 1 interfaz VPN
- En el servicio de acceso remoto, añada un dispositivo RAS
- Enlace la interfaz VPN al servidor RAS
- Configure la agrupación IP de 192.168.141.70—192.168.141.73

Añada un nombre de usuario NT **rtr-1** y una contraseña de **rtr-1**. Esto debe coincidir con los valores configurados en la Tabla 129 en la página 338. Inhabilite la opción ″change password on first logon″ (cambiar contraseña en primera conexión) y establezca la contraseña para que no caduque nunca.

Debe poder establecerse contacto con el sistema NT a través de la nube IP. Para prevenir el uso ilegal, puede habilitar el filtro PPTP en la interfaz que está conectada a la nube IP. Esto hará que el servidor PPTP sólo acepte paquetes PPTP de usuarios autentificados. El usuario, (el direccionador remoto en nuestro ejemplo), se define utilizando la función de ″gestión de usuarios″ en NT. Todos los paquetes no PPTP o el tráfico PPTP procedente de usuarios no autentificados se eliminará.

Consulte la siguiente página Web de Microsoft para obtener información sobre cómo configurar el servidor PPTP:
`http://www.microsoft.com/NTServer/commserv/deployment/planguides/installing_pptp.asp`

Supervisión y resolución de problemas de la configuración

Utilice ELS para supervisar dinámicamente el túnel PPTP. Configure ELS para visualizar sólo el subsistema L2 emitiendo el mandato **NODISPLAY SUBSYSTEM ALL** seguido del mandato **DISPLAY SUBSYSTEM L2 ALL ALL**. A continuación, emita el mandato **TALK 2** como se muestra en la Tabla 138 en la página 343.

Observe que habrá un tráfico de tipo ″keepalive″ cada 30 segundos incluso aunque no haya ningún otro tráfico.

Tabla 138. Salida de ELS para el subsistema L2

```
VPNRTR2 *TALK 2

40:19:49   L2.024: PPTP PAYLOAD SEND 38 bytes, net=6, callid=55253
40:19:49   L2.041: SND PPTP:F=3081,L=54,Tid=0,Cid=0,NS=121,NR=122,O=0
40:19:49   L2.040: RCV PPTP:F=3081,L=38,Tid=20169,Cid=55253,NS=123,NR=121,O=0
40:19:49   L2.022: PPTP PAYLOAD RCVD 38 bytes, net 6, callid=55253
40:19:59   L2.024: PPTP PAYLOAD SEND 38 bytes, net=6, callid=55253
40:19:59   L2.041: SND PPTP:F=3081,L=54,Tid=0,Cid=0,NS=122,NR=123,O=0
40:19:59   L2.040: RCV PPTP:F=3081,L=38,Tid=20169,Cid=55253,NS=124,NR=122,O=0
40:19:59   L2.022: PPTP PAYLOAD RCVD 38 bytes, net 6, callid=55253
```

Para este ejemplo, al emitir el mandato **INTERFACE** en el indicador de Protocolo IP de Talk 5, se muestra que a la interfaz PPP/4 se le ha asignado una dirección IP en la subred en el otro extremo del túnel. Recuerde que hemos configurado el RAS NT para asignar direcciones IP de una agrupación que empieza en 192.168.141.70 y finaliza en 192.168.141.73.

El sistema principal RAS NT ha tomado .70 para su dirección de punto final de túnel y ha asignado .71 al Network Utility en el otro punto final del túnel.

Tabla 139. Visualizar la información de interfaz

```
VPNRTR2 *TALK 5

CGW Operator Console
VPNRTR2 + PROTOCOL IP
VPNRTR2 IP>INTERFACE
Interface    MTU   IP Address(es)   Mask(s)         Address-MTU
  PPP/0     2044   192.168.141.17   255.255.255.240 Unspecified
  TKR/0     4082   9.24.106.8       255.255.255.0   Unspecified
  PPP/4     1500   192.168.141.71   255.255.255.255 Unspecified
VPNRTR2 IP>EXIT
```

Utilice los mandatos **call state** y **call statistics** en el indicador FEATURE Layer-2-Tunneling como se muestra en la Tabla 140 para verificar la actividad de túnel.

Tabla 140. Visualizar estado y estadísticas de túnel

```
VPNRTR2 +FEATURE Layer-2-Tunneling
Layer-2-Tunneling Information
VPNRTR2 Layer-2-Tunneling Console> CALL STATE
CallID │ Serial # │ Net # │    State    │ Time Since Chg │ PeerID │ TunnelID
 64985 │        0 │     6 │ Established │     0:13:46    │      0 │    19704

VPNRTR2 Layer-2-Tunneling Console> CALL STATISTICS
CallID │ Serial # │ Tx Pkts │ Tx Bytes │ Rx Pkts │ Rx Bytes │  RTT  │  ATO
 64985 │        0 │      95 │     3440 │      97 │     3415 │     0 │
0
VPNRTR2 Layer-2-Tunneling Console>
```

Nota: En >FEATURE Layer-2-Tunneling, puede utilizar la secuencia de mandatos siguiente: =>T5, =>NET 6, =>LIST ALL.

Túnel L2TP voluntario iniciado por Network Utility de IBM

Siga los pasos del apartado Túnel PPTP voluntario iniciado por Network Utility de IBM con las excepciones siguientes:

- Habilite L2TP
- Especifique L2TP en el perfil de túnel

Nota: Los indicadores son ligeramente diferentes en este paso (consulte la Tabla 141).

Tabla 141. Especificar L2TP en el perfil de túnel

```
add tunnel-profile
Enter name: [ ]? L2TP peer
Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
Enter local host name: [ ] netU
Set shared secret? (Yes, No): [No] y
Shared secret for tunnel authentication: * will not appear
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0] 192.168.141.34

      Tunnel name: L2TP peer
      Tunn Type 3: L2TP
      Endpoint: 192.168.141.34
      Local Hostname: netU
Tunnel 'NT' has been added
```

Túnel L2TP terminado en un LNS de Network Utility de IBM

El escenario de ejemplo de L2TP establecerá la conexión entre un usuario de llamada remoto de la bifurcación y el Network Utility de la corporación utilizando el túnel L2TP. Consulte el diagrama de red de ejemplo de la Figura 78 en la página 345.

Conexión de usuarios que llaman desde una ubicación remota

Otra aplicación de VPN es conectar usuarios remotos que llaman a una ubicación central desde una red IP pública, por ejemplo Internet. El servidor de acceso remoto puede administrarlo un ISP o la compañía del usuario. Este escenario muestra cómo utilizar el IBM Nways 2210/Network Utility como servidores RLAN (Remote LAN Access) (Acceso de LAN remoto) utilizando las características L2TP y DIALs (Dial In Access to LANs) (Acceso a las LAN mediante llamada) del IBM Nways 2210/Network Utility.

