Tecnología de marcación manual: Descripciones y explicaciones

Contenido

Introducción

Este capítulo presenta y explica algunas de las tecnologías utilizadas en las redes de marcación manual. Encontrará consejos de configuración e interpretaciones de algunos de los comandos **show**, que son útiles para verificar el correcto funcionamiento de la red. Los procedimientos de resolución de problemas están fuera del alcance de este documento y se pueden encontrar en el documento titulado *Resolución de problemas de marcado*.

Antes de comenzar

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Prerequisites

No hay requisitos previos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Operaciones del módem

Esta sección explica los problemas relacionados específicamente con la configuración, verificación y uso de módems con routers Cisco.

Uso del comando Modem Autoconfigure

Si utiliza Cisco Internetwork Operating System (Cisco IOS) versión 11.1 o posterior, puede configurar el router Cisco para que se comunique con el módem y lo configure automáticamente.

Utilice el siguiente procedimiento para configurar un router Cisco para intentar automáticamente descubrir qué tipo de módem está conectado a la línea y, a continuación, configurar el módem:

1. Para descubrir el tipo de módem conectado al router, utilice el comando de configuración de línea **modem autoconfigure discovery**.
2. Cuando el módem se descubre correctamente, configure automáticamente el módem mediante el comando de configuración de línea **modem autoconfigure type** ***modem-name***.

Si desea mostrar la lista de módems para los que el router tiene entradas, utilice el *nombre de módem* ***show modemcap***. Si desea cambiar un valor de módem que se devolvió desde el comando **show modemcap**, utilice el comando de configuración de línea **modemcap edit** ***modem-name attribute value*** .

Para obtener información completa sobre el uso de estos comandos, refiérase a la *Guía de Configuración de Soluciones de Marcado de Documentación de Cisco IOS y Referencia de Comandos de Soluciones de Marcado*.

Nota: No introduzca **&W** en la entrada modemcap que se utiliza para la configuración automática. Esto hace que la NVRAM se reescriba cada vez que se realiza una configuración automática del módem y destruirá el módem.

Establecimiento de una sesión Telnet inversa a un módem

Para fines de diagnóstico, o para configurar inicialmente el módem si está ejecutando Cisco IOS Release 11.0 o anterior, debe establecer una sesión Telnet inversa para configurar un módem para comunicarse con un dispositivo Cisco. Siempre y cuando se bloquee la velocidad del módem lateral del equipo de terminal de datos (DTE), el módem se comunicará siempre con el servidor de acceso o el router a la velocidad deseada. Consulte la Tabla 16-5 para obtener información sobre el bloqueo de la velocidad del módem. Asegúrese de que la velocidad del dispositivo Cisco esté configurada antes de ejecutar comandos al módem a través de una sesión Telnet inversa. Una vez más, consulte la tabla 16-5 para obtener información sobre la configuración de la velocidad del servidor de acceso o del router.

Para configurar el módem para una sesión Telnet inversa, utilice el comando de configuración de línea **transport input telnet**. Para configurar un grupo rotatorio (en este caso, en el puerto 1), ingrese el comando de configuración de línea **rotary 1**. Si se colocan estos comandos bajo la configuración de línea, el IOS asigna receptores IP para conexiones entrantes en intervalos de puertos comenzando por los siguientes números base:

2000	protocolo Telnet
3000	Protocolo Telnet con protocolo rotativo
4000	protocolo TCP sin procesar
5000	Protocolo TCP sin formato con protocolo rotativo
6000	protocolo Telnet, modo binario
7000	protocolo Telnet, modo binario con rotatorio
9000	protocolo Xremote
10000	Protocolo XRemote con rotatorio

Para iniciar una sesión Telnet inversa al módem, realice los siguientes pasos:

1. Desde su terminal, utilice el comando **telnet ip-address 20yy** donde *ip-address* es la dirección IP de cualquier interfaz conectada activa en el dispositivo Cisco, e yy es el número de línea al que está conectado el módem.Por ejemplo, el siguiente comando lo conectaría al puerto auxiliar en un router Cisco 2501 con la dirección IP 192.169.53.52: **telnet 192.169.53.52 2001**. Generalmente, un comando Telnet de este tipo puede ejecutarse desde cualquier lugar de la red, si puede **hacer ping** a la dirección IP en cuestión.**Nota:** En la mayoría de los routers Cisco, el puerto 01 es el puerto auxiliar. En un servidor de acceso de Cisco, el puerto auxiliar es el último TTY +1. A modo de ejemplo, el puerto auxiliar en un 2511 es el puerto 17 (16 puertos TTY + 1). Utilice siempre el comando **show line** exec para encontrar el número de puerto auxiliar, particularmente en las series 2600 y 3600, que utilizan números de puerto no contiguos para acomodar tamaños de módulo asíncronos variables.
2. Si se rechaza la conexión, podría indicar que no hay receptor en la dirección y el puerto especificados o que alguien ya está conectado a ese puerto. Verifique la dirección de conexión y el número de puerto. Además, asegúrese de que el comando **modem inout** o **modem DTR-active**, así como **transport input all**, aparezcan en la configuración de línea para las líneas a las que se llega.Si utiliza la función rotatoria, asegúrese de que el comando *rotary n* también aparezca en la configuración de línea donde n es el número del grupo rotatorio. Para verificar si alguien ya está conectado, telnet al router y use el comando **show line *n*** . Busque un asterisco para indicar que la línea está en uso. Asegúrese de que el CTS es alto y que el DSR no lo es. Utilice el comando **clear line *n*** para desconectar la sesión

actual en el número de puerto n. Si la conexión sigue rechazada, el módem puede estar afirmando el Detección de portadora (CD) todo el tiempo. Desconecte el módem de la línea, establezca una sesión Telnet inversa y, a continuación, conecte el módem.

3. Después de realizar correctamente la conexión Telnet, ingrese AT y asegúrese de que el módem responda con OK.
4. Si el módem no responde, consulte la siguiente tabla.

La tabla 16-1 a continuación describe las posibles causas de los síntomas de los problemas de conectividad de módem a router y describe las soluciones a esos problemas.

Tabla 16-1: No hay conectividad entre módem y router

Posibles Causas	Acciones sugeridas

El control del módem no está activado en el servidor de acceso o en el router	1. Utilice el comando **show line** exec en el servidor de acceso o el router. La salida para el puerto auxiliar debe mostrar **InOut** o **RlisCD** en la columna Módem. Esto indica que el control del módem está habilitado en la línea del servidor de acceso o del router. Para obtener una explicación de la salida **show line**, refiérase a "Uso de Comandos Debug" en el capítulo 15.
	2. Configure la línea para el control del módem mediante el comando de configuración de línea **modem inout**. El control del módem está ahora habilitado en el servidor de acceso.
	Ejemplo: El siguiente ejemplo ilustra cómo configurar una línea para las llamadas entrantes y salientes:
	`line 5`
	`modem inout`
	Nota: Asegúrese de utilizar el comando **modem inout**, y no el comando **modem dialin** mientras la conectividad del módem está en cuestión. Este último comando permite a la línea aceptar sólo llamadas entrantes. Las llamadas salientes serán rechazadas y será imposible establecer una sesión Telnet con el módem para configurarlo. Si desea utilizar el comando **modem dialin**, hágalo sólo después de estar seguro de que el módem funciona correctamente.

El módem puede estar	Ingrese **AT&FE1Q0** para devolverlo a los valores predeterminados de fábrica y asegúrese de que el módem esté configurado en caracteres de eco y de que devuelva la salida. Es posible que el módem tenga una sesión

mal configurado o tener una sesión bloqueada.	bloqueada. Utilice "^**U**" para borrar la línea y "^**Q**" para abrir el control de flujo (XON). Verifique la configuración de paridad.
Cableado incorrecto	1. Verifique el cableado entre el módem y el servidor de acceso o router. Confirme que el módem está conectado al puerto auxiliar del servidor de acceso o router con un cable RJ-45 enrollado y un adaptador MMOD DB-25. Cisco recomienda y admite esta configuración de cableado para puertos RJ-45. (Estos conectores se suelen denominar "Módem"). 2. Utilice el comando **show line** exec para verificar que el cableado es correcto. Vea la explicación del resultado del comando **show line** en la sección titulada "Uso de comandos de depuración" en el capítulo 15.
Problema de hardware	1. Compruebe que está utilizando el cableado correcto y que todas las conexiones son correctas. 2. Compruebe la existencia de daños en todo el hardware, incluidos el cableado (cables rotos), los adaptadores (pines sueltos), los puertos del servidor de acceso y el módem. 3. Consulte el capítulo 3, "Resolución de problemas de hardware y arranque", para obtener más información sobre la resolución de problemas de hardware.

Uso de grupos rotativos

Para algunas aplicaciones, los módems de un router determinado deben ser compartidos por un grupo de usuarios. Cisco Dialout Utility es un ejemplo de este tipo de aplicación. Básicamente, los usuarios se conectan a un puerto que los conecta a un módem disponible. Para agregar una línea asíncrona a un grupo rotatorio, simplemente ingrese **rotary *n*** donde *n* es el número del grupo rotativo en la configuración para la línea asíncrona. Consulte el ejemplo a continuación.

```
line 1 16
 modem InOut
 transport input all
 rotary 1
 speed 115200
 flowcontrol hardware
```

La configuración de línea anterior permitiría a los usuarios conectarse al grupo rotatorio ingresando **telnet 192.169.53.52 3001** para telnet normal. Entre las alternativas se incluyen los puertos 5001 para Raw TCP, 7001 para binario telnet (que Cisco Dialout Utility utiliza) y 10001 para conexiones Xremote.

Nota: Para verificar la configuración de Cisco Dialout Utility, haga doble clic en el icono de la utilidad de marcado de salida en la parte inferior derecha de la pantalla y presione el botón Más>. A continuación, pulse el botón Configurar puertos>. Asegúrese de que el puerto esté en el rango 7000, si utiliza grupos rotativos, y en el rango 6000, si la utilidad de marcado está dirigida a un módem individual. También debe habilitar el registro del módem en el PC. Para ello, seleccione la secuencia siguiente: **Inicio->Panel de control-> módems->(elija su módem Cisco Dialout)->Propiedades->Conexión ->Avanzadas...->Grabar un archivo de registro**.

Interpretación del resultado de show line

El resultado del comando **show line** *line-number* exec es útil para solucionar problemas de conexión de módem a servidor de acceso o router. A continuación se muestra el resultado del comando **show line**.

```
as5200-1#show line 1
   Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
   1 TTY 115200/115200-    -      -    -    -      0       0     0/0       -

Line 1, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits
Status: No Exit Banner
Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
Modem state: Hanging up
  modem(slot/port)=1/0, state=IDLE
  dsx1(slot/unit/channel)=NONE, status=VDEV_STATUS_UNLOCKED
Group codes:    0
Modem hardware state: CTS noDSR  noDTR RTS
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
                ^^x    none   -     -       none
Timeouts:      Idle EXEC    Idle Session   Modem Answer  Session   Dispatch
               00:10:00        never                       none     not set
                            Idle Session Disconnect Warning
                              never
                            Login-sequence User Response
                             00:00:30
                            Autoselect Initial Wait
                              not set
Modem type is unknown.
Session limit is not set.
Time since activation: never
Editing is enabled.
History is enabled, history size is 10.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed transports are lat pad telnet rlogin udptn v120 lapb-ta.
Preferred is l
at pad telnet rlogin udptn v120 lapb-ta.
No output characters are padded
No special data dispatching characters
as5200-1#
```

Cuando se producen problemas de conectividad, aparece un resultado importante en los campos de estado del módem y del hardware del módem.

Nota: El campo de estado del hardware del módem no aparece en el resultado **show line** para cada plataforma. En algunos casos, las indicaciones para los estados de señal se mostrarán en el campo de estado del módem.

La tabla 16-2 muestra las cadenas de estado de estado de módem y de hardware de módem típicas de la salida del comando **show line**. También explica el significado de cada estado.

Tabla 16-2: Estados de Hardware del Módem y del Módem en Salida de Línea Show

Estado del módem	Estado del hardware del módem	Significado
Inactivo	CTS noDSR DTR RTS	Estos son los estados de módem adecuados para las conexiones entre un servidor de acceso o un router y un módem (cuando no hay ninguna llamada entrante). La salida de cualquier otro tipo indica generalmente un problema.
Listo	-	Si el estado del módem es Ready, en lugar de Idle, considere lo siguiente: 1. El control del módem no está configurado en el servidor de acceso o en el router. Configure el servidor de acceso o el router con el comando de configuración de línea **modem inout**. 2. Existe una sesión en la línea. Utilice el comando **show users** exec y utilice el comando **clear line** privileged exec para detener la sesión si lo desea. 3. La DSR es alta. Hay dos posibles razones para ello: Problemas de Cableado. Si el conector utiliza DB-25 pin 6 y no tiene pin 8, debe mover el pin de 6 a 8 o obtener el conector adecuado.El módem configurado para DCD siempre es alto. El módem se debe reconfigurar para que tenga DCD de alta solamente un CD(1). Esto suele hacerse con el comando modem **&C1**, pero verifique la documentación del módem

		para ver la sintaxis exacta para su módem. Si su software no soporta el control del módem, debe configurar la línea de servidor de acceso a la cual el módem está conectado con el comando de configuración de línea **no exec**. Borre la línea con el comando exec **clear line** privileged, inicie una sesión Telnet inversa con el módem y vuelva a configurar el módem para que DCD sólo esté alto en el CD. Para finalizar la sesión Telnet, introduzca **disconnect** y vuelva a configurar la línea del servidor de acceso con el comando de configuración de línea exec.
Listo	noCTS noDSR DTR RTS (2)	La cadena noCTS aparece en el campo de estado de hardware del módem por una de las cuatro razones siguientes: 1. El módem está apagado. 2. El módem no está conectado correctamente al servidor de acceso. Verifique las conexiones de cableado del módem al servidor de acceso. 3. Cableado incorrecto (MDCE enrollado o MDTE recto, pero sin los pines movidos). La configuración de cableado recomendada se indica anteriormente en esta tabla. 4. El módem no está configurado para el control de flujo de hardware. Utilice el comando de configuración de línea **no flowcontrol hardware** para inhabilitar el control de flujo de hardware en el servidor de acceso. A continuación, active el control de flujo de hardware en el módem mediante una sesión Telnet inversa. (Consulte la documentación del módem y consulte la sección "Establecimiento de una sesión Telnet inversa a un módem" que aparece anteriormente en este capítulo). Vuelva a habilitar el control de flujo de hardware en el servidor de acceso con el comando de configuración de línea **flowcontrol hardware**.
Listo	CTS DS	La cadena DSR (en lugar de la cadena noDSR) aparece en el campo Estado del

	R DT R RTS (2)	hardware del módem por uno de los siguientes motivos: 1. Cableado incorrecto (MDCE enrollado o MDTE recto, pero sin los pines movidos). La configuración de cableado recomendada se indica anteriormente en esta tabla. 2. El módem está configurado para DCD siempre alto. Vuelva a configurar el módem de modo que el DCD sólo esté alto en el CD. Esto suele hacerse con el comando modem **&C1**, pero verifique la documentación del módem para ver la sintaxis exacta para su módem. Configure la línea de servidor de acceso a la que el módem está conectado con el comando de configuración de línea **no exec**. Borre la línea con el comando exec **clear line** privileged, inicie una sesión Telnet inversa con el módem y vuelva a configurar el módem para que DCD sólo esté alto en el CD. Para finalizar la sesión Telnet, introduzca **disconnect**. Vuelva a configurar la línea del servidor de acceso con el comando de configuración de línea exec.
List o	CTS * DS R* DT R RTS (2)	Si esta cadena aparece en el campo Estado del hardware del módem, es probable que el control del módem no esté habilitado en el servidor de acceso. Utilice el comando de configuración de línea **modem inout** para habilitar el control del módem en la línea. Anteriormente, en esta tabla se proporciona información adicional sobre la configuración del control del módem en un servidor de acceso o una línea de router.

(1) CD = Detección de portadora

(2) Un * junto a una señal indica una de dos cosas: La señal ha cambiado en los últimos segundos o el método de control del módem seleccionado no está utilizando la señal.

