Tecnología de marcación manual: Descripciones y explicaciones

Contenido

Introducción

Este capítulo introduce y explica algunas de las Tecnologías usadas en las redes de marcación manual. Usted encontrará las extremidades de la configuración y las interpretaciones de algunos de los **comandos show**, que son útiles para verificar la operación correcta de la red. Los procedimientos deTroubleshooting están fuera del alcance de este documento y se pueden encontrar en el documento titulado *resolviendo problemas el Dialup*.

Antes de comenzar

Convenciones

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

prerrequisitos

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. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). 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, la verificación, y el uso de los módems con los routeres Cisco.

Usando el comando modem autoconfigure

Si usted está utilizando la versión 11.1 del sistema operativo de Cisco internetwork (Cisco IOS) o más adelante, usted puede configurar a su router Cisco para comunicar con y para configurar su módem automáticamente.

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

1. Para descubrir el tipo de módem asociado a su router, utilice el **comando modem autoconfigure discovery line configuration**.
2. Cuando el módem se descubre con éxito, configure el módem automáticamente usando el **comando modem autoconfigure type modem-name line configuration**.

Si usted quiere visualizar la lista de módems para los cuales el router tenga entradas, utilice el módem-*nombre del* **modemcap de la demostración**. Si usted quiere cambiar un valor del módem que fue vuelto del **comando show modemcap**, utilice el **comando modemcap edit modem-name attribute value line configuration**.

Para toda la información sobre el uso de estos comandos, refiera a la *guía de configuración y al Dial Solutions Command Reference de las soluciones del dial de la documentación sobre Cisco IOS*.

Nota: No ingrese el **&W** en la entrada modemcap que se utiliza para el autoconfigure. Esto hace el NVRAM ser reescrita cada vez que un módem autoconfigure se realiza y destruirá el módem.

Establecimiento de una sesión Telnet inversa a un módem

Para los objetivos de hacer un diagnóstico, o configurar inicialmente el módem si usted está funcionando con el Cisco IOS Release 11.0 o Anterior, usted debe establecer a una sesión telnet reversa para configurar un módem para comunicar con un dispositivo de Cisco. Mientras usted bloquee la velocidad del módem del lado del equipo de terminal de datos (DTE), el módem comunicará siempre con el servidor de acceso o el router en la velocidad deseada. Refiera al cuadro 16-5 para la información sobre bloquear la velocidad del módem. Esté seguro que la velocidad del dispositivo de Cisco está configurada antes de publicar los comandos al módem vía una sesión telnet reversa. Una vez más refiera al cuadro 16-5 para la información sobre configurar la velocidad del servidor de acceso o del router.

Para configurar el módem para una sesión telnet reversa, utilice comando transport input telnet de configuración de línea. Para configurar a un grupo rotativo (en este caso, en el puerto 1), ingresa el comando line configuration **1. rotatorio** que pone estos comandos conforme al IOS de las causas de la configuración de línea de afectar un aparato a los módulos de escucha IP para las conexiones entrantes en los rangos de puertos que comienzan con los números base siguientes:

2000	Telnet Protocol
3000	Telnet Protocol con rotatorio
4000	Protocolo TCP sin procesar
5000	Protocolo TCP sin procesar con rotatorio
6000	Telnet Protocol, modo binario
7000	Telnet Protocol, modo binario con rotatorio
9000	Protocolo XRemote
10000	Protocolo XRemote con rotatorio

Para iniciar a una sesión telnet reversa a su módem, realice los pasos siguientes:

1. De su terminal, utilice el comando telnet ip-address 20yy donde está la dirección IP el *IP address de* cualquier active, interfaz conectada en el dispositivo de Cisco, y el yy es el número de línea con el cual el módem está conectado.Por ejemplo, el siguiente comando le conectaría con el puerto auxiliar en un Cisco 2501 Router con la dirección IP 192.169.53.52: **telnet 192.169.53.52 2001**. Generalmente, un comando telnet de esta clase puede ser publicado dondequiera encendido de la red, si puede **hacer ping la** dirección IP en la pregunta.**Nota:** En la mayoría de los routeres Cisco, el puerto 01 es el puerto auxiliar. En un Cisco Access Server, el puerto auxiliar es el último TTY +1. Como un ejemplo, el puerto auxiliar en 2511 es el puerto 17 (16 puertos TTY + 1). Utilice siempre el **comando show line exec** de encontrar el número del puerto auxiliar - determinado en las 2600 y 3600 Series, que utilizan los números del puerto NON-contiguos para acomodar los tamaños diversos del módulo del async.
2. Si se rechaza la conexión, podría indicar que no hay o módulo de escucha en la dirección especificada y puerto, o que alguien está conectada ya con ese puerto. Verifique el direccionamiento y el número del puerto de la conexión. También, aseegurese el comando modem inout o modem DTR-active, así como la **entrada de transporte toda**, aparece bajo configuración de línea para las líneas que son alcanzadas.Si usa la función rotativa, aseegurese el comando rotary n también aparece en la configuración de línea donde está el número n del grupo rotativo. Para marcar si alguien está conectada ya, el telnet al router y utilizar el comando show line *N.* busca un asterisco para indicar que la línea es funcionando. Aseegurese el CTS es alto y el DSR no es. Utilice el comando clear line n de desconectar a

la sesión en curso en el número del puerto N. Si la conexión todavía se rechaza, el módem pudo afirmar el Carrier Detect (CD) todo el tiempo. Desconecte el módem de la línea, establezca a una sesión telnet reversa, y después conecte el módem.

3. Después con éxito de hacer la conexión Telnet, ingrese EN y esté seguro las contestaciones del módem con la AUTORIZACIÓN.
4. Si el módem no es responsivo, refiera a la tabla siguiente.

El cuadro 16-1 abajo delinea las posibles causas de los síntomas del problema de conectividad del módem-a-router y describe las soluciones a esos problemas.

Cuadro 16-1: Ninguna Conectividad entre el módem y el router

Posibles Causas	Acciones sugeridas
El control del módem no se habilita en el servidor de acceso o 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 **RIisCD** en la columna de módem. Esto indica que el control del módem está habilitado en la línea del servidor de acceso o del router. Para una explicación de la **salida de línea de la demostración**, refiera a “usando los comandos Debug” en el capítulo 15. 2. Configure la línea para el control del módem usando el **comando modem inout line configuration**. El control del módem ahora se habilita en el servidor de acceso. Ejemplo: El siguiente ejemplo ilustra cómo configurar una línea para ambas llamadas entrante y saliente: `line 5` `modem inout` **Nota:** Esté seguro de utilizar el **comando modem inout**, y no el **comando modem dialin** mientras que la Conectividad del módem está en la pregunta. El u'ltimo comando permite que la línea valide las llamadas entrantes solamente. Las llamadas salientes serán rechazadas y será imposible establecer a una sesión telnet con el módem para configurarlo. Si usted quiere utilizar el **comando modem dialin**, haga tan solamente después que usted está seguro que está funcionando el módem correctamente.
El módem podía ser config	Ingrese **AT&FE1Q0** para volverlo a los valores predeterminados de fábrica y aseegurarse el módem se fija para producir eco los caracteres y vuelve la salida. El módem puede tener una sesión bloqueada. Utilice el “^U” para borrar la línea y el “^Q” para abrir el control de flujo (XON).

urado mal o tener una sesión bloqueada.	Verifique las configuraciones de paridad.
Cableado incorrecto	1. Marque el cableado entre el módem y el servidor de acceso o el router. Confirme que el módem está conectado con el puerto auxiliar en el servidor de acceso o el router con un cable rolled RJ-45 y un adaptador MMOD DB-25. Esta configuración del cableado es recomendada y soportada por Cisco para los puertos RJ-45. (Estos conectores típicamente se etiquetan “Modem.") 2. Utilice el **comando show line exec** de verificar que el cableado está correcto. Vea la explicación de la salida del **comando show line** en la sección titulada “usando los comandos Debug” en el capítulo 15.
Problema de hardware	1. Verifique que usted esté utilizando el cableado adecuado y que todas las conexiones son buenas. 2. Marque todo el hardware para el daño, incluyendo el cableado (cables dañados), los adaptadores (contactos flexibles), los puertos de servidor de acceso, y el módem. 3. Vea el capítulo 3, “resolviendo problemas el hardware y los problemas de arranque,” para más información sobre el Troubleshooting de hardware.