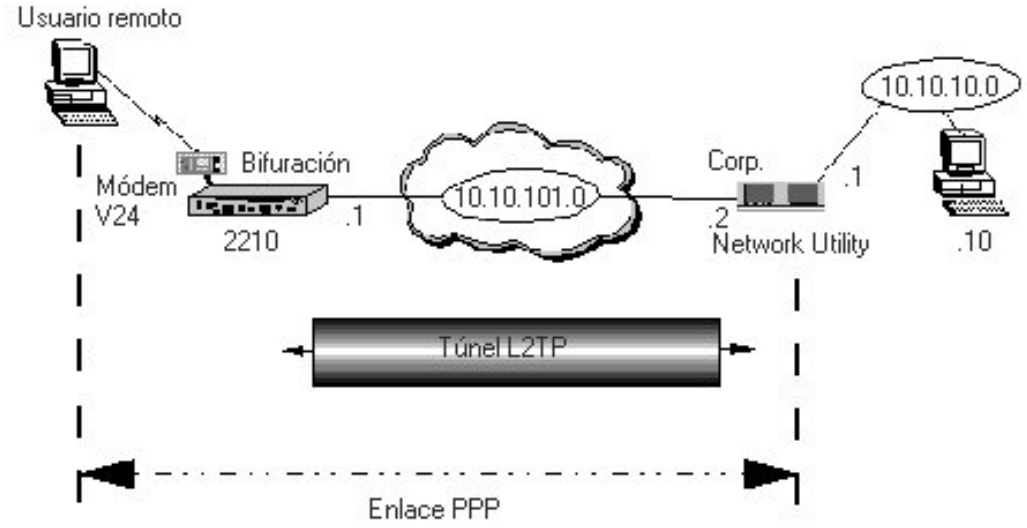


Figura 78. Configuración de ejemplo de L2TP

En este ejemplo se ha utilizado el IBM Nways 2210/Network Utility, y el 2210 de la bifurcación proporciona un servidor de acceso RLAN para los usuarios que llaman desde una ubicación remota. Se define un túnel L2TP entre el direccionador de bifurcación y el Network Utility en el centro de datos para que los usuarios remotos puedan utilizar la función RLAN en el Network Utility a fin de acceder a recursos de la intranet corporativa. Dado que la conexión 2TP se basa en IP, este tráfico también se puede enviar a través del túnel IPSec si IPSec también está configurado. Con esta alternativa, L2TP está dentro del túnel IPSec.

Configuración del direccionador de bifurcación para que actúe de servidor de acceso de llamadas entrantes

El direccionador de bifurcación 2210 se ha configurado para que un usuario remoto pueda acceder a él a través de un módem de llamada V.34 y luego extender las sesiones del usuario remoto a la ubicación del centro de datos corporativo a través de una red IP, por ejemplo Internet, utilizando L2TP para colocar en el túnel la sesión PPP desde el 2210 de la sucursal al Network Utility de IBM de la ubicación central.

Notas:

1. En este escenario se muestra el uso de V.34 para el acceso de usuario remoto. Sin embargo, el 2210 soporta V.34, RDSI BRI y V.25bis. V.34 se soporta mediante módems externos conectados a puertos WAN o a través de los Adaptadores de acceso de llamada de 4 u 8 puertos que disponen de módems V.34 integrados.
2. La red IP puede ser cualquier red basada en IP, por ejemplo Internet o una red frame-relay pública. En este escenario, la red IP se representa mediante un enlace WAN serie PPP.

El primer paso de la configuración de RLAN es añadir una interfaz V.34. Esto se muestra en la Tabla 142 en la página 346.

Tabla 142. Adición de una dirección V.34 y configuración de la interfaz V.34

```
Branch *t 6
Gateway user configuration
Branch Config>add V34-ADDRESS
Assign address name [1-23] chars []? local
Assign network dial address [1-30 digits] []? 9193013461
Branch Config>set data v34
Interface Number [0]? 4
Branch Config>net 4
V.34 Data Link Configuration
Branch V.34 System Net Config 4>set local-address
Local network address name []? local
```

Debe correlacionar el puerto V.34 con la dirección V.34. También puede establecer la velocidad y la serie de inicialización del módem, pero en este ejemplo se utilizan los parámetros por omisión. Puede comprobar los parámetros que ha configurado con el mandato **'list all'**, tal como se muestra en la Tabla 143.

Tabla 143. Listado de la configuración del puerto V.34

```
Branch V.34 System Net Config   4>LIST all

         V.34 System Net Configuration:

Local Network Address Name    = local
Local Network Address         = 9193013461

Non-Responding addresses:
Retries                       = 1
Timeout                       = 0 seconds

Mode                          = Switched

Call timeouts:
Command Delay                 = 0 ms
Connect                       = 60 seconds
Disconnect                    = 2 seconds

Modem strings:
Initialization string         =

Speed (bps)                   = 115200
```

El paso siguiente es crear las interfaces virtuales utilizadas para las conexiones de llamadas remotas. Los usuarios de RLAN utilizan una clase especial de circuito para llamada, que se denomina 'circuito de llamada'. En este escenario, se crea una interfaz virtual para nuestro usuario de prueba RLAN individual. Sin embargo, puede crear muchas más interfaces virtuales. El límite práctico es el número de puertos asíncronos disponibles en el direccionador.

Las interfaces para las llamadas remotas se añaden desde el indicador **talk 6 Config>** como se muestra en la tabla siguiente.

Tabla 144. Creación de las interfaces virtuales de llamada

```
Branch Config>ADD DEVICE DIAL-IN
Enter the number of PPP Dial-in Circuit interfaces [1]?
Adding device as interface 6
Base net for this circuit [0]? 4
Enable as a Multilink PPP link? [no]
Disabled as a Multilink PPP link.
Defaulting Data-link protocol to PPP
Add more dial circuit interface(s)?(Yes or [No]):
Use "net " command to configure circuit parameters

Branch Config>LIST DEVICES
Ifc 0     Ethernet            CSR  81600, CSR2  80C00, vector 94
Ifc 1     WAN PPP             CSR  81620, CSR2  80D00, vector 93
Ifc 2     WAN PPP             CSR  81640, CSR2  80E00, vector 92
Ifc 3     WAN PPP             CSR 381620, CSR2 380D00, vector 125
Ifc 4     V.34 Base Net       CSR 381640, CSR2 380E00, vector 124
Ifc 5     Token Ring          CSR 6000000, vector 95
Ifc 6     PPP Dial-in Circuit

Branch Config>NETWORK 6
Circuit configuration
Branch Dial-in Circuit config:   6>LIST all

Base net                       = 4
Circuit priority               = 8
```

Nota: Sólo se soporta PPP por V.34. Sin embargo, con DIALs, se pueden soportar múltiples protocolos (IP, IPX, NetBIOS, 802.2 y LLC) por la conexión PPP.