Recolección de información de rendimiento del módem

Esta sección explica los métodos para recopilar datos de rendimiento en los módems digitales MICA que se encuentran en la familia de servidores de acceso Cisco AS5x00. Los datos de rendimiento se pueden utilizar para el análisis de tendencias y son útiles para solucionar los problemas de rendimiento que puedan surgir. Al observar las cifras que se presentan a continuación, tenga en cuenta que la perfección no es posible en el mundo real. La posible

velocidad de éxito de llamadas del módem (CSR) depende de la calidad de los circuitos, la base de usuarios del módem cliente y el conjunto de modulaciones que se utilizan. Un porcentaje de CSR típico para llamadas V.34 es del 95%. Se puede esperar que las llamadas V.90 se conecten correctamente el 92% del tiempo. Es probable que las caídas prematuras ocurran el 10% del tiempo.

Utilice los siguientes comandos para obtener una vista general del comportamiento del módem en el servidor de acceso:

- **show modem**
- **show modem summary**
- **show modem connect-speed**
- **show modem call-stats**

La siguiente información es útil para solucionar problemas de una conexión de módem individual o recopilar datos para el análisis de tendencias:

- debug modem csm
- modem call-record terse
- show modem op (MICA) / AT@E1 (Microcom) mientras estaba conectado
- show modem log para la sesión de interés después de la desconexión
- ANI (número de la persona que llama)
- Hora del día
- Revisión de firmware/hardware del módem del cliente
- Información interesante del cliente (después de la desconexión)-ATI6, ATI11, AT&V, AT&V1, etc.
- Un registro de audio (.wav file) del intento de preparación del módem cliente

En las secciones siguientes, los comandos se explicarán con más detalle y se discutirán algunas tendencias comunes.

Show Modem / Show Modem Summary

El comando **show modem** proporciona una vista de módems individuales. A partir de estos números se puede ver el estado de los módems individuales.

```
router# show modem
  Codes:
  * - Modem has an active call
  C - Call in setup
  T - Back-to-Back test in progress
  R - Modem is being Reset
  p - Download request is pending and modem cannot be used for taking calls
  D - Download in progress
  B - Modem is marked bad and cannot be used for taking calls
  b - Modem is either busied out or shut-down
  d - DSP software download is required for achieving K56flex connections
  ! - Upgrade request is pending
                Inc calls     Out calls     Busied   Failed  No       Succ
  Mdm  Usage    Succ   Fail   Succ   Fail   Out      Dial    Answer   Pct.
* 1/0    17%      74      3      0      0       0        0       0     96%
* 1/1    15%      80      4      0      0       0        1       1     95%
* 1/2    15%      82      0      0      0       0        0       0    100%
  1/3    21%      62      1      0      0       0        0       0     98%
  1/4    21%      49      5      0      0       0        0       0     90%
```

```
* 1/5    18%      65      3      0      0       0        0       0     95%
```

Para ver los números agregados para todos los módems en el router, utilice el comando **show modem summary**.

```
router#show modem summary
         Incoming calls       Outgoing calls      Busied   Failed   No    Succ
Usage  Succ    Fail  Avail   Succ    Fail  Avail    Out      Dial     Ans   Pct.
   0%  6297     185     64      0       0      0        0        0      0     97%
```

Tabla 16-3: show modem Fields

Campos	Descripciones
Llamadas entrantes y salientes	Llamadas que entran y salen del módem. • Uso: porcentaje del tiempo de actividad total del sistema que todos los módems están en uso. • Correcto: total de llamadas conectadas correctamente. • Fallo: total de llamadas que no se han conectado correctamente. • Disponible: total de módems disponibles para su uso en el sistema.
Expulsado	Número total de veces que los módems fueron retirados del servicio con el comando **modem busy** o el comando **modem shutdown**.
Marcación fallida	Número total de intentos que los módems no han colgado o no hay tono de marcado.
No Ans	Número total de veces que se ha detectado el timbre de llamada, pero el módem no ha contestado las llamadas.
Correcto Pct.	Porcentaje de conexión exitoso de los módems disponibles totales.

[Salida de Show Modem Call-Stats]

```
compress  retrain lostCarr  rmtLink  trainup hostDrop wdogTimr inacTout
  Mdm     #   %    #   %    #   %    #   %    #   %    #   %    #   %    #   %
 Total    9       41      271     3277        7     2114        0        0
```

Tabla 16-4: show modem call-stats Fields

rmt Link	Esto muestra que la corrección de errores estaba en vigor y la llamada fue colgada por el sistema cliente conectado al módem remoto.
hos	Muestra que el sistema host IOS colgó la llamada.

tDrop	Algunas de las razones comunes son: tiempo de espera inactivo, un circuito despejado de la compañía telefónica o una petición LCP PPP del cliente. La mejor manera de determinar el motivo del bloqueo es mediante el uso del comando modem call-record terse o la contabilidad AAA.

Las otras razones de desconexión deberían sumar menos del 10% del total.

Salida Show Modem Connect-Speeds

```
router>show modem connect 33600 0
 Mdm   26400  28000  28800  29333  30667  31200  32000  33333  33600 TotCnt
Tot      614      0   1053      0      0   1682      0      0    822   6304

router>show modem connect 56000 0
 Mdm   48000  49333  50000  50666  52000  53333  54000  54666  56000 TotCnt
Tot      178    308     68     97     86     16      0      0      0   6304
```

Se espera ver una distribución de velocidades V.34. Debe haber un pico a 26.4, si los T1s utilizan la señalización asociada al canal (CAS). Para los T1s ISDN (PRI), el pico debe estar en 31.2. Además, busque algunas velocidades K56Flex, V.90. Si no hay conexiones V.90, puede haber un problema de topología de red.

Introducción al comando Modem Call-Record Terse (11.3AA/12.0T)

En lugar de un comando exec, éste es un comando de configuración ubicado en el nivel del sistema del servidor de acceso en cuestión. Cuando un usuario se desconecta, se muestra un mensaje similar al siguiente:

```
*May 31 18:11:09.558: %CALLRECORD-3-MICA_TERSE_CALL_REC: DS0 slot/contr/chan=2/0/18,
slot/port=1/29, call_id=378, userid=cisco, ip=0.0.0.0, calling=5205554099,
called=4085553932, std=V.90, prot=LAP-M, comp=V.42bis both,
init-rx/tx b-rate=26400/41333, finl-rx/tx brate=28800/41333, rbs=0, d-pad=6.0 dB,
retr=1, sq=4, snr=29, rx/tx chars=93501/94046, bad=5, rx/tx ec=1612/732, bad=0,
time=337, finl-state=Steady, disc(radius)=Lost Carrier/Lost Carrier,
disc(modem)=A220 Rx (line to host) data flushing - not OK/EC condition - locally
detected/received
DISC frame -- normal LAPM termination
```

Comando Show Modem Operational-Status

El comando exec **show modem operational-status** muestra los parámetros actuales (o más recientes) que pertenecen a la conexión del módem.

La entrada de documentación para este comando se encuentra en la *Referencia de Comandos de Soluciones de Marcado de Cisco IOS Release 12.0*. **show modem operational-status** es sólo para módems MICA. El comando equivalente para los módems Microcom es **modem at-mode / AT@E1**. Utilice el comando **modem at-mode <slot>/<port>** para conectarse al módem y luego ejecute el comando **AT@E1**. La documentación completa del comando **modem at-mode** se puede encontrar en la *Guía de Configuración del Software Cisco AS5300*, y la documentación para el

comando **AT@E1** está en la *Referencia de Comandos de AT Command Set y Register Summary for Microcom Modem Modules*.

Utilice los pasos siguientes para determinar qué módems está entrando un usuario:

1. Ejecute el comando **show user** y busque el TTY al que están conectados.
2. Utilice el comando **show line** y busque los números de puerto/ranura del módem.

Recopilación de datos de rendimiento del lado del cliente

Para el análisis de tendencias, es muy importante recopilar datos de rendimiento del cliente. Intente siempre obtener la siguiente información:

- versión de firmware/modelo de hardware del cliente (alcanzable con el comando **ATI3I7** en el módem del cliente)
- razones de desconexión notificadas por el cliente (use **ATI6** o **AT&V1**)

Otra información disponible en el extremo del cliente incluye el modemlog.txt y ppplog.txt del equipo. Debe configurar específicamente el PC para generar estos archivos.

Análisis de los datos de rendimiento

Una vez que haya recopilado y comprendido los datos de rendimiento del sistema del módem, deberá examinar los patrones y componentes restantes que puedan necesitar mejoras.

Problemas con módems de servidor específicos

Utilice **show modem** o **show modem call-stats** para identificar cualquier módem con tasas anormalmente altas de fallas de preparación o tasas de desconexión incorrectas (MICA). Si los pares adyacentes de módems están teniendo problemas, el problema es probablemente un DSP colgado/muerto. Utilice **copy flash modem** al HMM afectado para recuperarse. Asegúrese de que los módems están ejecutando la última versión de portware. Para verificar que todos los módems estén correctamente configurados, utilice el comando de configuración **modem autoconfigure type mica/microcom_server** en la configuración de línea. Para asegurarse de que los módems se configuran automáticamente cada vez que se cuelga una llamada, utilice el comando exec **debug confmodem**. Para corregir módems mal configurados, es posible que necesite establecer una sesión Telnet inversa.

Problemas con DS0 particulares

Los problemas de DS0 son raros, pero posibles. Para localizar DS0 que funcionan mal, utilice el comando **show controller t1 call-counters** y busque DS0 con TotalCalls anormalmente altas y TotalDuration anormalmente baja. Para dirigirse a los DS0 sospechosos, es posible que tenga que ocupar otros DS0 con el comando de configuración **isdn service dsl, ds0 busyout** en la interfaz serial para T1. El resultado de **show controller t1 call-counters** es similar al siguiente:

```
TimeSlot    Type    TotalCalls    TotalDuration
    1        pri          873        1w6d
    2        pri          753        2w2d
    3        pri          4444       00:05:22
```

Obviamente, el intervalo de tiempo 3 es el canal sospechoso en este caso.

Tendencias comunes adicionales

A continuación se muestran algunas de las tendencias más comunes observadas por el TAC de Cisco.

1. Rutas de circuito defectuosasEs posible que esté recibiendo trayectos de circuito defectuosos a través de la red telefónica pública conmutada (PSTN) si tiene los siguientes problemas:las llamadas de larga distancia tienen problemas, pero las llamadas locales no (o viceversa)las llamadas a determinadas horas del día tienen problemaslas llamadas de intercambios remotos específicos tienen problemas
2. Problemas con las llamadas de larga distanciaSi su servicio de larga distancia no funciona correctamente o en absoluto (pero el servicio local está bien):Asegúrese de que la línea digital se conecte a un switch digital, no a un banco de canal .Indique a las compañías telefónicas que examinen las rutas de circuito utilizadas para la larga distancia.
3. Problemas con las llamadas de áreas de llamada específicas.Si las llamadas de regiones geográficas o intercambios específicos tienden a tener problemas, debe obtener la topología de red de la compañía telefónica.Si se requieren varias conversiones analógicas a digitales, las conexiones del módem V.90/K56flex no serán posibles y V.34 puede degradarse un poco. Las conversiones analógicas a digitales se requieren en áreas que se sirven mediante switches digitales no integrados o switches analógicos.

Operaciones ISDN

ISDN hace referencia a un conjunto de servicios digitales disponibles para los usuarios finales. ISDN implica la digitalización de la red telefónica de modo que se pueda proporcionar voz, datos, texto, gráficos, música, vídeo y otro material de origen a los usuarios finales desde un único terminal de usuario final a través de un cableado telefónico existente. Los partidarios de ISDN imaginan una red mundial similar a la actual red telefónica, pero con transmisión digital y una variedad de nuevos servicios.

ISDN es un esfuerzo para estandarizar los servicios de suscriptores, las interfaces de usuario/red y las capacidades de red e interconexión. La estandarización de los servicios de suscriptores intenta garantizar un nivel de compatibilidad internacional. La estandarización de la interfaz de usuario/red estimula el desarrollo y el marketing de estas interfaces por parte de fabricantes de terceros. La estandarización de las capacidades de red e interconexión ayuda a alcanzar el objetivo de la conectividad mundial al garantizar que las redes ISDN se comuniquen fácilmente entre sí.

Las aplicaciones ISDN incluyen aplicaciones de imagen de alta velocidad (como facsímil de grupo IV), líneas telefónicas adicionales en los hogares para el sector del teletrabajo, transferencia de archivos de alta velocidad y videoconferencia. La voz, por supuesto, también es una aplicación popular para ISDN.

El mercado de acceso doméstico se está dividiendo entre diferentes tecnologías. En las zonas en las que están disponibles tecnologías más económicas como DSL y Cable, el mercado doméstico se está alejando de la RDSI. Sin embargo, las empresas siguen utilizando ISDN en forma de PRI T1/E1s para transportar grandes cantidades de datos o para proporcionar acceso de marcado v.90.

Componentes ISDN

Los componentes ISDN incluyen terminales, adaptadores de terminal (TA), dispositivos de terminación de red, equipos de terminación de línea y equipos de terminación de intercambio. Los terminales ISDN vienen en dos tipos. Los terminales ISDN especializados se denominan equipos terminales tipo 1 (TE1). Los terminales no ISDN, como DTE que son anteriores a los estándares ISDN, se denominan equipos terminales tipo 2 (TE2). Los TE1 se conectan a la red ISDN a través de un link digital de cuatro cables y par trenzado. Los TE2 se conectan a la red ISDN a través de un adaptador de terminal. El ISDN TA puede ser un dispositivo independiente o una placa dentro del TE2. Si el TE2 se implementa como un dispositivo independiente, se conecta al TA a través de una interfaz de capa física estándar. Algunos ejemplos son EIA/TIA-232-C (anteriormente RS-232-C), V.24 y V.35.

Más allá de los dispositivos TE1 y TE2, el siguiente punto de conexión en la red ISDN es el dispositivo de terminación de red tipo 1 (NT1) o de terminación de red tipo 2 (NT2). Estos son dispositivos de terminación de red que conectan el cableado del suscriptor de cuatro hilos al loop local convencional de dos hilos. En Norteamérica, NT1 es un dispositivo de equipo en las instalaciones del cliente (CPE). En la mayoría de otras partes del mundo, el NT1 es parte de la red proporcionada por el portador. NT2 es un dispositivo más complicado, que se encuentra normalmente en las centralitas privadas digitales (PBX), que realiza funciones de protocolo de capa 2 y 3 y servicios de concentración. También existe un dispositivo NT1/2; es un único dispositivo que combina las funciones de un NT1 y un NT2.

En ISDN se especifican varios puntos de referencia. Estos puntos de referencia definen las interfaces lógicas entre los grupos funcionales como los TA y NT1s. Los puntos de referencia ISDN incluyen lo siguiente:

- R-El punto de referencia entre un equipo no ISDN y un TA
- S-El punto de referencia entre los terminales de usuario y NT2
- T-El punto de referencia entre los dispositivos NT1 y NT2
- U-El punto de referencia entre los dispositivos NT1 y el equipo de terminación de línea en la red portadora. El punto de referencia U sólo es relevante en Norteamérica, donde la función NT1 no es proporcionada por la red portadora

A continuación se muestra un ejemplo de configuración ISDN. Este ejemplo muestra tres dispositivos conectados a un switch ISDN en la oficina central. Dos de estos dispositivos son compatibles con ISDN, por lo que se pueden conectar a través de un punto de referencia S a dispositivos NT2. El tercer dispositivo (un teléfono estándar no ISDN) se conecta a través del punto de referencia R a un TA. Cualquiera de estos dispositivos también podría conectarse a un dispositivo NT1/2, que reemplazaría tanto al NT1 como al NT2. Y, aunque no se muestran, se conectan estaciones de usuario similares al switch ISDN de extrema derecha.

Ejemplo de configuración ISDN

```
2503B#show running-config
Building configuration...

Current configuration:
!
version 11.1
service timestamps debug datetime msec
service udp-small-servers
service tcp-small-servers
```

```
!
hostname 2503B
!
!
username 2503A password
ip subnet-zero
isdn switch-type basic-5ess
!
interface Ethernet0
 ip address 172.16.141.11 255.255.255.192
!
interface Serial0
 no ip address
 shutdown
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 description phone#5553754
 ip address 172.16.20.2 255.255.255.0
 encapsulation ppp
 dialer idle-timeout 300
 dialer map ip 172.16.20.1 name 2503A broadcast 5553759
 dialer-group 1
 ppp authentication chap
!
no ip classless
!
dialer-list 1 protocol ip permit
!
line con 0
line aux 0
line vty 0 4
!
end

2503B#
```

Servicios ISDN

El servicio ISDN Basic Rate Interface (BRI) ofrece dos canales B y un canal D (2B+D). El servicio BRI B-channel funciona a 64 kbps y está diseñado para transportar datos del usuario; El servicio BRI D-channel funciona a 16 kbps y tiene la intención de transportar información de control y señalización, aunque puede soportar la transmisión de datos del usuario en ciertas circunstancias. El protocolo de señalización del canal D incluye las capas 1 a 3 del modelo de referencia OSI. BRI también proporciona control de entramado y otras sobrecargas, con lo que su velocidad de bits total alcanza los 192 kbps. La especificación de la capa física BRI es el Sector de estandarización de telecomunicaciones de la Unión Internacional de Telecomunicaciones (ITU-T; antes Comité Consultivo de Telégrafos y Teléfonos Internacionales [CCITT]) I.430.