Usando los grupos rotativos

Para algunas aplicaciones, los módems en un router dado necesitan ser compartidos por un grupo de usuarios. El utilitario de discado de salida Cisco es un ejemplo de este tipo de aplicación. Básicamente, los usuarios conectan con un puerto que los conecte con un módem disponible. Para agregar una línea asincrónica a un grupo rotativo, ingrese simplemente *n* **rotatoria** donde está el número *n del* grupo rotativo en la configuración para la línea asincrónica. Refiera al ejemplo abajo.

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

La configuración de línea antedicha permitiría que los usuarios conectaran con el grupo rotativo ingresando **telnet 192.169.53.52 3001** para la telnet normal. Las alternativas incluyen los puertos 5001 para el TCP sin procesar, 7001 para la telnet binario (que las aplicaciones del utilitario de discado de salida Cisco), y 10001 para las conexiones Xremote.

Nota: Para verificar la configuración del utilitario de discado de salida Cisco, el doble hace clic en el icono de la utilidad de marcado de salida en la inferior derecha de la pantalla y presiona el botón de More>. Después, presione el botón de Ports> de la configuración. Aseegurese el puerto está en el rango 7000, si usa los grupos rotativos, y el rango 6000, si la utilidad de Dialout está apuntando un módem individual. Usted debe también habilitar el módem que abre una sesión el PC. Esto es hecha seleccionando la secuencia siguiente: **Modems-> de Start->Control Panel->** (elija su módem del discado de salida de Cisco) - >Properties->Connection->Advanced… - >Record un **archivo del registro**.

Interpretación de la salida de línea de la demostración

La salida del **comando show line line-number exec** es útil al resolver problemas una conexión del Access Server al módem o de router. Abajo está la salida 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 ocurren los problemas de conectividad, la salida importante aparece en el estado del módem y los campo de estado del hardware del módem.

Nota: El campo de estado del hardware del módem no aparece en la **salida de línea de la demostración** para cada plataforma. En ciertos casos, las indicaciones para los estados de la señal serán mostradas en el campo del estado del módem en lugar de otro.

Demostraciones cadenas típicas del estado del módem del cuadro 16-2 y del estado del hardware del módem de la salida del **comando show line**. También explica el significado de cada estado.

Cuadro 16-2: Módem y estados del hardware del módem en la salida de línea de la demostración

Estado del módem	Estado del hardware del módem	Significado
Ina	NoD	Éstos son los estados del módem apropiados

ctivo	SR DT R RTS CTS	para las conexiones entre un servidor de acceso o un router y un módem (cuando no hay llamada entrante). La salida de cualquier otra clase indica generalmente un problema.
Listo	-	Si el estado del módem está listo, en vez de la marcha lenta, considere el siguiente: 1. El control del módem no se configura en el servidor de acceso o el router. Configure el servidor de acceso o al router con el **comando modem inout line configuration**. 2. Una sesión existe en la línea. Utilice el **comando show users exec** y utilice el **comando clear line privileged exec** de parar la sesión si está deseado. 3. El DSR es alto. Hay dos razones posibles de esto: Problemas del cableado. Si su conector utiliza DB-25 el pin 6 y no tiene ningún pin 8, usted debe mover el pin a partir del 6 a 8 o conseguir el conector apropiado.El módem configurado para el DCD es siempre alto. El módem se debe configurar de nuevo para tener DCD alta solamente un CD(1). Esto se hace generalmente con el comando modem **&C1**, pero marca su documentación del módem para la sintaxis exacta para su módem. Si su software no soporta el control del módem, usted debe configurar la línea del Access Server con la cual el módem está conectado con el **comando no exec line configuration**. Borre la línea con el **comando clear line privileged exec**, inicie a una sesión telnet reversa con el módem, y configure de nuevo el módem de modo que el DCD sea alto solamente en el CD. Termine a la sesión telnet ingresando la **desconexión** y configure de nuevo la línea del Access Server con el comando exec line configuration.
Listo	noDSR del noCTS DTR	La cadena del noCTS aparece en el campo de estado del hardware del módem para una de las cuatro razones siguientes: 1. Se apaga el módem. 2. El módem no está conectado correctamente con el servidor de acceso.