Para cada circuito de llamada, existen diversos parámetros que pueden configurarse; sin embargo, éstos se dejan generalmente en los valores por omisión.

Para direccionar IP a través de la interfaz V.34, se debe asignar una dirección IP a la interfaz. Cuando el cliente llama, el direccionador añade automáticamente una ruta estática a la tabla de direccionamiento que indica que el siguiente salto para el usuario remoto es la dirección IP de la interfaz virtual V.34.

La dirección debe estar en una subred diferente de la del segmento LAN de destino. Puede utilizar una dirección IP real o una IP sin número. El formato de la dirección IP sin número es 0.0.0.n, donde n es el número de interfaz. La Tabla 145 muestra el diálogo para este escenario. La interfaz 6 es la interfaz virtual para el usuario de llamada de prueba.

Tabla 145. Configuración de direcciones IP en las interfaces virtuales

```
Branch IP config>LIST ADDRESSES
IP addresses for each interface:
   intf     0                                IP disabled on this interface
   intf     1  10.10.101.1 255.255.255.0     Local wire broadcast, fill 1
   intf     2                                IP disabled on this interface
   intf     3                                IP disabled on this interface
   intf     4                                IP disabled on this interface
   intf     5  10.10.1.1   255.255.255.0     Local wire broadcast, fill 1
   intf     6                                IP disabled on this interface

Branch IP config>add address
Which net is this address for [0]? 6
New address []? 0.0.0.6
Address mask [0.0.0.0]? 255.255.255.0
```

Debe habilitarse el direccionamiento de subred ARP a fin de permitir al direccionador responder a los ARP cuando el salto siguiente al destino sea a través

de una interfaz diferente de la que está recibiendo la petición ARP. Esto es lo que sucede en el caso de RLAN donde la dirección IP de cliente está en la misma subred que la interfaz de LAN del direccionador, pero el salto siguiente (la interfaz V.34) está en una subred diferente. El direccionamiento de subred ARP se habilita como se muestra en la Tabla 146.

Tabla 146. Habilitación del direccionamiento de subred ARP

```
Branch IP config>ENABLE ARP-SUBNET-ROUTING

Branch IP config>LIST ADDRESSES
IP addresses for each interface:
   intf     0                                  IP disabled on this interface
   intf     1  10.10.101.1 255.255.255.0       Local wire broadcast, fill 1
   intf     2                                  IP disabled on this interface
   intf     3                                  IP disabled on this interface
   intf     4                                  IP disabled on this interface
   intf     5  10.10.1.1   255.255.255.0       Local wire broadcast, fill 1
   intf     6  0.0.0.6     255.255.255.0       Local wire broadcast, fill 1
```

De este modo se concluye la configuración del direccionador de bifurcación para la función DIALs básica. Ahora el direccionador se reinicia para activar los cambios como se muestra en la Tabla 147.

Tabla 147. Reinicio del direccionador

```
Branch config>
Branch *res
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

Configuración de L2TP en el direccionador de bifurcación

Para este ejemplo, la conexión PPP del usuario de llamada puede extenderse definiendo un túnel L2TP entre el 2210 de la ubicación de sucursal y el Network Utility del centro de datos. El usuario final debe poder utilizar la función RLAN en el Network Utility para conectarse a recursos del centro de datos.

L2TP es un mecanismo que incluye un túnel entre un LAC (L2TP Access Concentrator) (Concentrador de acceso L2TP) y un LNS (L2TP Network Server) (Servidor de red L2TP). En este escenario, el 2210 de la sucursal se configurará como LAC y el Network Utility se configurará como LNS. El primer paso es habilitar L2TP en el LAC. Consulte la Tabla 148.

Tabla 148. Habilitación de L2TP en el LAC (Direccionador de bifurcación)

```
Branch Config> FEATURE Layer-2-Tunneling
Branch Layer-2-Tunneling Config>ENABLE L2TP

 Restart system for changes to take effect.
Branch Layer-2-Tunneling Config>EXIT
```

A continuación, se crea un túnel en el LAC. Esto se muestra en la Tabla 149 en la página 349.

Tabla 149. Creación del túnel L2TP en el LAC (Direccionador de bifurcación)

```
Branch Config>ADD TUNNEL-PROFILE
Enter name:  []? lns.org
Tunneling Protocol?  (PPTP, L2F, L2TP): [L2TP]
Enter local hostname: []? lac.org
set shared secret? (Yes, No): [No] y
Shared secret for tunnel authentication:
Enter again to verify:
Passwords do not match.
...try again
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 10.10.101.2

       Tunnel name: lns.org
          TunnType: L2TP
          Endpoint: 10.10.101.2
    Local Hostname: lac.org

Tunnel 'lns.org' has been added

Branch Config>LIST TUNNEL-PROFILES
TunnType  Endpoint         Tunnel name              Hostname

L2TP      10.10.101.2      lns.org                  lac.org

1 TUNNEL record displayed.
```

Las notas siguientes pertenecen a la configuración de túnel de LAC:

Tunnel name
Este nombre debe coincidir con el nombre de sistema principal que se ha configurado en el LNS (Network Utility).

Hostname
Éste es el nombre de sistema principal del LAC.

Tunnel-Server endpoint
Dirección IP del punto final del túnel. Esta dirección tiene que poderse acceder desde el LAC. Puede ser cualquier dirección de interfaz o una dirección IP interna del Network Utility. Aquí se utiliza la dirección de la interfaz que es el punto final del túnel.

Shared secret
Este parámetro debe establecerse si se necesita la autentificación en el túnel y el valor aquí debe coincidir con el valor configurado en el LNS. La autentificación de túnel L2TP está habilitada por omisión.

Para activar estos cambios, se deberá reiniciar el direccionador.

Configuración de L2TP en el Network Utility

El 2216 se ha configurado como un Servidor de red L2TP (LNS). En primer lugar, se ha habilitado L2TP en el LNS. Esto se muestra en la Tabla 150.

Tabla 150. Habilitación de L2TP en el LNS

```
Corp Config>FEATURE Layer-2-Tunneling
Corp Layer-2-Tunneling Config>ENABLE L2TP

 Restart system for changes to take effect.
Corp Layer-2-Tunneling Config>EXIT
```

A continuación se crea el túnel en el LNS, apuntando a la dirección IP y al nombre del LAC. Esto se muestra en la Tabla 151.

Tabla 151. Creación del túnel L2TP en el LNS (Corp Network Utility)

```
Corp Config>ADD TUNNEL-PROFILE
Enter name:  []? lac.org
Tunneling Protocol?  (PPTP, L2F, L2TP): [L2TP]
Enter local hostname: []? lns.org
set shared secret? (Yes, No): [No] Y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 10.10.101.1