El servicio ISDN Primary Rate Interface (PRI) ofrece 23 canales B y un canal D en Norteamérica y Japón, lo que proporciona una velocidad de bits total de 1.544 Mbps (el canal PRI D funciona a 64 kbps). ISDN PRI en Europa, Australia y otras partes del mundo proporciona 30 B más un canal D de 64 kbps y una velocidad de interfaz total de 2,048 Mbps. La especificación de capa física PRI es ITU-T I.431.

Capa 1

Los formatos de trama de capa física (Capa 1) de ISDN difieren en función de si la trama es saliente (de terminal a red) o entrante (de red a terminal). Ambas interfaces de capa física se muestran en la figura 16-1.

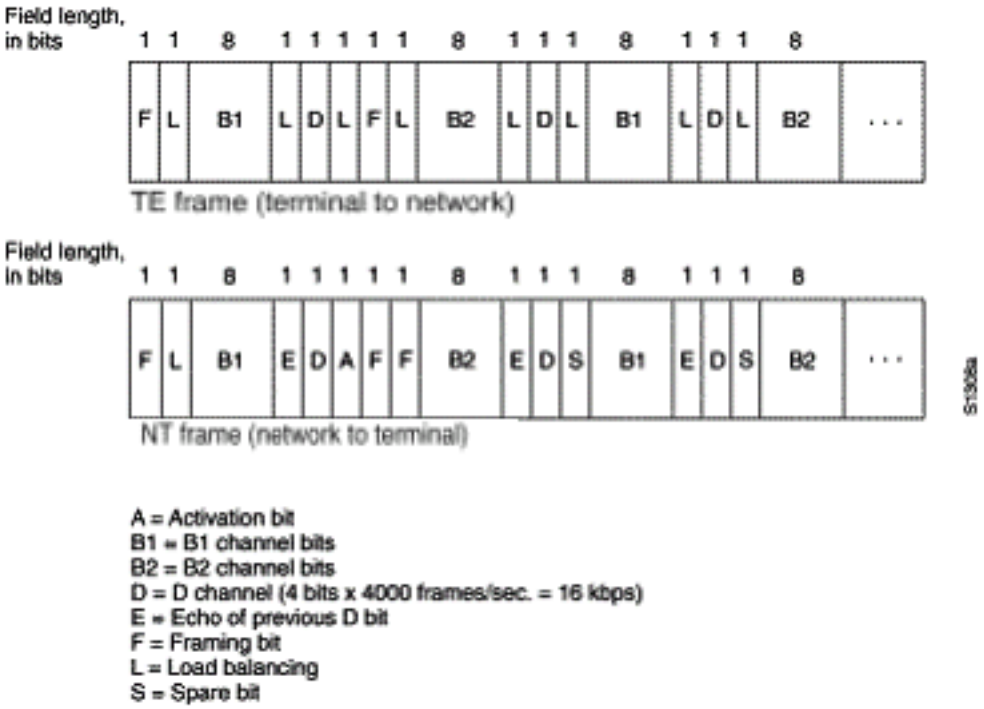

Figura 16-1: Formatos de Trama de Capa Física ISDN

Las tramas tienen 48 bits de longitud, de los cuales 36 bits representan datos. Los bits de una trama de capa física ISDN se utilizan de la siguiente manera:

- F: proporciona sincronización.
- L: ajusta el valor de bit promedio.
- E - Se utiliza para la resolución de contención cuando varios terminales en un campo de control de bus pasivo para un canal.
- A: activa los dispositivos.
- S: sin asignar.
- B1, B2 y D - Para datos de usuario.

Varios dispositivos de usuario ISDN se pueden conectar físicamente a un circuito. En esta configuración, pueden producirse colisiones si dos terminales transmiten simultáneamente. Por lo tanto, ISDN proporciona funciones para determinar la contención del link. Cuando un NT recibe un bit D de TE, se hace eco del bit en la siguiente posición de E-bit. El TE espera que el siguiente bit E sea el mismo que el último bit D transmitido.

Los terminales no pueden transmitir al canal D a menos que primero detecten un número específico de uno (que indica "no hay señal") correspondiente a una prioridad establecida previamente. Si el TE detecta un bit en el canal de eco (E) que es diferente de sus bits D, debe dejar de transmitir inmediatamente. Esta simple técnica asegura que sólo un terminal pueda transmitir su mensaje D a la vez. Después de la transmisión exitosa del mensaje D, el terminal tiene su prioridad reducida al ser requerido para detectar otros más continuos antes de la transmisión. Los terminales no pueden aumentar su prioridad hasta que todos los demás dispositivos de la misma línea hayan tenido la oportunidad de enviar un mensaje D. Las

conexiones telefónicas tienen mayor prioridad que todos los demás servicios y la información de señalización tiene mayor prioridad que la información de no señalización.

Capa 2

La Capa 2 del protocolo de señalización ISDN es el Procedimiento de Acceso de Link en el canal D, también conocido como LAPD. El LAPD es similar al control de enlace de datos de alto nivel (HDLC) y al procedimiento de acceso de enlace, equilibrado (LAPB). Como lo indica la ampliación de la abreviatura de la LAPD, se utiliza a través del canal D para asegurar que la información de control y señalización fluya y se reciba adecuadamente. El formato de trama LAPD (ver figura 16-2) es muy similar al de HDLC y, al igual que HDLC, LAPD utiliza tramas de supervisión, información y sin numerar. El protocolo LAPD se especifica formalmente en ITU-T Q.920 y ITU-T Q.921.

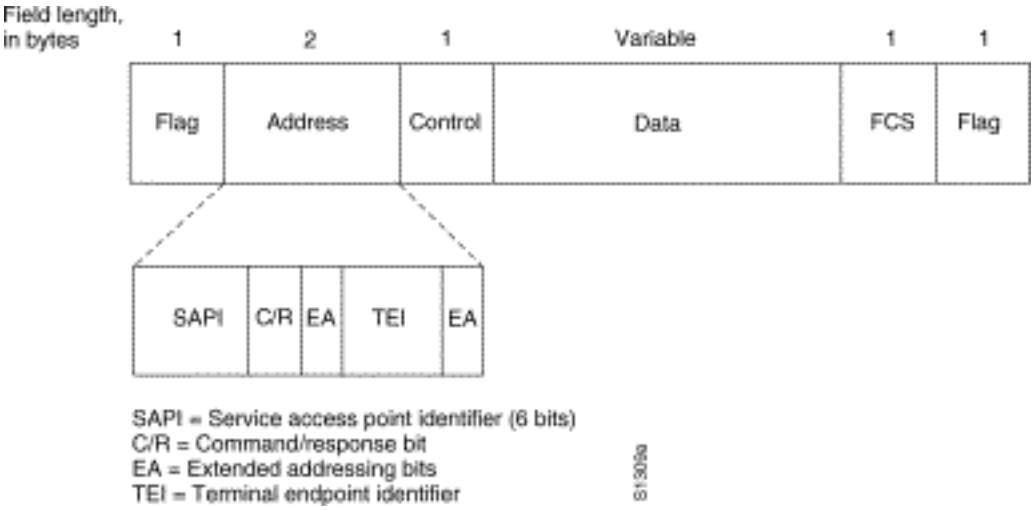

Figura 16-2: Formato de trama LAPD

Los campos LAPD Flag y Control son idénticos a los de HDLC. El campo Dirección LAPD puede tener 1 ó 2 bytes de longitud. Si se configura el bit de dirección extendida del primer byte, la dirección es 1 byte; si no se configura, la dirección es de 2 bytes. El primer byte de campo de dirección contiene el identificador de punto de acceso al servicio (SAPI), que identifica el portal en el que se proporcionan servicios LAPD a la capa 3. El bit C/R indica si la trama contiene un comando o una respuesta. El campo del identificador del terminal (TEI) identifica un único terminal o varios terminales. Un TEI de todos indica una transmisión.

Capa 3

Se utilizan dos especificaciones de Capa 3 para la señalización ISDN: ITU-T (anteriormente CCITT) I.450 (también conocido como ITU-T Q.930) y ITU-T I.451 (también conocido como ITU-T Q.931). Juntos, estos protocolos admiten conexiones de usuario a usuario, conmutación de circuito y conmutación de paquetes. Se especifican diversos mensajes de establecimiento de llamadas, finalización de llamadas, información y varios, incluidos SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS y DISCONNECT.

Estos mensajes son funcionalmente similares a los proporcionados por el protocolo X.25 (consulte el Capítulo 19, "Resolución de problemas de conexiones X.25" para obtener más información). La figura 16-3, de ITU-T I.451, muestra las etapas típicas de una llamada conmutada por circuito ISDN.

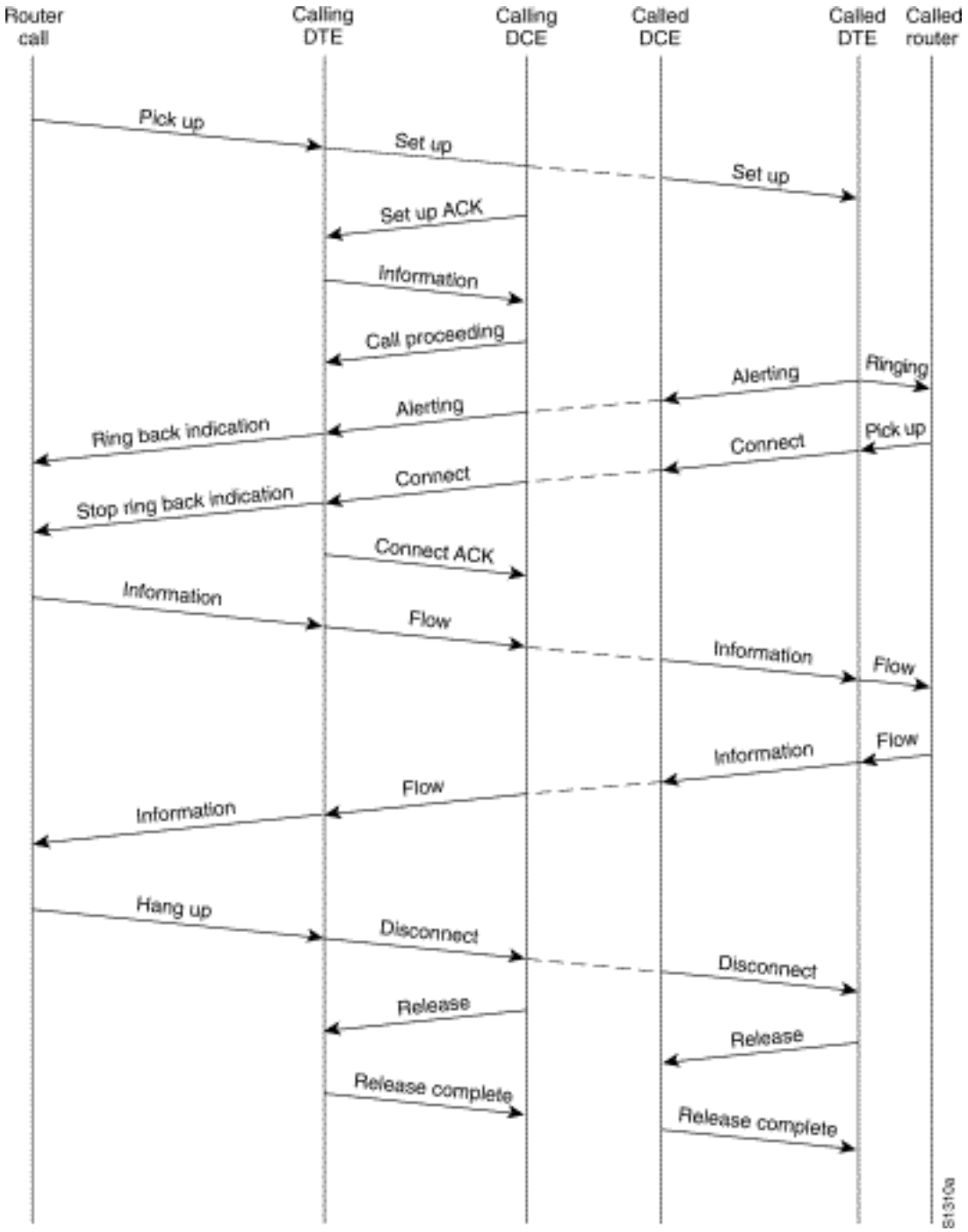

Figura 16-3 Etapas de llamadas conmutadas por circuito ISDN

Interpretación del Resultado Show ISDN Status

Para averiguar cuál es la condición actual de la conexión ISDN entre el router y el switch de la compañía telefónica, utilice el comando **show isdn status**. Los dos tipos de interfaces soportados por este comando son BRI y PRI.

```
3620-2#show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0/0 interface
        dsl 0, interface ISDN Switchtype = basic-ni
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 88, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
        TEI = 97, Ces = 2, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
```

```
Spid Status:
    TEI 88, ces = 1, state = 5(init)
        spid1 configured, no LDN, spid1 sent, spid1 valid
        Endpoint ID Info: epsf = 0, usid = 0, tid = 1
    TEI 97, ces = 2, state = 5(init)
        spid2 configured, no LDN, spid2 sent, spid2 valid
        Endpoint ID Info: epsf = 0, usid = 1, tid = 1
Layer 3 Status:
    0 Active Layer 3 Call(s)
Activated dsl 0 CCBs = 0
The Free Channel Mask:  0x80000003
```

Tabla 16-5:- show isdn status for BRI

Campo	Importancia
Estado de la capa 1: DESACTIVADO	Esto indica que la interfaz BRI no ve una señal en la línea. Hay cinco razones posibles para esta condición. • La interfaz BRI se apaga. Verifique la configuración para el comando **shutdown** en la interfaz BRI, o busque una indicación administrativamente inactiva del comando **show interface**. Utilice la utilidad de configuración e ingrese **no shutdown** en la interfaz BRI. Ingrese el comando **clear interface bri** en el mensaje exec para asegurarse de que la interfaz BRI se reinicie. • Existe un problema con el cableado. Deberá sustituir el cable. Asegúrese de utilizar un cable RJ-45 directo. Para comprobar el cable, mantenga los extremos del cable RJ-45 uno al lado del otro. Si los pines están en el mismo orden, el cable es directo. Si se invierte el orden de los pines, el cable se enrollará. Reemplazar el cable • El puerto ISDN BRI de un router puede requerir un dispositivo NT1. En ISDN, NT1 es un dispositivo que proporciona la interfaz entre el equipo de las instalaciones del cliente y el equipo de conmutación de la oficina central. Si el router no tiene un NT1 interno, obtenga y conecte un NT1 al puerto BRI. Asegúrese de que la BRI o el adaptador de terminal están conectados al puerto S/T del NT1. Consulte la documentación del fabricante para verificar el correcto funcionamiento del NT1 externo. • Es posible que la línea no funcione. Póngase en contacto con la portadora para

	confirmar el funcionamiento de la conexión y verificar la configuración del tipo de switch. • Asegúrese de que el router funciona correctamente. Si hay un hardware defectuoso o que funciona mal, sustituya según sea necesario.