       Tunnel name: lac.org
          TunnType: L2TP
          Endpoint: 10.10.101.1
    Local Hostname: lns.org
Tunnel 'lac.org' has been added

Corp Config>LIST TUNNEL-PROFILES
TunnType  Endpoint         Tunnel name            Hostname

L2TP      10.10.101.1      lac.org                lns.org

1 TUNNEL record displayed.
```

Nota: Si está utilizando secretos compartidos, la clave debe coincidir con la configurada en el LAC.

Puede modificar los parámetros PPP para el túnel L2TP. Sin embargo, estos parámetros se negociarán entre el LAC y el LNS. El LAC actúa como proxy para el PC cliente en la negociación PPP. Se debe habilitar un protocolo de autentificación para el túnel L2TP. Para este escenario se han utilizado los parámetros PPP por omisión en el LNS.

A continuación, se añadieron las interfaces virtuales donde irán a parar las conexiones PPP. Éstas son análogas a la interfaz de llamada entrante añadida al direccionador de bifurcación cuando se configuró para la función DIALs. Sin embargo, en este caso, los usuarios entran a través de un túnel L2TP en lugar de una interfaz V.34.

En el LNS, se añaden las interfaces virtuales desde el indicador de configuración de característica L2TP. (En el LAC, se han añadido desde el indicador principal de talk 6). Esto se muestra en la Tabla 152.

Tabla 152. Adición de la interfaz virtual

```
Corp Config>FEATURE Layer-2-Tunneling
Corp Layer-2-Tunneling Config>ADD L2-NETS
Additional L2 nets:  [0]? 2
Add unnumbered IP addresses for each L2 net? [Yes]:
Adding device as interface 6
Defaulting Data-link protocol to PPP
Adding device as interface 7
Defaulting Data-link protocol to PPP
Enable IPX on L2T interfaces?(Yes or [No]):
Enable transparent bridging on L2T interfaces?(Yes or [No]):
Bridge configuration was not changed.

Restart router for changes to take affect.
Corp Layer-2-Tunneling Config>EXIT
```

Para direccionar IP a través de las redes L2, se debe asignar una dirección IP a la interfaz. Cuando el cliente establece la conexión PPP a través del túnel L2TP, el direccionador añade automáticamente una ruta estática a la tabla de direccionamiento que indica que el salto siguiente para el usuario remoto es la dirección IP de la interfaz virtual L2TP. La dirección debe estar en una subred diferente de la del segmento de LAN de destino.

Las direcciones IP para estas interfaces se añaden al crear las interfaces. Por omisión, son direcciones IP sin número. El formato de la dirección es 0.0.0.n donde n es el número de interfaz (por ejemplo, para la interfaz 7, la dirección IP sin número será 0.0.0.7).

Nota: Si necesita cambiar la dirección IP por omisión asociada con una red L2TP, puede hacerlo a través del indicador IP config en talk 6. Sin embargo, el direccionamiento IP sin número funciona muy bien para RLAN porque los usuarios se conectan a una red L2TP de forma arbitraria y la dirección IP particular asociada con una red L2TP no es muy crítica.

Se debe habilitar el direccionamiento de subred ARP a fin de permitir al direccionador responder a los ARP cuando el salto siguiente al destino es a través de una interfaz diferente de la interfaz que está recibiendo la petición ARP. Esto es lo que sucede en el caso de RLAN donde la dirección IP del cliente está en la misma subred que la interfaz LAN del direccionador pero el salto siguiente (la interfaz L2TP virtual) está en una subred diferente. El direccionamiento de subred ARP se habilita como se muestra en la Tabla 153.

Tabla 153. Habilitación del direccionamiento de subred ARP

```
Corp config>protocol ip
Corp IP config>ENABLE ARP-SUBNET-ROUTING
Corp IP config>EXIT
```

A continuación, se define el método para que los clientes obtengan una dirección IP. El servidor DIALs del Network Utility necesita configurarse como si los usuarios estuvieran llamando a través de RDSI o V.34 en lugar de estableciendo la conexión a través de un túnel L2TP. A los usuarios de DIALs es necesario asignarles una dirección IP que esté en la misma subred que la interfaz de LAN a la que desean conectarse. Hay cinco métodos disponibles:

Client (Cliente) La dirección IP se configura en el cliente.

User ID
(ID de usuario) La dirección IP se configura en el direccionador como parte de la definición de ID de usuario y se envía al cliente cuando está autentificada. En este caso, la dirección IP está asociada con un usuario específico.

Interface
(Interfaz) La dirección IP se configura en la interfaz y se envía al cliente. Aquí, la dirección IP está asociada con la interfaz en lugar del ID de usuario.

DHCP Proxy
(Proxy DHCP) La dirección IP la proporcionará un servidor DHCP y el direccionador actúa como un proxy DHCP para el cliente.

IP Pool
(Agrupación IP) La agrupación IP le permite definir un bloque de

direcciones IP que se almacenan en una agrupación. Cuando un cliente se conecta y solicita una dirección IP, el direccionador toma una dirección de la agrupación.

Los métodos para que los clientes obtengan una dirección IP se configuran desde el menú global de DIALs. Los métodos de cliente, ID de usuario, interfaz y Agrupación IP están habilitados. El direccionador intentará utilizar el primer método que esté habilitado (en el orden listado). También puede definir servidores de nombres de dominios primario y secundario cuyas direcciones se pasan al cliente durante las negociaciones IPCP. Esto se muestra en la Tabla 154.

Tabla 154. Listado de métodos para obtener direcciones IP

```
Corp Config>FEATURE DIALs
Dial-in Access to LANs global configuration
Corp Config>FEATURE DIALs
Dial-in Access to LANs global configuration
Corp DIALs config>LIST IP-ADDRESS-ASSIGNMENT
DIALs client IP address assignment:
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled
```

En este escenario, se asigna la dirección IP para los usuarios de DIALs de una agrupación IP. Esto se muestra en la Tabla 155.

Tabla 155. Adición de agrupación IP para usuarios de DIALs