Estado de la capa 2: Estado = TEI_ASSIGNED	Verifique la configuración del tipo de switch y SPIDS. La configuración del switch ISDN específico de la interfaz invalidará la configuración del switch global. El estado SPID indicará si el switch aceptó el SPIDS (válido o no). Póngase en contacto con su proveedor de servicios para verificar la configuración configurada en el router. Para cambiar la configuración SPID, utilice el comando de configuración de la interfaz **isdn *spidn***. Cuando *n* sea 1 o 2, dependiendo del canal en cuestión. Utilice la forma **no** de este comando para quitar el SPID especificado.
	`isdn spidn spid-number [ldn]`
	`no isdn spidn spid-number [ldn]`
	Descripción de la Sintaxis:
	`spid-number`
	El número que identifica el servicio al que se ha suscrito. Este valor lo asigna el proveedor de servicios ISDN y suele ser un número de teléfono de 10 dígitos con dígitos adicionales.
	`ldn`
	(Opcional) Número de directorio local (LDN), que es un número de 7 dígitos asignado por el proveedor de servicios. El switch en el mensaje de configuración entrante entrega esta información. Si no incluye el acceso del directorio local al switch, es posible que el otro canal B no pueda recibir llamadas entrantes. Para ver las negociaciones de capa 2 entre el switch y el router, utilice el comando privilegiado exec **debug isdn q921**. Las depuraciones q921 se documentan en la *Referencia de Comandos Debug*. Las depuraciones dependen en gran medida de los recursos de la CPU, por lo que hay que tener cuidado al utilizarlos.

```
5200-1# show isdn status
Global ISDN Switchtype = primary-5ess
ISDN Serial0:23 interface
        dsl 0, interface ISDN Switchtype = primary-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
```

```
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    The Free Channel Mask:  0x807FFFFF
    Total Allocated ISDN CCBs = 0
5200-1#
```

Si el comando **show isdn status** no funciona o no muestra el PRI, intente utilizar el comando **show isdn service**. Asegúrese de que el comando **pri-group** aparezca en la configuración bajo el controlador T1/E1 en la configuración. Si el comando no está presente, configure el controlador con el comando **pri-group**.

El siguiente es un ejemplo de configuración para un router Cisco con un controlador T1/PRI canalizado:

```
controller t1 0
framing esf
line code b8zs
pri-group timeslots 1-24
```

Tabla 16-6: show isdn status para PRI

Campo	Importancia
Estado de la capa 1: DESACTIVADO	Esto indica que la interfaz PRI no ve la alineación de tramas T1/E1 en la línea. Tenga en cuenta las siguientes causas posibles de esta condición: • La interfaz PRI se apaga. Verifique la configuración para el comando **shutdown** en la interfaz serial0:23 o busque una indicación administrativamente inactiva del comando **show interface**. Utilice la utilidad de configuración e ingrese **no shutdown** en la interfaz en cuestión. Ingrese el comando **clear controller T1/E1** *n* en el mensaje exec para asegurarse de que la interfaz PRI se reinicie. • Existe un problema con el cableado. Deberá sustituir el cable. Asegúrese de utilizar un cable RJ-45 directo. Para comprobar el cable, mantenga los extremos del cable RJ-45 uno al lado del otro. Si los pines están en el mismo orden, el cable es directo. Si se invierte el orden de los pines, el cable se enrollará. Reemplazar el cable • Es posible que la línea no funcione. Póngase en contacto con la portadora para confirmar el funcionamiento de la conexión

	y verificar los parámetros del tipo de switch. • Asegúrese de que el router funciona correctamente. Si hay un hardware defectuoso o que funciona mal, sustituya según sea necesario.
Estado de la capa 2: Estado = TEI_ASSIGNED	Compruebe la configuración del tipo de switch. La configuración del switch ISDN específico de la interfaz invalidará la configuración del switch global. Verifique que T1/E1 esté configurado para coincidir con el switch del proveedor (los problemas de T1/E1 se tratan en el Capítulo 15). Para ver las negociaciones de capa 2 entre el switch y el router, utilice el comando privilegiado exec **debug isdn q921**. Las depuraciones q921 se documentan en la *Referencia de Comandos Debug*. Las depuraciones dependen en gran medida de los recursos de la CPU, por lo que hay que tener cuidado al utilizarlos.
Número de llamadas / Bloques de control de llamadas en uso / Bloques de control de llamadas ISDN asignados totales	Estos números indican el número de llamadas en curso y el número de recursos asignados para admitir dichas llamadas. Si el número de BCC asignados es superior al número de BCC que se utilizan, considere que podría haber un problema en la liberación de BCC. Asegúrese de que hay CCB disponibles para las llamadas entrantes.

Dial on Demand Routing: Operaciones de la interfaz del marcador

Dial on Demand Routing (DDR) es un método para proporcionar conectividad WAN de forma económica y según sea necesario, ya sea como enlace principal o como copia de seguridad para un enlace serial que no sea de marcación.

Una **interfaz de marcador** se define como cualquier interfaz de router capaz de realizar o recibir una llamada. Este término genérico debe distinguirse del término **interfaz del marcador** (con una

D mayúscula), que hace referencia a una interfaz lógica configurada para controlar una o más interfaces físicas de un router y que se ve en una configuración del router como interfaz del marcador X. A partir de este punto, a menos que se indique lo contrario, utilizaremos el término dialer en su sentido genérico.

La configuración de la interfaz del marcador viene en dos tipos: dialer map-based (a veces denominado DDR heredado) y perfiles de marcador. El método que utilice dependerá de las circunstancias en las que necesite conectividad de marcado. Dialer map-based DDR se introdujo por primera vez en IOS versión 9.0, perfiles de marcador en IOS versión 11.2.

Activación de una marcación

En su esencia, DDR es sólo una extensión de ruteo donde *los paquetes interesantes* se rutean a una interfaz de marcador, lo que desencadena un intento de marcado. Las secciones siguientes explican los conceptos involucrados en la definición del tráfico interesante y explican el ruteo utilizado para las conexiones DDR.

Paquetes interesantes

Interesante es el término utilizado para describir paquetes o tráfico que activarán un intento de marcado o, si un link de marcado ya está activo, restablecerán el temporizador de inactividad en la interfaz del marcador. Para que un paquete se considere interesante:

- el paquete debe cumplir los criterios "permit" definidos por una lista de acceso
- la lista de acceso debe ser referenciada por la lista de marcador o el paquete debe ser de un protocolo universalmente permitido por la lista de marcador
- la lista de marcador debe estar asociada a una interfaz de marcador mediante un grupo de marcador

Los paquetes nunca se consideran automáticamente interesantes (de forma predeterminada). Las definiciones de paquetes interesantes deben declararse explícitamente en una configuración de router o servidor de acceso.

Grupo de marcador

En la configuración de cada interfaz de marcador en el router o servidor de acceso, debe haber un comando **dialer-group**. Si el comando **dialer-group** no está presente, no hay un link lógico entre las definiciones de paquetes interesantes y la interfaz. La sintaxis del comando:

```
dialer-group [group number]
```

El número de grupo es el número del grupo de acceso del marcador al que pertenece la interfaz específica. Este grupo de acceso se define con el comando **dialer-list**. Los valores aceptables son valores no cero, enteros positivos entre 1 y 10.

Una interfaz se puede asociar solamente con un grupo de acceso de marcador único; no se permite la asignación de varios dialer-group. Una segunda asignación de grupo de acceso de marcador reemplazará la primera. Un grupo de acceso de marcador se define con el comando **dialer-group**. El comando **dialer-list** asocia una lista de acceso a un grupo de acceso de marcador.

Los paquetes que coinciden con el grupo de marcador especificado activan una solicitud de

conexión.

La dirección de destino del paquete se evalúa contra la lista de acceso especificada en el comando **dialer-list** asociado. Si pasa, se inicia una llamada (si no se ha establecido ninguna conexión) o se restablece el temporizador de inactividad (si hay una llamada conectada actualmente).

Lista de marcadores

El comando de configuración global **dialer-list** se utiliza para definir una lista de marcador DDR para controlar la marcación por protocolo, o por una combinación de protocolo y lista de acceso. Los paquetes interesantes son aquellos que coinciden con el permiso de nivel de protocolo o que están permitidos por la lista en el comando **dialer-list**: **dialer-list dialer-group protocol protocol-name {permit | deny | list** *access-list-number* **| access-group}**

dialer-group es el número de un grupo de acceso de marcador identificado en cualquier comando de configuración de interfaz dialer-group.

protocol-name es una de las siguientes palabras clave del protocolo: appletalk, bridge, clns, clns_es, clns_is, decnet, decnet_router-L1, decnet_router-L2, decnet_node, ip, ipx, vines o xns.

permit permite el acceso a un protocolo completo.

deny niega el acceso a un protocolo completo.

list especifica que se utilizará una lista de acceso para definir una granularidad más fina que un protocolo completo.

access-list-number - Números de lista de acceso especificados en cualquier DECnet, Banyan VINES, IP, Novell IPX o XNS estándar o listas de acceso extendidas, incluidas las listas de acceso de punto de acceso de servicio extendido (SAP) Novell IPX y los tipos de conexión en puente. Consulte la tabla 16-7 para ver los números y tipos de lista de acceso admitidos.

access-group filter list name usado en los **comandos clns filter-set** y **clns access-group**.

Tabla 16-7: Numeración de lista de acceso por protocolo

Tipo de lista de acceso	Rango de números de lista de acceso (decimal)
AppleTalk	600-699
Banyan VINES (estándar)	1-100
Banyan VINES (ampliado)	101-200
DECnet	300-399
IP (estándar)	1-99
IP (extendido)	100-199
Novell IPX (estándar)	800-899
Novell IPX	900-999

(extendido)	
Uso de puente transparente	200-299
XNS	500-599

Lista de acceso

Para cada protocolo de red que se enviará a través de la conexión de marcado, se puede configurar una lista de acceso. A efectos de control de costos, normalmente es deseable configurar una lista de acceso para evitar que cierto tráfico, como las actualizaciones de ruteo, active o mantenga una conexión. Tenga en cuenta que cuando creamos listas de acceso con el propósito de definir el tráfico interesante y no interesante, no declaramos que los paquetes no interesantes no puedan cruzar el link de marcado. Solo indicamos que no restablecerán el temporizador de inactividad, ni que iniciarán una conexión por sí solas. Mientras la conexión de marcado esté activa, se permitirá que los paquetes no interesantes fluyan a través del link.

Por ejemplo, un router que ejecuta EIGRP como su protocolo de ruteo puede tener una lista de acceso configurada para declarar que los paquetes EIGRP no son interesantes y el resto del tráfico IP interesante:

```
access-list 101 deny eigrp any any
access-list 101 permit ip any any
```

Las listas de acceso se pueden configurar para todos los protocolos que puedan atravesar el link de marcado. Recuerde que para cualquier protocolo, el comportamiento predeterminado en ausencia de una sentencia **access-list permit** es denegar todo el tráfico. Si no hay lista de acceso y no hay ningún comando **dialer-list** que permita el protocolo, ese protocolo será poco interesante. En la práctica real, si no hay lista de marcadores para un protocolo, esos paquetes no fluirán a través del link en absoluto.

Ejemplo: Poniéndolo todo

Con todos los elementos implementados, puede examinar el proceso completo por el cual se determina el estado "interesante" de un paquete. En este ejemplo, IP e IPX son los protocolos que pueden cruzar el link de marcado. El usuario desea evitar que las transmisiones y las actualizaciones de ruteo inicien una llamada o mantengan el link activo.

```
!
interface async 1
 dialer-group 7
!
access-list 121 deny eigrp any any
access-list 121 deny ip any host 255.255.255.255
access-list 121 permit ip any any
access-list 903 deny -1 FFFFFFFF 0 FFFFFFFF 452
access-list 903 deny -1 FFFFFFFF 0 FFFFFFFF 453
access-list 903 deny -1 FFFFFFFF 0 FFFFFFFF 457
access-list 903 permit -1
!
dialer-list 7 protocol ip list 121
dialer-list 7 protocol ipx list 903
!
```

Un paquete debe ser permitido por las sentencias **access-list 121**, antes de cruzar la **interfaz asíncrona 1**, para ser considerado *interesante*. En este caso, se niegan los paquetes EIGRP, al igual que cualquier otro paquete de broadcast, mientras que se permite el resto del tráfico IP. Recuerde que esto no impide que los paquetes EIGRP transiten el link. Sólo significa que estos paquetes no restablecerán el temporizador de inactividad ni iniciarán un intento de marcado.

De manera similar, **access-list 903** declara que las solicitudes IPX RIP, SAP y GNS no son interesantes, mientras que el resto del tráfico IPX es interesante. Sin estas sentencias de denegación, es probable que la conexión de marcado nunca se interrumpa y que se produzca una factura telefónica muy grande, ya que los paquetes de estos tipos fluyen constantemente a través de una red IPX.

Con **dialer-group 7** configurado en la interfaz asíncrona, sabemos que **dialer-list 7** es necesario para vincular los filtros de tráfico interesantes (es decir, listas de acceso) a la interfaz. Se requiere una instrucción **dialer-list (y** *sólo* se puede configurar una) para cada protocolo, asegurándose de que el número de lista de marcador sea el mismo que el número de grupo de marcador en la interfaz.

Una vez más, es importante recordar que las sentencias *deny* en las listas de acceso configuradas para definir el tráfico interesante ***no*** impedirán que los paquetes denegados crucen el link.

Con el comando **debug dialer**, puede ver la actividad que activa un intento de marcado:

```
Dialing cause: Async1: ip (s=172.16.1.111 d=172.16.2.22)
```

Aquí vemos que el tráfico IP con una dirección de origen de 172.16.1.111 y una dirección de destino de 172.16.2.22 ha desencadenado un intento de marcado en la interfaz Async1.

Ruteo

Una vez definidos, los paquetes interesantes deben enrutarse correctamente para que se inicie una llamada. El proceso de ruteo depende de dos cosas: entradas de tabla de ruteo y una interfaz "up" sobre la cual rutear paquetes.

Interfaces - up/up (simulación)

Para que los paquetes sean ruteados hacia y a través de una interfaz, esa interfaz debe estar up/up como se ve en un resultado **show interfaces**:

```
Montecito# show interfaces ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is . . .
```

¿Qué sucede con una interfaz de marcador que no está conectada? Si el protocolo no está activo y en ejecución en la interfaz, la implicancia es que la propia interfaz no estará activa. Las rutas que dependen de esa interfaz se vaciarán de la tabla de ruteo y el tráfico no se enrutará a esa interfaz. El resultado es que la interfaz no iniciaría ninguna llamada.

La solución para contrarrestar esta posibilidad es permitir el estado **activo/activo (simulación)** para las interfaces del marcador. Cualquier interfaz se puede configurar como una interfaz de marcador. Por ejemplo, una interfaz serial o asíncrona se puede convertir en un marcador agregando el comando **dialer in-band** o **dialer dtr** a la configuración de la interfaz. Estas líneas son innecesarias para las interfaces que por naturaleza son una interfaz de marcador (BRI y PRI). El resultado para una interfaz show tendrá el siguiente aspecto:

```
Montecito# show interfaces bri 0
BRI0 is up, line protocol is up (spoofing)
  Hardware is BRI
  Internet address is . . .
```

En otras palabras, la interfaz "pretende" estar **activa/activa** para que las rutas asociadas permanezcan en vigor y para que los paquetes puedan ser enrutados a la interfaz.

Hay circunstancias en las que una interfaz de marcador no se **activará/activará (suplantación)**. La salida **show interface** puede mostrar que la interfaz está administrativamente inactiva:

```
Montecito# show interfaces bri 0
BRI0 is administratively down, line protocol is down
  Hardware is BRI
  Internet address is . . .
```

Administrativamente desactivado significa simplemente que la interfaz se ha configurado con el comando **shutdown**. Este es el estado predeterminado de cualquier interfaz de router cuando el router se inicia por primera vez. Para remediar esto, utilice el comando de configuración de interfaz **no shutdown**.

También puede verse que la interfaz está en modo de espera:

```
Montecito# show interfaces bri 0
BRI0 is standby mode, line protocol is down
  Hardware is BRI
  Internet address is . . .
```

Este estado indica que la interfaz se ha configurado como respaldo para otra interfaz. Cuando una conexión requiere redundancia en caso de falla, se puede configurar una interfaz de marcador como respaldo. Esto se logra agregando los siguientes comandos a la interfaz de la conexión primaria:

```
backup interface [interface]
backup delay [enable-delay] [disable-delay]
```

Una vez que el comando **backup interface** se ha configurado, la interfaz utilizada como respaldo se pondrá en modo standby hasta el momento en que la interfaz primaria pase a un estado **down/down**. En ese momento, la interfaz del marcador configurada como copia de seguridad pasará a un estado de **encendido/apagado (suplantación)** pendiente de un evento de marcado.

Rutas estáticas y rutas estáticas flotantes

La manera más segura de rutear paquetes a una interfaz de marcador es con ruteo estático. Estas rutas se ingresan manualmente en la configuración del router o del servidor de acceso con el comando:

ip route *prefix mask* {*address* | *interface*} [*distance*]

prefijo: Prefijo de ruta IP para el destino.

máscara: Máscara de prefijo para el destino.

dirección: Dirección IP del salto siguiente que se puede utilizar para alcanzar la red de destino.

interfaz: Interfaz de red que se utiliza para el tráfico saliente.

administrativa: (Opcional) Una distancia administrativa. Este argumento se utiliza en rutas estáticas flotantes.