```
Corp Config>FEATURE DIALs
Dial-in Access to LANs global configuration
Corp DIALs config>ADD IP-POOL
Base address []? 10.10.10.11
Number of addresses [1]? 20
Corp DIALs config>LIST IP-POOLS
Configured IP address pools:
     Base Address      Last Address        Number
     ------------      ------------        ------
      10.10.10.11       10.10.10.30            20
```

En este punto, el túnel está configurado en el LNS y el LAC y la característica DIALs está configurada en el LNS. Ahora es necesario configurar los usuarios de PPP que establecerán la conexión al LNS a través de un túnel. Existen dos modos de configurar los usuarios de PPP que establecerán la conexión por túnel:

- **Túnel basado en Rhelm:** Utilizando este método, sólo es necesario definir el usuario en el LNS. Se deberá utilizar el formato, nombreusuario@dominio, donde dominio es el nombre de sistema principal del LNS. Cuando el cliente marque en el LAC utilizando el formato nombreusuario@dominio (por ejemplo, Sharif@lns.org), el LAC creará un túnel hacia el dominio especificado (lns.org) y la conexión PPP pasará por el túnel al destino deseado. Mediante este método, todos los usuarios con el mismo nombre de dominio pasan por el túnel hacia el mismo destino.
- **Túnel basado en el usuario:** Con este método, el perfil del usuario necesita configurarse en el LAC y el LNS y no utiliza el formato nombreusuario@dominio. En el LAC, especifique el destino final en el perfil del usuario. En el LNS, configure un usuario de llamada normal.

La Tabla 156 en la página 353 muestra la definición de un usuario basado en Rhelm en el Network Utility del centro de datos.

Tabla 156. Adición de un usuario L2TP basado en Rhelm

```
Corp Config>ADD PPP-USER
Enter name:  []? sharif@lns.org
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
Number of days before account expires [0-1000] [0]?
Number of grace logins allowed after an expiration [0-100] [0]?
IP address: [0.0.0.0]?
Enter hostname: []?
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Will user be able to dial-out ? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No]
Disable user ? (Yes, No): [No]


     PPP user name: sharif@lns.org
   User IP address: Interface Default
     Netroute Mask: 255.255.255.255
          Hostname:       Virtual Conn: disabled
      Time alotted: Box Default
     Callback type: disabled
          Dial-out: disabled
        Encryption: disabled
            Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
    Account Expiry:    Password Expiry:
Is information correct? (Yes, No, Quit): [Yes]

User 'sharif@lns.org' has been added
```

Para el túnel basado en el usuario, el ID se define tanto en el LAC como en el LNS. La Tabla 157 en la página 354 muestra la definición de un ID basado en el usuario en el 2210 de la sucursal. Este usuario está establecido para pasar por el túnel, y se notifica al direccionador que configure el túnel L2TP cuando el usuario efectúe la llamada. Se especifica la dirección IP de destino del otro punto final del túnel junto con el nombre de sistema principal del 2210 a utilizar al crear el túnel.

Tabla 157. Adición de un usuario de túnel basado en usuario en el 2210 (LAC)

```
Branch Config>ADD PPP-USER
Enter name:  []? shoma
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No] y
Tunneling Protocol?  (PPTP, L2F, L2TP): [L2TP]
Enter local hostname: []? lac.org
Tunnel-Server endpoint address: [0.0.0.0]? 10.10.101.2

     PPP user name: shoma
          TunnType: L2TP
          Endpoint: 10.10.101.2
    Local Hostname: lac.org

Is information correct? (Yes, No, Quit): [Yes] y

User 'shoma' has been added
```

Nota: Tan pronto haya especificado que el usuario pasará por el túnel, el direccionador sabrá que para dicho usuario no deberá preguntarle si desea habilitar la función DIALs, ni cuál tendría que ser la dirección IP del cliente como tampoco sobre ninguno de los parámetros que se le solicitan cuando se define un usuario DIALs. Esto se debe a que la función DIALs para este usuario la proporciona el Network Utility. El 2210 está simplemente proporcionando un servicio de pasarela al Network Utility.

La Tabla 158 en la página 355 muestra la definición del mismo ID basado en usuario en el 2216 en el centro de datos. Aquí se define un usuario de DIALs normal. Este usuario no es un usuario de túnel dado que la función DIALs lo autentifica. Antes de que esté autentificado, todas las cabeceras L2TP se han eliminado y los paquetes son simplemente paquetes PPP normales. Esto completa la configuración del LNS.

Tabla 158. Adición de un usuario de túnel basado en usuario en el Network Utility (LNS)

```
Corp Config>ADD PPP-USER
Enter name:  []? shoma
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
Number of days before account expires [0-1000] [0]?
Number of grace logins allowed after an expiration [0-100] [0]?
IP address: [0.0.0.0]?
Enter hostname: []?
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Will user be able to dial-out ? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No]
Disable user ? (Yes, No): [No]


     PPP user name: shoma
   User IP address: Interface Default
     Netroute Mask: 255.255.255.255
          Hostname:       Virtual Conn: disabled
      Time alotted: Box Default
     Callback type: disabled
          Dial-out: disabled
        Encryption: disabled
            Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
    Account Expiry:    Password Expiry:
Is information correct? (Yes, No, Quit): [Yes] y

User 'shoma' has been added
```

Para activar estos cambios, se deberá reiniciar el Network Utility.

Supervisión de L2TP

Ahora que la configuración ya está en su sitio, se pueden probar las configuraciones de L2TP y RLAN. El L2TP puede probarse llamando desde el PC remoto, primero con el ID de usuario basado en Rhelm y, a continuación, con el ID basado en usuario.

La conectividad IP puede probarse utilizando PING desde el cliente PC al Network Utility. L2TP puede supervisarse desde ELS utilizando disp sub l2 all. En la Tabla 159 en la página 356 se muestra una sesión de talk 2 de ejemplo desde el LNS de Network Utility.

Tabla 159. Supervisión de L2TP desde ELS