Las rutas estáticas se utilizan en situaciones donde el link de marcado es la única conexión al sitio remoto. Una ruta estática tiene un valor de distancia administrativa de uno (1), lo que la hace preferible sobre las rutas dinámicas al mismo destino.

Por otra parte, las rutas estáticas flotantes (es decir, las rutas estáticas con una distancia administrativa predefinida) se utilizan normalmente en escenarios DDR de respaldo. En estos escenarios, un protocolo de ruteo dinámico, como RIP o EIGRP, enruta paquetes a través del link primario.

Una ruta estática normal (distancia administrativa = 1) es preferible a EIGRP (distancia administrativa = 90) o RIP (distancia administrativa = 120). La ruta estática hace que los paquetes sean enrutados a través de la línea de marcado, incluso si el primario está activo y es capaz de pasar tráfico. Sin embargo, si la ruta estática se configura con una distancia administrativa superior a la de cualquiera de los protocolos de ruteo dinámicos en uso en el router, la ruta estática flotante sólo se utilizará en ausencia de una ruta "mejor", una con una distancia administrativa menor.

Si el DDR de respaldo se invoca mediante el uso del comando **backup interface**, la situación es algo diferente. Debido a que la interfaz del marcador permanece en modo de espera mientras el primario está **activo**, se puede configurar una ruta estática o una ruta estática flotante. La interfaz del marcador no intentará conectarse hasta después de que la interfaz primaria se **haya caído/caído**.

Para una conexión determinada, el número de rutas estáticas (o estáticas flotantes) necesarias es una función del direccionamiento en las interfaces del marcador. En los casos en que las dos interfaces de marcador (una en cada uno de los dos routers) comparten una red o subred común, normalmente sólo se requiere una ruta estática. Señala a la LAN remota usando la dirección de la interfaz del marcador del router remoto como la dirección de salto siguiente.

Examples

Ejemplo 1: La marcación es la única conexión que utiliza interfaces numeradas. Una ruta es suficiente.

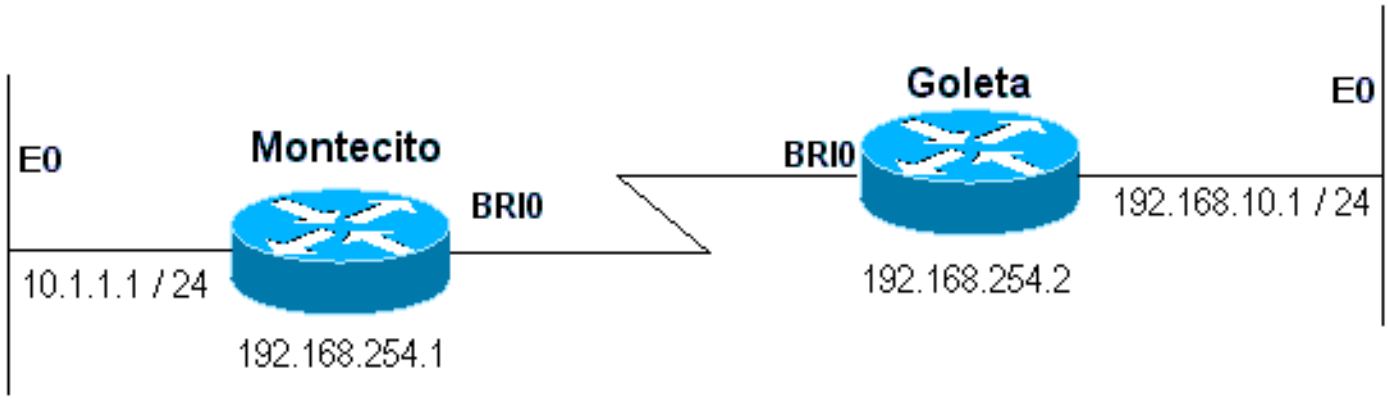

Figura 16-4: Marcación mediante interfaces numeradas

```
Montecito:
ip route 192.168.10.0 255.255.255.0 172.16.20.2
Goleta:
ip route 10.1.1.0 255.255.255.0 172.16.20.1
```

Ejemplo 2: La marcación es la única conexión que utiliza interfaces sin numerar. Esto se puede configurar con sólo una ruta, pero es común configurar dos rutas: una ruta de host a la interfaz LAN en el router remoto y una ruta a la LAN remota a través de la interfaz LAN remota. Esto se hace para evitar problemas de mapeo de Capa 3 a Capa 2, que pueden resultar en fallas de encapsulación.

Este método también se utiliza si las interfaces del marcador en los dos dispositivos están numeradas, pero no en la misma red o subred.

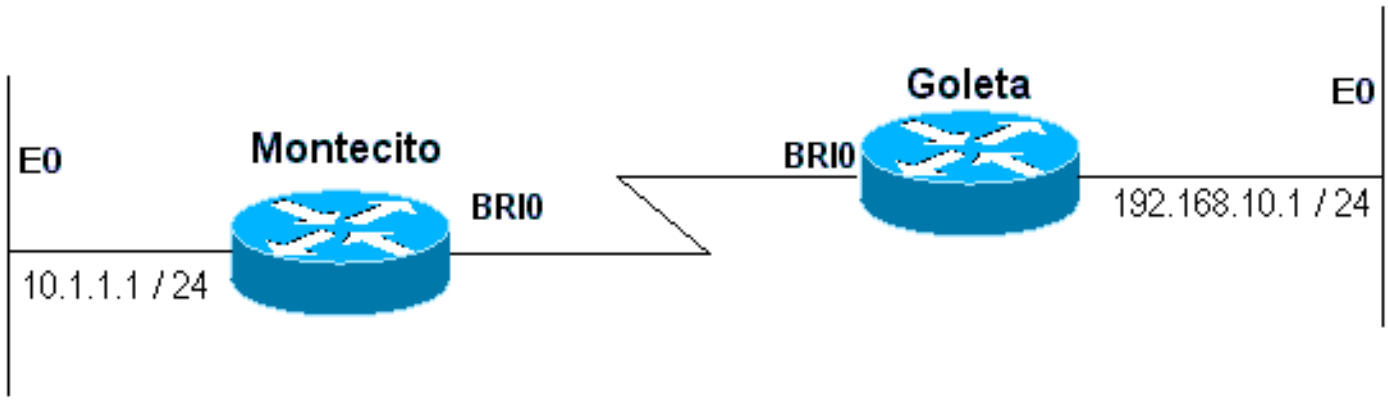

Figura 16-5: Marcación mediante interfaces sin numerar

```
Montecito:
ip route 192.168.10.0 255.255.255.0 192.168.10.1
ip route 192.168.10.1 255.255.255.255 BRI0
Goleta:
ip route 10.1.1.0 255.255.255.0 10.1.1.1
ip route 10.1.1.1 255.255.255.255 BRI0
```

Ejemplo 3: La marcación es una conexión de respaldo que utiliza interfaces numeradas. Se requiere una ruta estática flotante.

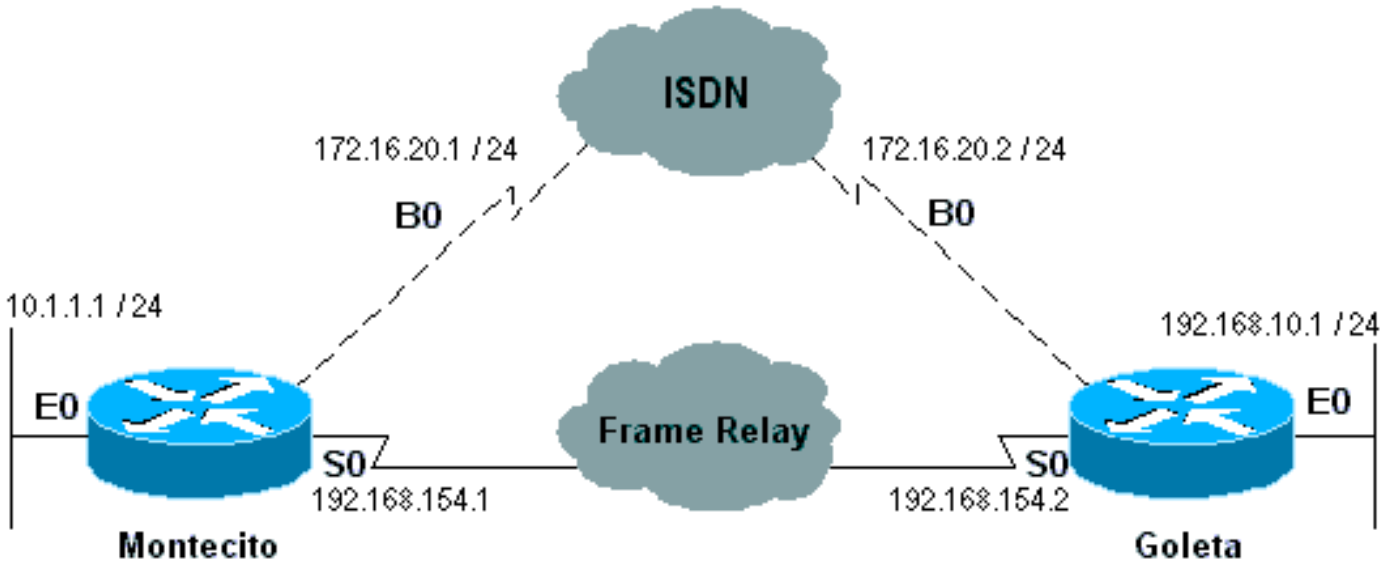

Figura 16-6: Copia de seguridad mediante interfaces numeradas

```
Montecito:
ip route 192.168.10.0 255.255.255.0 172.16.20.2 200
Goleta:
ip route 10.1.1.0 255.255.255.0 172.16.20.1 200
```

Ejemplo 4: La marcación es una conexión de respaldo que utiliza interfaces sin numerar. Como en el ejemplo 2 anterior, este método también se utiliza si las interfaces del marcador en los dos dispositivos están numeradas, pero no en la misma red o subred.

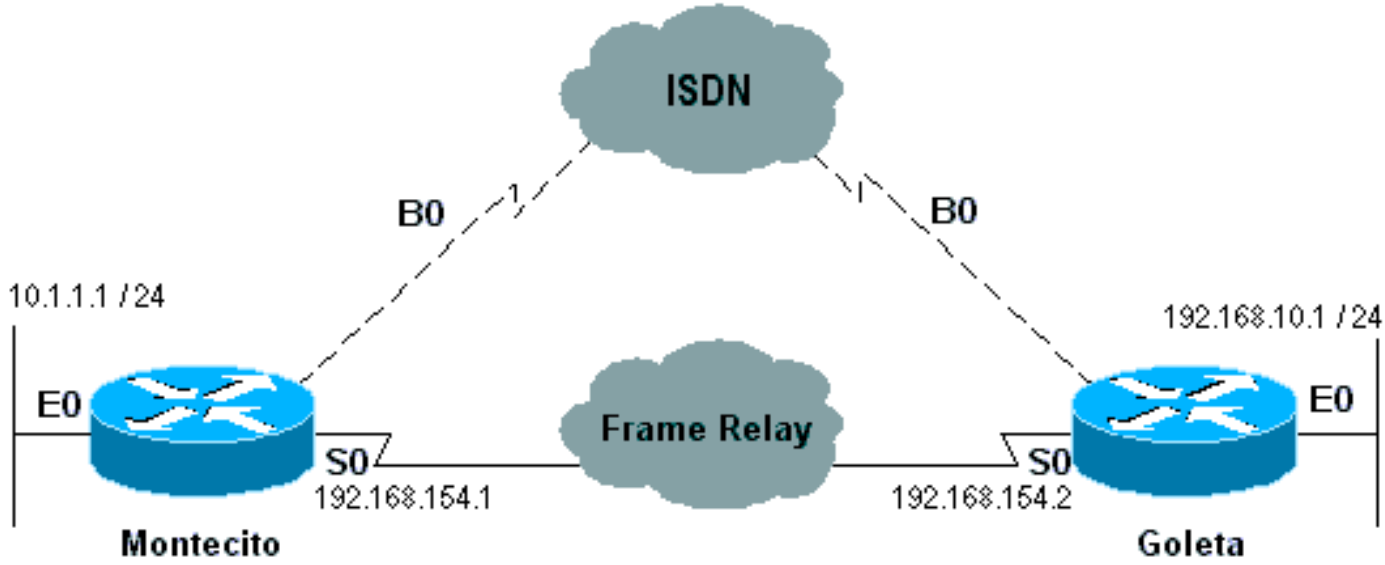

Figura 16-7: Copia de seguridad con interfaces sin numerar

```
Montecito:
ip route 192.168.10.0 255.255.255.0 192.168.10.1 200
ip route 192.168.10.1 255.255.255.255 BRI0 200
Goleta:
ip route 10.1.1.0 255.255.255.0 10.1.1.1 200
ip route 10.1.1.1 255.255.255.255 BRI0 200
```

Mapas del marcador

El DDR basado en mapa de marcador (heredado) es potente y completo, pero sus limitaciones afectan a la escalabilidad y la extensibilidad. El DDR basado en mapa del marcador se basa en un enlace estático entre la especificación de llamada por destino y la configuración de la interfaz física.

Sin embargo, el DDR basado en el mapa del marcador también tiene muchas fortalezas. Admite Frame Relay, ISO CLNS, LAPB, ruteo de instantáneas y todos los protocolos ruteados que se soportan en los routers Cisco. De forma predeterminada, el DDR basado en mapa del marcador admite fast switching.

Al configurar una interfaz para llamadas salientes, se debe configurar un mapa de marcador para cada destino remoto y para cada número llamado diferente en el destino remoto. Por ejemplo, si desea una conexión PPP de links múltiples al marcar desde un BRI ISDN a otra interfaz BRI ISDN que tenga un número de directorio local diferente para cada uno de sus canales B, necesita un mapa de marcador para cada uno de los números remotos:

```
!
interface bri 0
 dialer map ip 172.16.20.1 name Montecito broadcast 5551234
 dialer map ip 172.16.20.1 name Montecito broadcast 5554321
!
```

El orden en el que se configuran los mapas del marcador puede ser importante. Si dos o más comandos dialer map se refieren a la misma dirección remota, el router o el servidor de acceso los probarán uno tras otro, en orden, hasta que un comando establezca una conexión correctamente

Nota: IOS puede construir dinámicamente mapas de marcador en un router que recibe una llamada. El mapa del marcador se construye sobre la base del nombre de usuario autenticado y la dirección IP negociada de la persona que llama. Los mapas de marcador dinámicos sólo se pueden ver en el resultado del comando **show dialer map**. No puede verlos en la configuración en ejecución del router o del servidor de acceso.

Sintaxis del comando

Utilice la siguiente forma del comando de configuración de la interfaz **dialer map** para:

- configurar una interfaz serial o una interfaz ISDN para llamar a uno o varios sitios, o
- recibir llamadas desde varios sitios.