```
Corp *TALK 2
00:04:27   L2.052: Tunnel 7042/0 has 15 seconds to establish itself
00:04:27   L2.050: EVENT Rx-SCCRQ,tid=7042/0,state=Idle
00:04:27   L2.048: RCV l2tpGetHostname, tid=7042/0
00:04:27   L2.058: Peer TunnelID = 48802
00:04:27   L2.060: Peer Hostname = lac.org
00:04:27   L2.047: Tunnel 7042/48802 State Changed Idle -> Authorizing
00:04:27   L2.074: Upcall from AAA subsystem, request SUCCESS
00:04:27   L2.050: EVENT Continue-SCCRQ,tid=7042/48802,state=Authorizing
00:04:27   L2.048: RCV SCCRQ, tid=7042/48802
00:04:27   L2.058: Peer TunnelID = 48802
00:04:27   L2.060: Peer Hostname = lac.org
00:04:27   L2.058: Peer Rcv Window = 4
00:04:27   L2.058: Peer Challenge = 0
00:04:27   L2.049: SEND SCCRP, tid=7042/48802
00:04:27   L2.035: Tunnel Auth Create Challenge, Tid=7042/48802, Len=16
00:04:27   L2.035: Tunnel Auth Create Challenge Response, Tid=7042/48802,
Len=16
00:04:27   L2.044: Allocating UDP port 1026 for tunnelid=7042
00:04:27   L2.041: SND L2TP:F=C802,L=121,Tid=48802,Cid=0,NS=0,NR=1,O=0
00:04:27   L2.047: Tunnel 7042/48802 State Changed Authorizing -> Wait-ctl-cnn
00:04:27   L2.040: RCV L2TP:F=C800,L=42,Tid=7042,Cid=0,NS=1,NR=1,O=0
00:04:27   L2.050: EVENT Rx-SCCCN,tid=7042/48802,state=Wait-ctl-cnn
00:04:27   L2.048: RCV SCCCN, tid=7042/48802
00:04:27   L2.057: Processing Challenge Response from Peer 4.7.3.3
00:04:27   L2.039: NOTE:SCCCN: Tunnel Authenticated
00:04:27   L2.047: Tunnel 7042/48802 State Changed Wait-ctl-cnn -> Established
00:04:27   L2.040: RCV L2TP:F=C800,L=48,Tid=7042,Cid=0,NS=2,NR=1,O=0
00:04:27   L2.007: LNS Allocated L2 net 8
00:04:27   L2.020: RCV Inbound-Call-Request, callid=25642, net=8
00:04:27   L2.021: SEND Inbound-Call-Reply, callid=25642, net=8
00:04:27   L2.041: SND L2TP:F=C802,L=44,Tid=48802,Cid=1156,NS=1,NR=3,O=0
00:04:27   L2.013: L2TP Call 25642 State Changed Idle -> Wait Connect
00:04:27   L2.030: LNS Forcing LCP option ACFC
00:04:27   L2.039: NOTE:Proxy-LCP Callback received
00:04:27   L2.009: Call Rcv Proxy-Auth-Type AVP,attr=29,val=4,len=8,flag=8008
00:04:27   L2.009: Call Rcv SEQUENCING_REQUIRED AVP,attr=39,val=0,len=6,flag=800
00:04:27   L2.013: L2TP Call 25642 State Changed Wait Connect -> Established
00:04:27   L2.015: Call Established-LNS,net=8,speed=115200,flags=4802
00:04:27   L2.017: Using Proxy-LCP AUTH on net 8
00:04:27   L2.021: SEND Set-Link-Info, callid=25642, net=8
00:04:27   L2.041: SND L2TP:F=C802,L=36,Tid=48802,Cid=1156,NS=2,NR=4,O=0
00:04:27   L2.040: RCV L2TP:F=C800,L=12,Tid=7042,Cid=0,NS=4,NR=3,O=0
00:04:32   L2.022: L2TP PAYLOAD RCVD 53 bytes, net 8, callid=25642
00:04:32   L2.024: L2TP PAYLOAD SEND 6 bytes, net=8, callid=25642
00:04:32   L2.041: SND L2TP:F=6902,L=18,Tid=48802,Cid=1156,NS=1,NR=2,O=0
00:04:32   L2.024: L2TP PAYLOAD SEND 8 bytes, net=8, callid=25642
```

Se puede comprobar el estado de túnel L2TP desde talk 5 como se muestra en la Tabla 160 en la página 357.

Tabla 160. Supervisión de L2TP desde talk 5

```
Branch *TALK 5

Branch +FEATURE Layer-2-Tunneling
Layer-2-Tunneling Information
Branch Layer-2-Tunneling Console> TUNNEL STATE
Tunnel ID │ Type │ Peer ID │    State    │ Time Since Chg │ # Calls │ Flags
    35589 │ L2TP │   58774 │ Established │     0: 1:24    │       1 │  TL
 F
Branch Layer-2-Tunneling Console> TUNNEL STATISTICS
Tunnel ID │ Type │ Tx Pkts │ Tx Bytes │ Rx Pkts │ Rx Bytes │  RTT  │  ATO
    35589 │ L2TP │     108 │     7883 │     104 │     5388 │     5 │     5


Corp *TALK 5
Corp +FEATURE Layer-2-Tunneling
Layer-2-Tunneling Information
Corp Layer-2-Tunneling Console> TUNNEL STATE
Tunnel ID │ Type │ Peer ID │    State    │ Time Since Chg │ # Calls │ Flags
    58774 │ L2TP │   35589 │ Established │     0: 2: 9    │       1 │  TL
 F
Corp Layer-2-Tunneling Console> TUNNEL STATISTICS
Tunnel ID │ Type │ Tx Pkts │ Tx Bytes │ Rx Pkts │ Rx Bytes │  RTT  │  ATO
    58774 │ L2TP │     108 │     5540 │     112 │     8035 │     5 │     5
```

Esto completa la configuración y supervisión de L2TP para el Acceso a LAN remoto utilizando el IBM 2210 y Network Utility.

Parte 4. Apéndices

Apéndice A. Avisos

Las referencias que se hacen en esta publicación a productos, programas o servicios de IBM no implican que IBM tenga la intención de comercializarlos en todos los países en los que IBM realiza operaciones. Cualquier referencia a un producto, programa o servicio de IBM no pretende afirmar o dar a entender que sólo se pueda utilizar el producto, programa o servicio de IBM. En su lugar se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no vulnere los derechos de propiedad intelectual válidos u otros derechos legalmente protegidos de IBM. La evaluación y verificación del funcionamiento conjunto con otros productos, excepto aquéllos expresamente designados por IBM, son responsabilidad del usuario.

IBM puede tener patentes o solicitudes de patentes pendientes que afecten a los temas tratados en este documento. La entrega de este documento no confiere ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A

Aviso para los usuarios de las versiones en línea de este manual

Para las versiones en línea de este manual, le autorizamos a:

- Copiar, modificar e imprimir la documentación contenida en el soporte de almacenamiento, para uso dentro de la empresa, a condición de que reproduzca el aviso de copyright, todas las declaraciones de aviso y otras declaraciones necesarias en cada copia total o parcial.
- Transferir la copia original de la documentación sin modificarla al transferir el producto de IBM relacionado (que pueden ser máquinas de su propiedad o programas, si los términos de la licencia del programa permiten la transferencia). Al mismo tiempo, deberá destruir todas las demás copias de la documentación.

El usuario es responsable del pago de cualquier tasa, incluidas las tasas de propiedad personales, que se produzca debido a esta autorización.

NO HAY GARANTÍAS, EXPRESAS O IMPLÍCITAS, INCLUIDAS LAS GARANTÍAS DE COMERCIALIZACIÓN E IDONEIDAD PARA UNA FINALIDAD DETERMINADA.

Algunas jurisdicciones no permiten la exclusión de las garantías implícitas, por lo que la exclusión anterior puede que no se aplique a su caso.

El incumplimiento de los términos mencionados más arriba anula esta autorización, con lo que deberá destruir toda su documentación informatizada.

Avisos sobre emisiones electrónicas

Nota de la Comisión Federal de Comunicaciones (FCC)

Aviso: Este equipo genera y utiliza energía de radio frecuencia, y si no se instala y utiliza de acuerdo con el manual de instrucciones, puede causar interferencias en las comunicaciones de radio. Se ha probado y encontrado que cumple con los

límites para un dispositivo de proceso de Clase A, de acuerdo con las especificaciones del Subapartado J del Apartado 15 de las normas de la FCC, las cuales han sido diseñadas para proporcionar, en un entorno comercial, una protección razonable contra tales interferencias. Es probable que el funcionamiento de este equipo en un área residencial cause interferencias, en cuyo caso se requerirá al usuario que tome, a su cargo, las medidas que sean necesarias para corregir dichas interferencias.

Instrucciones para el Usuario

Deben utilizarse conectores y cables adecuadamente blindados y con toma de tierra para conectar periféricos a fin de cumplir los límites de emisiones de la FCC. Los Concesionarios Autorizados IBM tienen disponibles los cables adecuados. IBM no es responsable de ninguna interferencia de radio o televisión ocasionada por la utilización de cables distintos a los recomendados o por modificaciones no autorizadas en este equipo. Es responsabilidad del usuario corregir tales interferencias.

Industry Canada Class A Emission Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité aux normes d'Industrie Canada

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

Declaración del Consejo de control voluntario para interferencias (VCCI) de Japón

Este producto es un Equipo de tecnología de la información de Clase A y cumple con los estándares expuestos por el Consejo de control voluntario para interferencias (VCCI) producidas por Equipo de tecnología. En un entorno doméstico, este producto puede ocasionar interferencias de radio, en cuyo caso puede que se solicite al usuario que tome las medidas pertinentes.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Declaración de cumplimiento del CISPR22

Este producto se ha probado y se ha encontrado conforme con los límites para Equipo de tecnología de la información de Clase A de acuerdo con el CISPR 22/estándar europeo EN 55022. Los límites para el equipo de la Clase A se han obtenido para entornos comerciales e industriales a fin de proporcionar una protección razonable contra las interferencias con equipo de comunicaciones con licencia.

Aviso: Éste es un producto de Clase A. En un entorno doméstico, este producto puede ocasionar interferencias de radio, en cuyo caso puede que se solicite al usuario que tome las medidas pertinentes.

Declaración de aviso de Clase A de Taiwán

警告使用者:
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

Declaración 89/336/EEC de la directiva EMC

Este producto se ajusta a los requisitos de protección de la Directiva 89/336/EEC del Consejo de la CE basada en la aproximación de las leyes de los Estados Miembros en relación a la compatibilidad electromagnética. IBM no puede aceptar ninguna responsabilidad por el incumplimiento de los requisitos de protección como consecuencia de una modificación no recomendada del producto, incluyendo la instalación de tarjetas opcionales que no sean IBM.

El producto (2216 Modelo 400) lleva la marca Telecom CE (CE 168 X) para la Velocidad básica RDSI conforme con I-CTR3 (Medidas de puente) según la directiva europea 91/263/EEC (directiva TTE). El producto lleva la marca Telecom CE (CE 168 X) para: las interfaces eléctricas V.24/V.28,V36 y X.21 conformes con el nivel físico NET 1 y NET 2. Velocidad básica de RDSI que cumple con I-CTR3 (Medidas de puente) según la directiva europea 91/263/EEC (directiva TTE).

Aviso: Éste es un producto de Clase A. En un entorno doméstico, este producto puede ocasionar interferencias de radio, en cuyo caso puede que se solicite al usuario que tome las medidas pertinentes.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 30. August 1995 (bzw. der EMC EG Richlinie 89/336)

Dieses Gerät ist berechtigt in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraph 5 des EMVG ist die IBM Deutschland Informationssysteme GmbH, 70548 Stuttgart.

Informationen in Hinsicht EMVG Paragraph 3 Abs. (2) 2:

Das Gerät erfüllt die Schutzanforderungen nach EN 50082-1 und EN 55022 Klasse A.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: “Warnung: dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im

Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen."

EN 50082-1 Hinweis: "Wird dieses Gerät in einer industriellen Umgebung betrieben (wie in EN 50082-2 festgelegt), dann kann es dabei eventuell gestört werden. In solch einem Fall ist der Abstand bzw. die Abschirmung zu der industriellen Störquelle zu vergrößern."

Anmerkung: Um die Einhaltung des EMVG sicherzustellen sind die Geräte, wie in den IBM Handbüchern angegeben, zu installieren und zu betreiben.

Marcas registradas

Los términos siguientes son marcas registradas de IBM Corporation en EE.UU. y/o en otros países:

AIX	Microsoft	Parallel Sysplex
eNetwork	Nways	Presentation Manager
ESCON	NetView	VM/ESA