Todas las opciones se muestran en esta primera forma del comando. Para eliminar una entrada de correspondencia de marcador determinada, utilice una forma **no** de este comando.

```
dialer map protocol next-hop-address [name hostname] [spc] [speed 56 | 64]
[broadcast] [modem-script modem-regexp] [system-script system-regexp]
[dial-string[:isdn-subaddress]]
```

Utilice la siguiente forma del comando **dialer map** para:

- configure una interfaz serial o una interfaz ISDN para realizar una llamada a varios sitios, y
- para autenticar llamadas desde varios sitios.

```
dialer map protocol next-hop-address [name hostname] [spc] [speed 56 | 64]
```

```
[broadcast] [dial-string[:isdn-subaddress]]
```

Utilice la siguiente forma del comando **dialer map** para configurar una interfaz serial o una interfaz ISDN para soportar el bridging.

```
dialer map bridge [name hostname] [spc] [broadcast] [dial-string[:isdn-subaddress]]
```

Utilice la siguiente forma del comando **dialer map** para configurar una interfaz asincrónica para realizar una llamada a:

- un único sitio que requiera un script de sistema o que no tenga asignado un script de módem, o
- varios sitios en una sola línea, en varias líneas o en un grupo rotativo de marcador.

```
dialer map protocol next-hop-address [name hostname] [broadcast]
[modem-script modem-regexp] [system-script system-regexp] [dial-string]
```

Descripción de la Sintaxis

- *protocol* **-** Palabras clave del protocolo. Utilice una de las siguientes opciones: **appletalk, bridge, clns, decnet, ip, ipx, novell, instantánea, vines o xns.**
- *next-hop-address* - La dirección de protocolo utilizada para coincidir con las direcciones a las que se destinan los paquetes. Este argumento no se utiliza con la palabra clave **bridge** protocol.
- **name**: (Opcional) Indica el sistema remoto con el que se comunica el router local o el servidor de acceso. Se utiliza para autenticar el sistema remoto en llamadas entrantes.
- *nombre de host* : (opcional) Nombre o ID del dispositivo remoto que distingue entre mayúsculas y minúsculas (normalmente el nombre de host). Para los routers con interfaces ISDN, el campo *hostname* puede contener el número que proporciona el ID de línea de llamada (en los casos en los que la identificación de línea de llamada, también denominada *CLI* , *ID de la persona que llama* y *identificación automática de número* (ANI), está disponible).
- **spc**: (Opcional) Especifica una conexión semipermanente entre el equipo del cliente y el intercambio. Sólo se utiliza en Alemania para circuitos entre un ISDN BRI y un switch ISDN 1TR6 y en Australia para circuitos entre un ISDN PRI y un switch TS-014.
- **speed 56 | 64** - (Opcional) Palabra clave y valor que indica la velocidad de línea en kilobits por segundo para usar. Se utiliza sólo para ISDN. La velocidad predeterminada es 64 kbps.
- **broadcast**: (Opcional) Indica que las transmisiones deben reenviarse a esta dirección de protocolo.
- **modem-script**: (Opcional) Indica la secuencia de comandos del módem que se utilizará para la conexión (para interfaces asincrónicas).
- *modem-regexp* : expresión regular (opcional) a la que se hará coincidir un script de módem (para interfaces asincrónicas).
- **system-script**: (Opcional) Indica la secuencia de comandos del sistema que se utilizará para la conexión (para interfaces asincrónicas).
- *system-regexp* : expresión regular (opcional) a la que se hará coincidir una secuencia de comandos del sistema (para interfaces asincrónicas).
- *dial-string[:isdn-subaddress]* (Opcional) Número de teléfono enviado al dispositivo de

marcación tras el reconocimiento de paquetes con una dirección de salto siguiente especificada que coincida con la lista de acceso definida (y el número de subdirección opcional utilizado para las conexiones multipunto ISDN). La cadena de marcado y la subdirección ISDN, si se utilizan, deben ser el último elemento de la línea de comandos.

Perfiles de Marcador

Nota: En esta sección el término "interfaz de marcador" se refiere a la interfaz configurada; no a una interfaz física en el router o el servidor de acceso.

La implementación de perfiles de marcador de DDR, introducida en la versión 11.2 del IOS, se basa en una separación entre la configuración de interfaz lógica y física. Los perfiles de marcador también permiten que las configuraciones físicas y lógicas se unan dinámicamente por llamada.

La metodología Perfiles de marcador es ventajosa cuando desea hacer lo siguiente:

- compartir una interfaz (ISDN, asíncrona o serial sincrónica) para realizar o recibir llamadas
- cambiar cualquier configuración por usuario (excepto la encapsulación en la primera fase de perfiles de marcador)
- Bridge a muchos destinos
- evitar problemas de horizonte dividido

Los perfiles de marcador permiten separar la configuración de las interfaces físicas de la configuración lógica necesaria para una llamada, y también permiten que las configuraciones físicas y lógicas se unan dinámicamente por llamada.

Un *perfil de marcador* consta de los siguientes elementos:

- Una configuración de *interfaz del marcador* (una entidad lógica), incluidas una o más cadenas de marcado (cada una de las cuales se utiliza para alcanzar una subred de destino)
- Una clase de *mapa del marcador* que define todas las características de cualquier llamada a la cadena de marcado especificada
- Un *conjunto de marcadores ordenado* de interfaces físicas que será utilizado por la interfaz del marcador

Todas las llamadas que se dirigen a o desde la misma subred de destino utilizan el mismo perfil de marcador.

Una configuración de interfaz del marcador incluye todos los ajustes necesarios para alcanzar una subred de destino específica (y cualquier red a la que se llegue a través de ella). Se pueden especificar varias cadenas de marcación para la misma interfaz del marcador; cada cadena de marcado se puede asociar a una clase de mapa de marcador diferente. El dialer map-class define todas las características de cualquier llamada a la cadena de marcado especificada. Por ejemplo, la clase de mapa para un destino podría especificar una velocidad ISDN de 56 kbps. La clase de mapa para un destino diferente podría especificar una velocidad ISDN de 64 kbps.

Cada interfaz del marcador utiliza un conjunto de marcadores, que es un conjunto de interfaces físicas ordenadas según la prioridad asignada a cada interfaz física. Una interfaz física puede pertenecer a varios conjuntos de marcadores, con la contención resuelta por prioridad. Las interfaces ISDN BRI y PRI pueden establecer un límite en el número mínimo y máximo de canales B reservados por cualquier conjunto de marcadores. Un canal reservado por un conjunto de marcadores permanece inactivo hasta que el tráfico se dirige al conjunto.

Cuando se utilizan perfiles de marcador para configurar DDR, una interfaz física no tiene valores de configuración excepto encapsulación y los grupos de marcador a los que pertenece la interfaz.

Nota: El párrafo anterior tiene una excepción. Los comandos que se aplican antes de completar la autenticación deben configurarse en la interfaz física (o BRI o PRI) y no en el perfil del marcador. Los perfiles de marcador no copian los comandos de autenticación PPP (o los comandos LCP) en la interfaz física.

La figura 16-8 muestra una aplicación típica de perfiles de marcador. El Router A tiene la interfaz de marcador 1 para el ruteo de marcado a pedido con la subred 1.1.1.0, y la interfaz de marcador 2 para el ruteo de marcado a pedido con la subred 2.2.2.0. La dirección IP para la interfaz de marcador 1 es su dirección como nodo en la red 1.1.1.0. Al mismo tiempo, esa dirección IP funciona como la dirección IP de las interfaces físicas utilizadas por la interfaz del marcador 1. De manera similar, la dirección IP para la interfaz de marcador 2 es su dirección como nodo en la red 2.2.2.0.

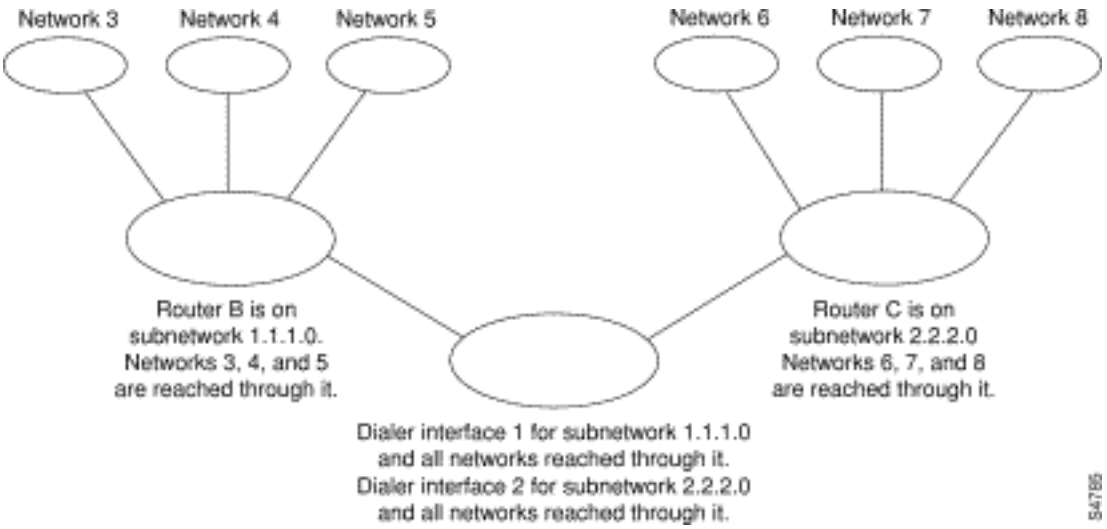

Figura 16-8: Aplicación de perfiles de marcador típica

Una interfaz de marcador utiliza sólo un conjunto de marcador. Sin embargo, una interfaz física puede ser miembro de uno o varios grupos de marcadores, y un grupo de marcadores puede tener varias interfaces físicas como miembros.

La figura 16-9 ilustra las relaciones entre los conceptos de interfaz de marcador, conjunto de marcador e interfaces físicas. La interfaz de marcador 0 utiliza el conjunto de marcador 2. La interfaz física BRI 1 pertenece al conjunto de marcadores 2 y tiene una prioridad específica en el conjunto. La interfaz física BRI 2 también pertenece al conjunto de marcadores 2. Debido a que la contención se resuelve sobre la base de niveles de prioridad de las interfaces físicas en el conjunto, se deben asignar prioridades diferentes a BRI 1 y BRI 2 en el conjunto. Tal vez a BRI 1 se le asigne la prioridad 100 y a BRI 2 se le asigne la prioridad 50 en el conjunto de marcadores 2 (una prioridad de 50 es mayor que una prioridad de 100). BRI 2 tiene una prioridad más alta en el conjunto y sus llamadas se realizarán primero.

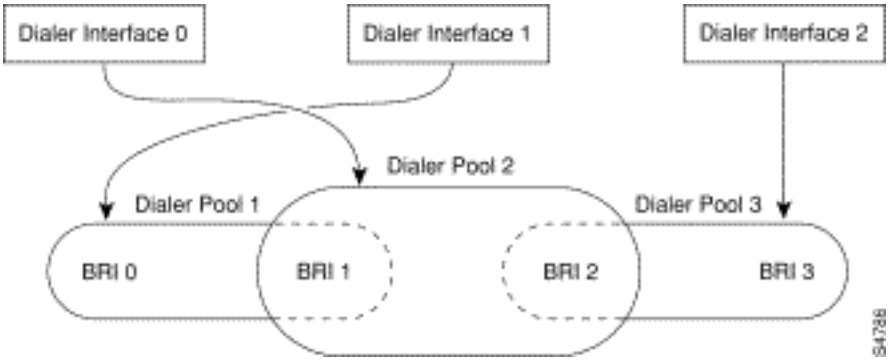

Figura 16-9: Relaciones entre interfaces de marcador, grupos de marcador e interfaces físicas

Pasos de configuración del perfil del marcador

Comando	Propósito
número de marcador de interfaz	Cree una interfaz de marcador.
máscara de dirección ***IP***	Especifique la dirección y máscara IP de la interfaz de marcador como nodo en la red de destino a llamar.
encapsulación ppp	Especifique el encapsulado de PPP.
dialer remote-name username	Especifique el nombre de autenticación CHAP del router remoto.
dialer string dial-string class class-name	Especifique el destino remoto para la llamada y la clase de asociador que define las características para las llamadas a este destino.
número de grupo ***de marcador***	Especifique el grupo de marcado a utilizar para llamadas a este destino.
dialer-group group-number	Asigne la interfaz del marcador a un grupo de marcador.
dialer-list dialer-group protocol protocol-name {permit | deny | list ***access-list-number*****}**	Especifique una lista de acceso por número de lista o por protocolo y número de lista para definir los paquetes "interesantes" que pueden activar una llamada.

Operaciones PPP

El protocolo punto a punto (PPP) es el protocolo de transporte de capa de enlace más común, ya que usurpó por completo el SLIP como protocolo de elección para las conexiones seriales síncronas y asíncronas de marcado (y en muchos casos, sin marcado). PPP fue definido originalmente en 1989 por RFC 1134, que desde entonces se ha vuelto obsoleto por una serie de RFC que culminan (a partir de este texto) en RFC1661. También hay numerosos RFC que definen elementos del protocolo, como RFC1990 (el PPP Multilink Protocol), RFC2125 (el PPP Bandwidth Allocation Protocol) y muchos otros. Puede encontrar un repositorio en línea de RFCs

en:

http://www.ietf.org/rfc.html

Quizás la mejor definición de PPP se encuentre en RFC1661, que dice:

El Protocolo punto a punto (PPP) ofrece un método estándar para transportar datagramas multiprotocolo a través de enlaces de punto a punto. PPP está conformado por tres componentes principales:

1. Método para encapsular datagramas multiprotocolo.
2. Protocolo de control de enlaces (LCP) para establecer, configurar y probar la conexión de enlace de datos.
3. Una familia de protocolos de control de red (NCP) para establecer y configurar diferentes protocolos de capa de red.

Etapas de la negociación PPP

La negociación PPP consta de tres fases: Protocolo de control de enlaces (LCP), autenticación y protocolo de control de red (NCP). Cada producto se realiza en orden, luego del establecimiento de la conexión asíncrona o ISDN.

LCP (Protocolo de control de enlace)

PPP no sigue un modelo cliente/servidor. Todas las conexiones son de igual a igual. Por lo tanto, cuando hay una persona que llama y un receptor, ambos extremos de la conexión punto a punto deben acordar los protocolos y parámetros negociados.

Cuando comienza la negociación, cada uno de los peers que desea establecer una conexión PPP debe enviar una solicitud de configuración (vista en **debug ppp negotiation** y referida a continuación como CONFREQ). En la CONFREQ se incluye cualquier opción que no sea la predeterminada del link. Estos suelen incluir la unidad máxima de recepción (MRU), el mapa asíncrono de caracteres de control (ACCM), el protocolo de autenticación (AuthProto) y el número mágico. También se ven la unidad de recepción máxima reconstruida (MRU) y el discriminador de terminales (EndpointDisc), que se utilizan para PPP de enlaces múltiples.

Hay tres respuestas posibles a cualquier CONFREQ:

- Se debe emitir un Configure-Acknowledge (CONFACK) si el par reconoce las opciones y acepta los valores que se ven en el CONFREQ.
- Debe enviarse un mensaje de Configure-Reject (CONFREJ) si no se reconoce ninguna de las opciones de CONFREQ (por ejemplo, algunas opciones específicas del proveedor) o si los valores de cualquiera de las opciones se han anulado explícitamente en la configuración del par.
- Se debe enviar un mensaje Configure-Negative-Acknowledge (CONFNAK) si se reconocen todas las opciones de CONFREQ, pero los valores no son aceptables para el par.

Los dos pares continúan intercambiando CONFREQs, CONFREJs y CONFNAKs hasta que cada uno envía un mensaje CONFACK, hasta que se interrumpe la conexión de marcado, o hasta que uno o ambos pares indiquen que la negociación no puede completarse.

Autenticación

Después de completar con éxito la negociación LCP y alcanzar un acuerdo sobre AuthProto, el siguiente paso es la autenticación. La autenticación, aunque no es obligatoria según RFC1661, es altamente recomendada en todas las conexiones de marcado. En algunos casos, es un requisito para el buen funcionamiento; Perfiles de marcador que son un ejemplo de ello.

Los dos tipos principales de autenticación en PPP son el protocolo de autenticación de contraseña (PAP) y el protocolo de autenticación por desafío mutuo (CHAP), definido por RFC1334 y actualizado por RFC1994.

PAP es el más simple de los dos, pero es menos seguro porque la contraseña de texto sin formato se envía a través de la conexión de marcado. CHAP es más seguro porque la contraseña de texto sin formato nunca se envía a través de la conexión de marcado.

El PAP puede ser necesario en uno de los siguientes entornos:

- Una gran base de aplicaciones cliente instalada que no admite CHAP
- Incompatibilidad entre las distintas instrumentaciones de vendedores de CHAP

Al hablar de autenticación, es útil utilizar los términos "solicitante" y "autenticador" para distinguir las funciones que desempeñan los dispositivos en cualquiera de los extremos de la conexión, aunque cualquiera de los pares puede actuar en cualquiera de las dos funciones. "Solicitante" describe el dispositivo que solicita acceso a la red y suministra información de autenticación; el "autenticador" verifica la validez de la información de autenticación y permite o no la conexión. Es común que ambos pares actúen en ambas funciones cuando se realiza una conexión DDR entre routers.

PAP

PAP es bastante simple. Después de completar correctamente la negociación LCP, el solicitante envía repetidamente su combinación de nombre de usuario/contraseña a través del link hasta que el autenticador responda con un reconocimiento o hasta que el link se rompa. El autenticador puede desconectar el link si determina que la combinación nombre de usuario/contraseña no es válida.

CHAP

CHAP es algo más complicado. El autenticador envía un desafío al solicitante, que luego responde con un valor. Este valor se calcula utilizando una función "hash unidireccional" para hash el desafío y la contraseña CHAP juntos. El valor resultante se envía al autenticador junto con el nombre de host CHAP del solicitante (que puede ser diferente de su nombre de host real) en un mensaje *de respuesta*.

El autenticador lee el nombre de host en el mensaje de respuesta, busca la contraseña esperada para ese nombre de host y luego calcula el valor que espera que el solicitante envíe en su respuesta realizando la misma función hash que el solicitante realizó. Si los valores resultantes coinciden, la autenticación es correcta. El fallo debe provocar una desconexión.

AAA

Se puede utilizar un servicio de autenticación, autorización y contabilidad (AAA), como TACACS+

o RADIUS, para lograr PAP o CHAP.

NCP

Después de una autenticación exitosa, comienza la fase NCP. Al igual que en LCP, los pares intercambian CONFREQ, CONFREJ, CONFNAK y CONFACK. Sin embargo, en esta fase de negociación, los elementos que se negocian tienen que ver con protocolos de capa más alta: IP, IPX, Bridging, CDP, etc. Se puede negociar uno o más de estos protocolos. Dado que es el más utilizado y que otros protocolos funcionan de la misma manera, el protocolo de control de protocolo de Internet (IPCP), definido en RFC1332, es el foco de esta discusión. Otros RFC pertinentes incluyen, entre otros:

- RFC1552 (protocolo de control IPX)
- RFC1378 (protocolo de control AppleTalk)
- RFC1638 (protocolo de control de puente)
- RFC1762 (Protocolo de control DECnet)
- RFC1763 (protocolo de control de vinas)

Además, el protocolo de control de protocolo de detección de Cisco (CDPCP) se puede negociar durante el NCP, aunque esto no es común. Los ingenieros del TAC de Cisco normalmente aconsejarán que el comando no cdp enable se configure en todas las interfaces del marcador para evitar que los paquetes CDP mantengan una llamada activa indefinidamente.

El elemento clave negociado en IPCP es la dirección de cada entidad par. Cada uno de los pares está en uno de los dos estados posibles; Tiene una dirección IP o no tiene dirección IP. Si el par ya tiene una dirección, la enviará en una CONFREQ al otro par. Si la dirección es aceptable para el otro par, se devolverá una CONFACK. Si la dirección no es aceptable, la respuesta será una CONFNAK que contenga una dirección para que la utilice el par.

Si el par no tiene dirección, enviará una CONFREQ con la dirección 0.0.0.0. Esto indica al otro par que asigne una dirección, lo que se logra al enviar una CONFNAK con la dirección adecuada.

Otras opciones pueden negociarse en IPCP. Las direcciones principales y secundarias de Servidor de nombres de dominio y Servidor de nombres NetBIOS que se describen en RFC1877 informativo son las más frecuentes. El protocolo de compresión IP (RFC1332) también es común.

Metodologías PPP alternativas

Las metodologías PPP alternativas incluyen PPP de links múltiples, PPP de chasis múltiples y perfiles virtuales.

PPP de links múltiples

La función Multilink Point-to-Point Protocol (MLP) proporciona funcionalidad de equilibrio de carga en varios enlaces WAN. Al mismo tiempo, proporciona interoperabilidad de varios proveedores, fragmentación de paquetes y secuenciación adecuada, y cálculo de carga tanto en el tráfico entrante como saliente. La implementación de Cisco de PPP de links múltiples soporta las especificaciones de fragmentación y secuenciación de paquetes en RFC1717.

Multilink PPP permite que los paquetes se fragmenten. Estos fragmentos se pueden enviar al mismo tiempo a través de varios links punto a punto a la misma dirección remota. Los links múltiples aparecen en respuesta a un umbral de carga del marcador que usted define. La carga

se puede calcular en el tráfico entrante, el tráfico saliente, o en cualquiera, según sea necesario para el tráfico entre los sitios específicos. MLP proporciona el ancho de banda solicitado y reduce la latencia de la transmisión a través de los links WAN.

El PPP de links múltiples funciona sobre los siguientes tipos de interfaz (único o múltiple) configurados para soportar tanto los grupos rotatorios de marcado a pedido como la encapsulación PPP:

- interfaces seriales asíncronas
- BRI
- PRI

Configuración

Para configurar Multilink PPP en interfaces asincrónicas, configure las interfaces asincrónicas para soportar la encapsulación DDR y PPP. A continuación, configure una interfaz Dialer para soportar la encapsulación PPP, el ancho de banda a demanda y el PPP de links múltiples. Sin embargo, en algún momento, agregar más interfaces asincrónicas no mejora el rendimiento. Con el tamaño de MTU predeterminado, el PPP de links múltiples debe soportar tres interfaces asincrónicas usando módems V.34. Sin embargo, los paquetes pueden ser descartados ocasionalmente si la MTU es pequeña o si se producen grandes ráfagas de tramas cortas.

Para habilitar Multilink PPP en una sola interfaz ISDN BRI o PRI, no es necesario definir un grupo rotativo de marcador por separado porque las interfaces ISDN son grupos rotatorios de marcador de forma predeterminada. Si no utiliza procedimientos de autenticación PPP, el servicio telefónico debe pasar la información de identificación de llamada.

Se requiere un número de umbral de carga. Para ver un ejemplo de configuración de Multilink PPP en una sola interfaz ISDN BRI, vea el *Ejemplo de Multilink PPP en una Interfaz ISDN* a continuación.

Cuando se configura Multilink PPP y se desea conectar un agrupamiento multilink indefinidamente, utilice el comando **dialer idle-timeout** para establecer un temporizador de inactividad muy alto. El comando **dialer-load threshold 1** no mantiene un agrupamiento de links múltiples *n* conectados indefinidamente, y el comando **dialer-load threshold 2** no mantiene un agrupamiento de links múltiples conectado indefinidamente.

Para habilitar el PPP de links múltiples en interfaces ISDN BRI o PRI múltiples, usted configura una interfaz rotativa de marcador y lo configura para PPP de links múltiples. A continuación, configure las BRI por separado y agréguelas a cada grupo rotatorio. Vea el *ejemplo de PPP de links múltiples en interfaces ISDN múltiples* a continuación.

Ejemplo de Multilink PPP en una Interfaz ISDN

El siguiente ejemplo habilita Multilink PPP en la interfaz BRI 0. Cuando se configura un BRI, no se requiere ninguna configuración de grupo rotatorio de marcador (la interfaz ISDN es un grupo rotatorio de forma predeterminada).

```
interface bri 0
ip address 171.1.1.7 255.255.255.0
 encapsulation ppp
```

```
 dialer idle-timeout 30
 dialer load-threshold 40 either
 dialer map ip 172.16.20.2 name Goleta 5551212
 dialer-group 1
 ppp authentication pap
 ppp multilink
```

Ejemplo de Multilink PPP en Varias Interfaces ISDN

El siguiente ejemplo configura varios BRI ISDN para que pertenezcan al mismo grupo rotativo de marcador para PPP de links múltiples. Utilice el comando **dialer rotary-group** para asignar cada una de las BRI ISDN a ese grupo rotativo de marcador que debe coincidir con el número de la interfaz del marcador (número 0 en este caso).

```
interface BRI0
 no ip address
 encapsulation ppp
 dialer rotary-group 0
!
interface BRI1
 no ip address
 encapsulation ppp
 dialer rotary-group 0
!
interface Dialer0
 ip address 172.16.20.1 255.255.255.0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 500
 dialer map ip 172.16.20.2 name Goleta broadcast 5551212
 dialer load-threshold 30 either
 dialer-group 1
 ppp authentication chap
 ppp multilink
```

Multichasis Multilink PPP

El PPP de links múltiples proporciona la capacidad de dividir y recombinar paquetes a un único sistema extremo a través de una canalización lógica (también llamada *agrupamiento*) formada por links múltiples. Multilink PPP proporciona ancho de banda a demanda y reduce la latencia de transmisión a través de los links WAN.

Multichassis Multilink PPP (MMP), por otra parte, proporciona la capacidad adicional para que los enlaces terminen en varios routers con diferentes direcciones remotas. MMP también puede manejar tráfico analógico y digital.

Esta funcionalidad está pensada para situaciones en las que hay grandes grupos de usuarios de marcado, en las que un solo servidor de acceso no puede proporcionar suficientes puertos de marcado. MMP permite a las empresas proporcionar un único número de marcado a sus usuarios y aplicar la misma solución a las llamadas analógicas y digitales. Esta función permite a los proveedores de servicios de Internet, por ejemplo, asignar un único número rotatorio ISDN a varios PRI ISDN en varios routers.

Para obtener una descripción completa de los comandos MMP a los que se hace referencia en este documento, consulte la *Referencia de Comandos de Soluciones de Marcado de Cisco*. Para

encontrar documentación de otros comandos que aparecen en este capítulo, utilice el índice principal de referencia de comandos, o busque en línea.

El MMP se soporta en las plataformas de las series 7500, 4500 y 2500 de Cisco y en las interfaces seriales sincrónicas, seriales asíncronas, ISDN BRI, ISDN PRI y Dialer.

MMP no requiere reconfiguración de los switches de la compañía telefónica.

Configuración

Los routers o los servidores de acceso se configuran para pertenecer a grupos de peers, llamados *grupos de pila*. Todos los miembros del grupo de pila son peers; los grupos de pila no necesitan un router principal permanente. Cualquier miembro del grupo de pila puede contestar llamadas provenientes de un único número de acceso, que normalmente es un grupo de búsqueda PRI ISDN. Las llamadas pueden llegar desde dispositivos de usuario remotos, como routers, módems, adaptadores de terminal ISDN o tarjetas de PC.

Una vez que se establece una conexión con un miembro de un *grupo de pila*, ese miembro es el propietario de la llamada. Si entra una segunda llamada del mismo cliente y un router diferente responde la llamada, el router establece un túnel y reenvía todos los paquetes que pertenecen a la llamada al router que posee la llamada. El proceso de establecer un túnel y reenviar llamadas a través de él al router que posee la llamada a veces se denomina *proyección del link PPP al call master*.

Si hay disponible un router más potente, se puede configurar como miembro del grupo de pila y los demás miembros del grupo de pila pueden establecer túneles y reenviar todas las llamadas a él. En tal caso, los otros miembros del grupo de pila sólo están respondiendo llamadas y reenviando el tráfico al router de *descarga* más potente.

Nota: Las líneas WAN de alta latencia entre los miembros del grupo de pila pueden hacer que el funcionamiento del grupo de pila sea ineficiente.

Las operaciones de gestión de llamadas, licitación y reenvío de Capa 2 de MMP en el grupo de pila proceden de la siguiente manera. También se muestra en la figura 16-10.

1. Cuando la primera llamada entra en el grupo de pila, el Router A contesta.
2. En la licitación, el router A gana porque ya tiene la llamada. El Router A se convierte en el *call-master* para esa sesión con el dispositivo remoto. El Router A también puede ser llamado el *host a la interfaz del agrupamiento maestro*.
3. Cuando el dispositivo remoto que inició la llamada necesita más ancho de banda, realiza una segunda llamada PPP de links múltiples al grupo.
4. Cuando entra la segunda llamada, el Router D la contesta e informa al grupo de la pila. El router A gana la licitación porque ya está manejando la sesión con ese dispositivo remoto.
5. El Router D establece un túnel al Router A y reenvía los datos PPP sin procesar al Router A.
6. El Router A vuelve a ensamblar y secuenciar los paquetes.
7. Si entran más llamadas al Router D y también pertenecen al Router A, el túnel entre A y D se amplía para manejar el tráfico agregado. El router D no establece un túnel adicional a A.
8. Si ingresan más llamadas y son contestadas por cualquier otro router, ese router también establece un túnel a A y reenvía los datos PPP sin procesar.
9. Los datos reensamblados se transmiten en la red corporativa como si todos hubieran pasado por un enlace físico.

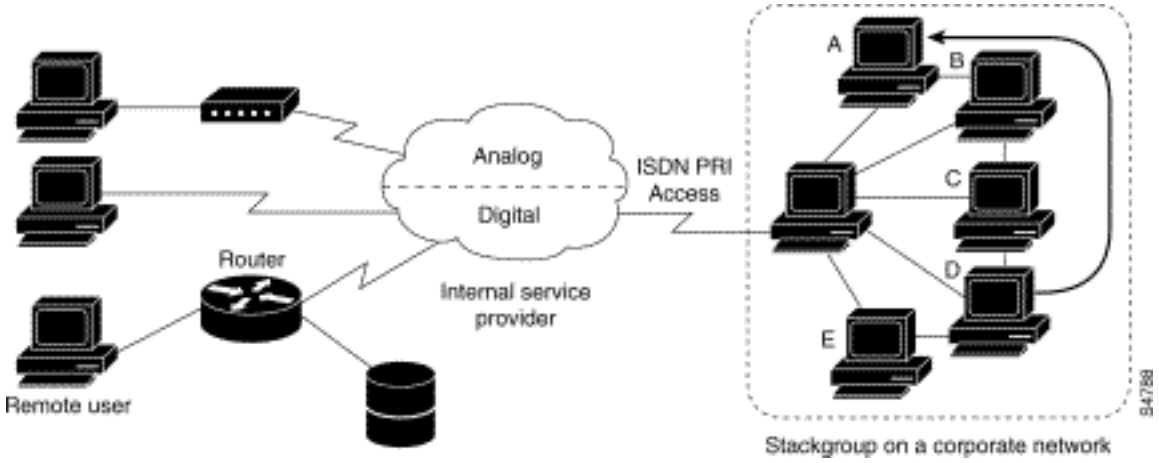

Figura 16-10: Escenario típico de PPP de links múltiples de varios chasis

A diferencia de la figura anterior, la figura 16-11 incluye un router de descarga. Acceda a los servidores que pertenecen a un grupo de pila para contestar llamadas, establecer túneles y reenviar llamadas a un router Cisco 4700 que gane la licitación y sea el call-master para todas las llamadas. El Cisco 4700 reensambla y vuelve a secuenciar todos los paquetes que ingresan a través del grupo de pila.

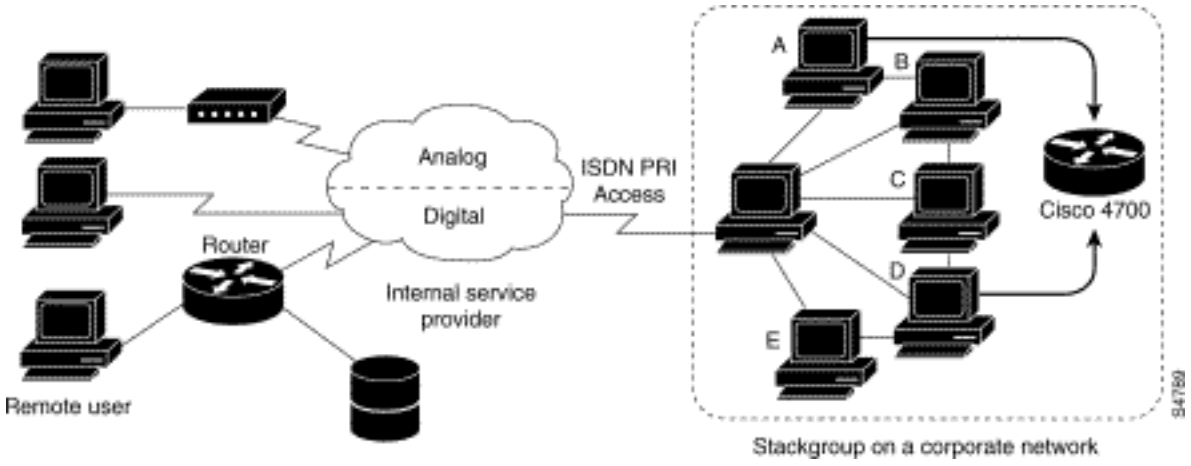

Figura 16-11: Multichassis Multilink PPP con un router de descarga como miembro de grupo de pila

Nota: Puede generar grupos de pila utilizando diferentes plataformas de servidor de acceso, switching y router. Sin embargo, los servidores de acceso universal como Cisco AS5200 no deben combinarse con ISDN. Esto sólo se debe hacer con servidores de acceso como la plataforma 4x00. Dado que las llamadas de la oficina central se asignan de forma arbitraria, esta combinación podría dar lugar a que se entregue una llamada analógica a un servidor de acceso solo digital, que no podría manejar la llamada.