IBM	OS/2	

Tivoli es una marca registrada de Tivoli Systems Inc. en EE.UU. y/o en otros países.

Java y todas las marcas registradas y logotipos basados en Java son marcas registradas de Sun Microsystems, Inc. en EE.UU. y/o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en EE.UU. y/o en otros países.

Otros nombres de compañías, productos y servicios pueden ser marcas registradas o marcas de servicio de otras compañías.

Apéndice B. Información de seguridad

Danger: Before you begin to install this product, read the safety information in *Caution: Safety Information—Read This First*, SD21-0030. This booklet describes safe procedures for cabling and plugging in electrical equipment.

Gevaar: Voordat u begint met de installatie van dit produkt, moet u eerst de veiligheidsinstructies lezen in de brochure *PAS OP! Veiligheidsinstructies—Lees dit eerst,* SD21-0030. Hierin wordt beschreven hoe u electrische apparatuur op een veilige manier moet bekabelen en aansluiten.

Danger: Avant de procéder à l'installation de ce produit, lisez d'abord les consignes de sécurité dans la brochure *ATTENTION: Consignes de sécurité—A lire au préalable,* SD21-0030. Cette brochure décrit les procédures pour câbler et connecter les appareils électriques en toute sécurité.

Perigo: Antes de começar a instalar este produto, leia as informações de segurança contidas em *Cuidado: Informações Sobre Segurança—Leia Isto Primeiro,* SD21-0030. Esse folheto descreve procedimentos de segurança para a instalação de cabos e conexões em equipamentos elétricos.

危險：安裝本產品之前， 請先閱讀 "Caution: Safety Information--Read This First" SD21-0030 手冊中所提供的安全注意事項。 這本手冊將會說明使用電器設備的纜線及電源的安全程序。

Opasnost: Prije nego sto počnete sa instalacijom produkta, pročitajte naputak o pravilima o sigurnom rukovanju u Upozorenje: Pravila o sigurnom rukovanju - Prvo pročitaj ovo, SD21-0030. Ovaj privitak opisuje sigurnosne postupke za priključrivanje kabela i priključivanje na električno napajanje.

Upozornění: než zahájíte instalaci tohoto produktu, přečtěte si nejprve bezpečnostní informace v pokynech „Bezpečnostní informace“ č. 21-0030. Tato brožurka popisuje bezpečnostní opatření pro kabeláž a zapojení elektrického zařízení.

Fare! Før du installerer dette produkt, skal du læse sikkerhedsforskrifterne i *NB: Sikkerhedsforskrifter—Læs dette først* SD21-0030. Vejledningen beskriver den fremgangsmåde, du skal bruge ved tilslutning af kabler og udstyr.

Gevaar Voordat u begint met het installeren van dit produkt, dient u eerst de veiligheidsrichtlijnen te lezen die zijn vermeld in de publikatie *Caution: Safety Information - Read This First* , SD21-0030. In dit boekje vindt u veilige procedures voor het aansluiten van elektrische appratuur.

VAARA: Ennen kuin aloitat tämän tuotteen asennuksen, lue julkaisussa *Varoitus: Turvaohjeet—Lue tämä ensin* , SD21-0030, olevat turvaohjeet. Tässä kirjasessa on ohjeet siitä, miten sähkölaitteet kaapeloidaan ja kytketään turvallisesti.

Danger : Avant d'installer le présent produit, consultez le livret *Attention : Informations pour la sécurité — Lisez-moi d'abord* SD21-0030, qui décrit les procédures à respecter pour effectuer les opérations de câblage et brancher les équipements électriques en toute sécurité.

Vorsicht: Bevor mit der Installation des Produktes begonnen wird, die Sicherheitshinweise in *Achtung: Sicherheitsinformationen—Bitte zuerst lesen,* IBM Form SD21-0030. Diese Veröffentlichung beschreibt die Sicherheitsvorkehrungen für das Verkabeln und Anschließen elektrischer Geräte.

Vigyázat: Mielôtt megkezdi a berendezés üzembe helyezését, olvassa el a *Caution: Safety Information— Read This First,* SD21-0030 könyvecskében leírt biztonsági információkat. Ez a könyv leírja, milyen biztonsági intézkedéseket kell megtenni az elektromos berendezés huzalozásakor illetve csatlakoztatásakor.

Pericolo: prima di iniziare l'installazione di questo prodotto, leggere le informazioni relative alla sicurezza riportate nell'opuscolo *Attenzione: Informazioni di sicurezza — Prime informazioni da leggere* in cui sono descritte le procedure per il cablaggio ed il collegamento di apparecchiature elettriche.

危険： 導入作業を開始する前に、安全に関する
小冊子SD21-0030 の「最初にお読みください」
(Read This First)の項をお読みください。
この小冊子は、電気機器の安全な配線と接続の
手順について説明しています。

위험: 이 제품을 설치하기 전에 반드시
"주의: 안전 정보-시작하기 전에"
(SD21-0030) 에 있는 안전 정보를
읽으십시오.

Fare: Før du begynner å installere dette produktet, må du lese sikkerhetsinformasjonen i *Advarsel: Sikkerhetsinformasjon — Les dette først* , SD21-0030 som beskriver sikkerhetsrutinene for kabling og tilkobling av elektrisk utstyr.

Uwaga:
Przed rozpoczęciem instalacji produktu należy zapoznać się z instrukcją:
"Caution: Safety Information - Read This First", SD21-0030.
Zawiera ona warunki bezpieczeństwa przy podłączaniu do sieci elektrycznej
i eksploatacji.

Perigo: Antes de iniciar a instalação deste produto, leia as informações de segurança *Cuidado: Informações de Segurança — Leia Primeiro* , SD21-0030. Este documento descreve como efectuar, de um modo seguro, as ligações eléctricas dos equipamentos.

ОСТОРОЖНО: Прежде чем инсталлировать этот продукт, прочтите Инструкцию по технике безопасности в документе "Внимание: Инструкция по технике безопасности -- Прочесть в первую очередь", SD21-0030. В этой брошюре описаны безопасные способы каблирования и подключения электрического оборудования.

Nebezpečenstvo: Pred inštaláciou výrobku si prečítajte
bezpečnosté predpisy v
Výstraha: Bezpeč osté predpisy - Prečítaj ako prvé,
SD21 0030. V tejto brožúrke sú opísané bezpečnosté
postupy pre pripojenie elektrických zariadení.

Pozor: Preden zaènete z instalacijo tega produkta preberite poglavje: 'Opozorilo: Informacije o varnem rokovanju-preberi pred uporabo," SD21-0030. To poglavje opisuje pravilne postopke za kabliranje,

 **Peligro:** Antes de empezar a instalar este producto, lea la información de seguridad en *Atención: Información de Seguridad — Lea Esto Primero,* SD21-0030. Este documento describe los procedimientos de seguridad para cablear y enchufar equipos eléctricos.

 **Varning — livsfara:** Innan du börjar installera den här produkten bör du läsa säkerhetsinformationen i dokumentet *Varning: Säkerhetsföreskrifter— Läs detta först,* SD21-0030. Där beskrivs hur du på ett säkert sätt ansluter elektrisk utrustning.

危險：

開始安裝此產品之前，請先閱讀安全資訊。

注意：

請先閱讀 - 安全資訊 SD21-0030

此冊子說明插接電器設備之電纜線的安全程序。

Índice

Caracteres Especiales

Números

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

Hoja de Comentarios

Network Utility
Instalación,
iniciación
y guía del usuario

Número de Publicación GA10-5247-00

Por favor, sírvase facilitarnos su opinión sobre esta publicación, tanto a nivel general (organización, contenido, utilidad, facilidad de lectura,...) como a nivel específico (errores u omisiones concretos). Tenga en cuenta que los comentarios que nos envíe deben estar relacionados exclusivamente con la información contenida en este manual y a la forma de presentación de ésta.

Para realizar consultas técnicas o solicitar información acerca de productos y precios, por favor diríjase a su sucursal de IBM, business partner de IBM o concesionario autorizado.

Para preguntas de tipo general, llame a ″IBM Responde″ (número de teléfono 901 300 000).

Al enviar comentarios a IBM, se garantiza a IBM el derecho no exclusivo de utilizar o distribuir dichos comentarios en la forma que considere apropiada sin incurrir por ello en ninguna obligación con el remitente.

Comentarios:

Gracias por su colaboración.

Para enviar sus comentarios:
- Envíelos por correo a la dirección indicada en el reverso.
- Envíelos por fax al número siguiente:

Si desea obtener respuesta de IBM, rellene la información siguiente:

Nombre	Dirección
Compañía	
Número de teléfono	Dirección de e-mail

Hoja de Comentarios
GA10-5247-00

IBM, S.A.
National Language Solutions Center
Av. Diagonal, 571 ″Ed. L'Illa″
08029 Barcelona, España

Número Pieza: 31L3207

Printed in the United States of America

31L3207

GA10-5247-00