La compatibilidad con MMP en un grupo de routers requiere que cada router esté configurado para soportar lo siguiente:

- PPP de links múltiples
- Protocolo de licitación de grupo de pila (SGBP)
- Plantilla virtual utilizada para clonar la configuración de la interfaz para soportar MMP

[Perfiles virtuales]

Virtual Profiles es una aplicación única de Point-to-Point Protocol (PPP) que puede crear y configurar una interfaz de acceso virtual dinámicamente cuando se recibe una llamada de marcado y desconectar la interfaz dinámicamente cuando finaliza la llamada. Los perfiles virtuales funcionan con PPP directo y con PPP de enlaces múltiples (MLP).

La información de configuración de una interfaz de acceso virtual de perfiles virtuales puede provenir de una interfaz de plantilla virtual, o de una configuración específica del usuario almacenada en un servidor de autenticación, autorización y contabilidad (AAA), o de ambos.

La configuración AAA específica del usuario utilizada por Virtual Profiles es la configuración *de interfaz* y se descarga durante las negociaciones LCP. Otra función, llamada Configuración por usuario, también utiliza la información de configuración obtenida de un servidor AAA. Sin embargo, la configuración por usuario utiliza la configuración de *red* (como listas de acceso y filtros de ruta) descargada durante las negociaciones de NCP.

Dos reglas rigen la configuración de la interfaz de acceso virtual por interfaces de plantilla virtual de Virtual Profiles y configuraciones AAA:

- Cada aplicación de acceso virtual puede tener, como máximo, una plantilla a partir de la cual clonar. Sin embargo, puede tener varias configuraciones AAA de las que clonar (información AAA de perfiles virtuales y configuración AAA por usuario, que a su vez podría incluir la configuración para varios protocolos).
- Cuando la plantilla virtual configura Perfiles virtuales, ésta tiene mayor prioridad que cualquier otra plantilla virtual.

Consulte la sección "Interoperabilidad con otras funciones de marcación de Cisco" a continuación para obtener una descripción de las posibles secuencias de configuración que dependen de la presencia o ausencia de MLP u otra función de acceso virtual que clona una interfaz de plantilla virtual.

Esta función se ejecuta en todas las plataformas de Cisco IOS que soportan MLP.

Para obtener una descripción completa de los comandos mencionados en esta sección, refiérase al capítulo "Comandos de Perfiles Virtuales" de la *Referencia de Comandos de Soluciones de Marcado* en el conjunto de documentación de Cisco IOS. Para localizar la documentación de otros comandos que aparecen en este capítulo, puede utilizar el índice maestro de referencia de comandos o buscar en línea.

Antecedentes

Esta sección presenta información general sobre perfiles virtuales para ayudarle a comprender esta aplicación antes de comenzar a configurarla.

Restricciones

Recomendamos que las direcciones sin numerar se utilicen en las interfaces de plantilla virtual para garantizar que no se crean direcciones de red duplicadas en las interfaces de acceso virtual.

Prerequisites

El uso de la información de configuración de interfaz AAA específica del usuario con perfiles

virtuales requiere que el router se configure para AAA y que el servidor AAA tenga pares AV de configuración de interfaz específica del usuario. Los pares AV relevantes (en un servidor RADIUS) comienzan de la siguiente manera:

```
cisco-avpair = "lcp:interface-config=...",
```

La información que sigue al signo igual (=) podría ser cualquier comando de configuración de la interfaz de Cisco IOS. Por ejemplo, la línea podría ser la siguiente:

```
cisco-avpair = "lcp:interface-config=ip address 200.200.200.200
255.255.255.0",
```

El uso de una interfaz de plantilla virtual con perfiles virtuales requiere que se defina una plantilla virtual específicamente para los perfiles virtuales.

Interoperabilidad con otras funciones de marcación de Cisco

Los perfiles virtuales interoperan con Cisco DDR, Multilink PPP (MLP) y marcadores como ISDN.

Configuración DDR de interfaces físicas

Los perfiles virtuales interoperan completamente con interfaces físicas en los siguientes estados de configuración DDR cuando no se configura ninguna otra aplicación de interfaz de acceso virtual:

- Los perfiles de marcador se configuran para la interfaz. El perfil del marcador se utiliza en lugar de la configuración de Perfiles virtuales.
- DDR no está configurado en la interfaz. Virtual Profiles anula la configuración actual.
- DDR heredado se configura en la interfaz. Virtual Profiles anula la configuración actual.

Nota: Si se utiliza una interfaz de marcador (incluido cualquier marcador ISDN), su configuración se utiliza en la interfaz física en lugar de en la configuración de Perfiles virtuales.

Efecto PPP de links múltiples en la configuración de la interfaz de acceso virtual

Como se muestra en la tabla 16-8, la configuración exacta de una interfaz de acceso virtual depende de los tres factores siguientes:

- Si los perfiles virtuales se configuran mediante plantilla virtual, AAA, por ambos o por ninguno de los dos. Estos estados se muestran como "VP VT only", "VP AAA only", "VP VT y VP AAA" y "No VP en absoluto", respectivamente, en la tabla.
- La presencia o ausencia de una interfaz de marcador.
- La presencia o ausencia de MLP. La etiqueta de columna "MLP" es un soporte para cualquier función de acceso virtual que admita MLP y clones de una interfaz de plantilla virtual.

En la tabla 16-8, "Multilink VT" significa que se clona una interfaz de plantilla virtual *si* se define una para MLP o una función de acceso virtual que utiliza MLP.

Tabla 16-8: Secuencia de clonación de configuración de perfiles virtuales

Configura	No	Marca	No MLP No	No MLP

ción de perfiles virtuales	Dialer de MLP	dor MLP	Dialer	Dialer
VP VT solamente	VP VT	VP VT	VP VT	VP VT
Solo VP AAA	(Multilink VT) VP AAA	(Multilink VT) VP AAA	VP AAA	VP AAA
VP VT y VP AAA	VP VT VP AAA	VP VT VP AAA	VP VT VP AAA	VP VT VP AAA
Ningún vicepresidente en absoluto	(Multilink VT)	Marcador	No se crea ninguna interfaz de acceso virtual.	No se crea ninguna interfaz de acceso virtual.

El orden de los elementos de cualquier celda de la tabla es importante. Cuando se muestra VP VT sobre VP AAA, significa que primero se clona la plantilla virtual de perfiles virtuales en la interfaz y después se aplica la configuración de interfaz AAA para el usuario. La configuración de la interfaz AAA específica del usuario se agrega a la configuración y reemplaza cualquier interfaz física en conflicto o cualquier comando de configuración de plantilla virtual.

Interoperabilidad con otras funciones que utilizan plantillas virtuales

Los perfiles virtuales también interactúan con las aplicaciones de acceso virtual que clonan una interfaz de plantilla virtual. Cada aplicación de acceso virtual puede tener, como máximo, una plantilla a partir de la cual clonar, pero puede clonar desde varias configuraciones AAA.

La interacción entre los perfiles virtuales y otras aplicaciones de plantillas virtuales es la siguiente:

- Si se habilita Virtual Profiles y se define una plantilla virtual para ella, se utiliza la plantilla virtual Virtual Profiles .
- Si sólo AAA configura perfiles virtuales (no se define ninguna plantilla virtual para perfiles virtuales), la plantilla virtual de otra aplicación de acceso virtual (VPDN, por ejemplo) se puede clonar en la interfaz de acceso virtual.
- Una plantilla virtual, si la hay, se clona en una interfaz de acceso virtual antes de la configuración AAA de perfiles virtuales o la configuración AAA por usuario. La configuración AAA por usuario, si se utiliza, se aplica en último lugar.

Terminology

En este capítulo se utilizan los siguientes términos nuevos o poco comunes:

Par AV: Un parámetro de configuración en un servidor AAA; parte de la configuración del usuario que el servidor AAA envía al router, en respuesta a las solicitudes de autorización específicas del usuario. El router interpreta cada par AV como un comando de configuración del router Cisco IOS

y aplica los pares AV en orden. En este capítulo, el término par AV hace referencia a un parámetro de configuración de interfaz en un servidor RADIUS.

Un par AV de configuración de interfaz para perfiles virtuales puede adoptar un formato como este:

```
cisco-avpair = "lcp:interface-config=ip address 1.1.1.1 255.255.255.255.0",
```

clonación: Crear y configurar una interfaz de acceso virtual mediante la aplicación de comandos de configuración desde una plantilla virtual específica. La plantilla virtual es el origen de la información genérica del usuario y de la información dependiente del router. El resultado de la clonación es una interfaz de acceso virtual configurada con todos los comandos de la plantilla.

interfaz de acceso virtual: Instancia de una interfaz virtual única que se crea dinámicamente y existe temporalmente. Las interfaces de acceso virtual se pueden crear y configurar de forma diferente mediante diferentes aplicaciones, como perfiles virtuales y redes de marcación privada virtual.

interfaz de plantilla virtual: Configuración de interfaz genérica para determinados usuarios o para un fin determinado, además de información dependiente del router. Esto toma la forma de una lista de los comandos de interfaz de Cisco IOS que se aplicarán a la interfaz virtual según sea necesario.

perfil virtual: Instancia de una interfaz de acceso virtual única que se crea dinámicamente cuando ciertos usuarios llaman y se desconecta dinámicamente cuando la llamada se desconecta. El perfil virtual de un usuario específico puede configurarse mediante una interfaz de plantilla virtual, una configuración de interfaz específica del usuario almacenada en un servidor AAA, o bien una interfaz de plantilla virtual y una configuración de interfaz específica del usuario desde AAA.

La configuración de una interfaz de acceso virtual comienza con una interfaz de plantilla virtual (si la hay), seguida de la aplicación de una configuración específica del usuario para la sesión de acceso telefónico del usuario concreto (si la hay).

Ejemplo Anotado de Negociación PPP

En este ejemplo, un ping muestra un link ISDN entre los routers *Montecito* y *Goleta*. Tenga en cuenta que, si bien no hay marca de tiempo en este ejemplo, se recomienda utilizar el comando de configuración global **service timestamps debug datetime msec**.

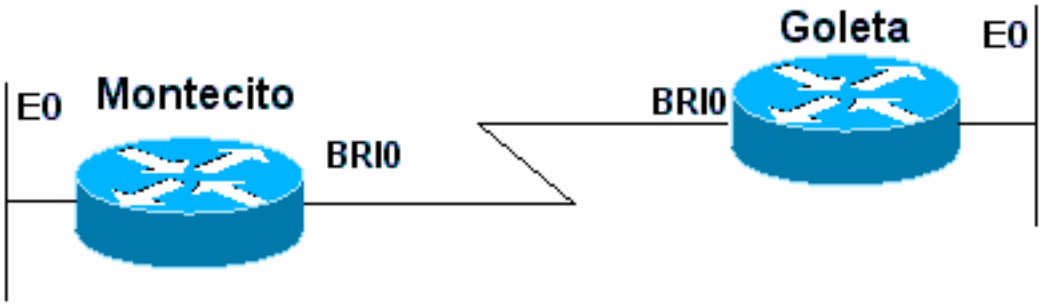

Figura 16-12: Router-ISDN-Router

Estas depuraciones se toman de *Montecito*; sin embargo, el debugging en *Goleta* se vería de la

misma manera.

Nota: Es posible que sus depuraciones aparezcan en un formato diferente. Este resultado es el formato de salida de depuración PPP anterior a las modificaciones introducidas en la versión 11.2(8) del IOS. Consulte el Capítulo 17 para ver un ejemplo de depuración PPP en las versiones más recientes del IOS.

```
Montecito#show debugging

  PPP:

    PPP authentication debugging is on

    PPP protocol negotiation debugging is on

A
 Montecito#ping 172.16.20.2


  Type escape sequence to abort.

  Sending 5, 100-byte ICMP Echoes to 172.16.20.2, timeout is 2 seconds:


B
 %LINK-3-UPDOWN: Interface BRI0: B-Channel 1, changed state to up

C
 ppp: sending CONFREQ, type = 3 (CI_AUTHTYPE), value = C223/5

C
 ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 29EBD1A7

D
 PPP BRI0: B-Channel 1: received config for type = 0x3 (AUTHTYPE)
value = 0xC223 digest = 0x5 acked

D
 PPP BRI0: B-Channel 1: received config for type = 0x5 (MAGICNUMBER)
value = 0x28FC9083 acked

E
 PPP BRI0: B-Channel 1: state = ACKsent fsm_rconfack(0xC021): rcvd id 0x65

F
 ppp: config ACK received, type = 3 (CI_AUTHTYPE), value = C223

F
 ppp: config ACK received, type = 5 (CI_MAGICNUMBER), value = 29EBD1A7

G
 PPP BRI0: B-Channel 1: Send CHAP challenge id=1 to remote

H
 PPP BRI0: B-Channel 1: CHAP challenge from Goleta

J
 PPP BRI0: B-Channel 1: CHAP response id=1 received from Goleta

K
 PPP BRI0: B-Channel 1: Send CHAP success id=1 to remote
```

```
L
 PPP BRI0: B-Channel 1: remote passed CHAP authentication.

M
 PPP BRI0: B-Channel 1: Passed CHAP authentication with remote.

N
 ipcp: sending CONFREQ, type = 3 (CI_ADDRESS), Address = 172.16.20.1

P
 ppp BRI0: B-Channel 1: Negotiate IP address: her address 172.16.20.2 (ACK)

Q
 ppp: ipcp_reqci: returning CONFACK.

R
 PPP BRI0: B-Channel 1: state = ACKsent fsm_rconfack(0x8021): rcvd id 0x25

S
 ipcp: config ACK received, type = 3 (CI_ADDRESS), Address = 172.16.20.1

T
 BRI0: install route to 172.16.20.2

U
 %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0: B-Channel 1,
changed state to up
```

A - El tráfico se genera para iniciar un intento de marcado.

B - La conexión se establece (depuraciones ISDN no utilizadas en este ejemplo).

Comenzar LCP:

C - *Montecito* envía solicitudes de configuración LCP para AUTHTYPE y MAGICNUMBER.

D - *Goleta* envía sus CONFREQ. Si el valor para MAGICNUMBER es el mismo que el valor enviado por *Montecito*, existe una alta probabilidad de que la línea se encuentre con loop.

E - Esto indica que *Montecito* ha enviado reconocimientos a los CONFREQ de *Goleta*.

F - *Montecito* recibe CONFACKs de *Goleta*.

Comenzar fase de autenticación:

G, H - *Montecito* y *Goleta* se impugnan mutuamente para la autenticación.

J - *Goleta* responde al desafío.

K, L - *Goleta* pasa con éxito la autenticación.

M - Mensaje de *Goleta* a *Montecito*: autenticación correcta.

Comienza la negociación NCP:

N, P: Cada router envía su dirección IP configurada en una CONFREQ.

Q, R - *Montecito* envía un CONFACK al CONFREQ de *Goleta*.

S - ? y viceversa.

T, U - Se instala una ruta de *Montecito* a *Goleta* y el protocolo en la interfaz cambia a "up", lo que indica que las negociaciones del NCP se han completado exitosamente.

Antes de llamar al equipo del TAC de Cisco Systems

Antes de llamar al centro de asistencia técnica Cisco Systems Technical Assistance Center (TAC), asegúrese de leer este capítulo y completar las acciones sugeridas para el problema del sistema.

Además, haga lo que se describe a continuación y documente los resultados para que podamos proporcionarle una mejor asistencia:

Para todos los problemas, recopile el resultado de **show running-config** y **show version**. Asegúrese de que el comando **service timestamps debug datetime msec** esté en la configuración.

Para los problemas de DDR, recopile lo siguiente:

- **show dialer map**
- **debug dialer**
- **debug ppp negotiation**
- **debug ppp authentication**

Si está involucrado ISDN, recopile:

- **mostrar estado isdn**
- **debug isdn q931**
- **debug isdn events**

Si hay módems involucrados, recopile:

- show lines
- show line [x]
- **show modem** (si hay módems integrados involucrados)
- **show modem version** (si hay módems integrados involucrados)
- **debug modem**
- **debug modem csm** (si hay módems integrados involucrados)
- **debug chat** (si se trata de un escenario DDR)

Si hay T1s o PRIs involucrados, recopile:

- **show controller t1**

Información Relacionada

- Guía de soluciones de marcado de Cisco IOS

- Información general de interfaces, controladores y líneas utilizadas para el acceso por marcación
- Ruteo Entre Líneas De Módem
- Configuración troncal del puerto serial y del T1/E1
- Diseño de Interredes DDR
- Decidir y prepararse para configurar DDR
- Configuración de DDRtitle
- Descripción General de la Tecnología PPP
- Diseño de Interredes ISDN
- Tipos de switch, códigos y valores de ISDN
- Aprovisionamiento de la línea ISDN
- Soporte Técnico y Documentación - Cisco Systems