	RTS (2)	Marque las conexiones de cableado del módem al servidor de acceso. 3. Cableado incorrecto (MDCE enrollado, o MDTE recto, pero sin los contactos movidos). La configuración de cableado recomendada se da anterior en esta tabla. 4. El módem no se configura para el control de flujo de hardware. Utilice el **comando no flowcontrol hardware line configuration** de inhabilitar el control de flujo de hardware en el servidor de acceso. Entonces habilite el control de flujo de hardware en el módem vía una sesión telnet reversa. (Consulte su documentación del módem y vea la sección el “establecer de una sesión telnet reversa a un módem” anterior en este capítulo.) Vuelva a permitir el control de flujo de hardware en el servidor de acceso con el **comando flowcontrol hardware line configuration**.
Listo	CTS DSR DTR RTS (2)	La cadena DSR (en vez de la cadena del noDSR) aparece en el campo de estado del hardware del módem para una de las razones siguientes: 1. Cableado incorrecto (MDCE enrollado, o MDTE recto, pero sin los contactos movidos). La configuración de cableado recomendada se da anterior en esta tabla. 2. El módem se configura para el DCD siempre arriba. Configure de nuevo el módem de modo que el DCD sea solamente alto en el CD. Esto se hace generalmente con el comando modem **&C1**, pero marca su documentación del módem para la sintaxis exacta para su módem. Configure la línea del Access Server con la cual el módem está conectado con el **comando no exec line configuration**. Borre la línea con el **comando clear line privileged exec**, inicie a una sesión telnet reversa con el módem, y configure de nuevo el módem de modo que el DCD sea alto solamente en el CD. Termine a la sesión telnet

		ingresando la **desconexión**. Configure de nuevo la línea del Access Server con el comando exec line configuration.
List o	CTS * DS R* DT R RTS (2)	Si esta cadena aparece en el campo de estado del hardware del módem, el control del módem no se habilita probablemente en el servidor de acceso. Utilice el **comando modem inout line configuration** de habilitar el control del módem en la línea. La información adicional en configurar el control del módem en un servidor de acceso o una línea del router se proporciona anterior en esta tabla.

(1) CD = detección de la portadora

(2) * al lado de una señal indica una de dos cosas: La señal ha cambiado dentro de los últimos segundos o la señal no está siendo utilizada por el método de control del módem seleccionado.

Recolección de información de rendimiento del módem

Esta sección explica los métodos para recopilar los Datos del rendimiento en los módems digitales MICA encontrados en la familia del Cisco AS5x00 de Access Servers. Los Datos del rendimiento se pueden utilizar para la análisis de tendencia y son útiles en los problemas de rendimiento del troubleshooting que pudieron ser encontrados. Cuando la mirada de los números presentó abajo, tenga en cuenta que la perfección no es posible en el mundo real. El índice de éxito posible de la llamada del módem (CSR) es una función de la calidad de los circuitos, del userbase del modem del cliente, y del conjunto de las modulaciones que son utilizadas. Un porcentaje típico de CSR para las llamadas V.34 es el 95%. Las llamadas del v.90 se pueden esperar para conectar con éxito el 92% del tiempo. Los descensos prematuros son probables suceder el 10% del tiempo.

Utilice los siguientes comandos de ganar una visión de conjunto del comportamiento del módem en el servidor de acceso:

- **muestre el módem**
- **muestre el modem summary**
- **muestre las conectar-velocidades del módem**
- **muestre el modem call-stats**

La siguiente información es útil al resolver problemas una conexión de módem individual o recopilando los datos para la análisis de tendencia:

- debug modem csm
- modem call-record terse
- muestran módem de Op. Sys. ()/AT@E1 (Microcom) MICA mientras que está conectado
- muestre el registro del módem para la sesión del interés después de la desconexión
- ANI (el número del llamador)
- Time Of Day
- Hardware/revisión de firmware del modem del cliente
- Información de interés del cliente (después de disconnect)-ATI6, ATI11, AT&V, AT&V1, y así sucesivamente

- Un expediente audio (archivo del .wav) de la tentativa del trainup del modem del cliente

En las secciones siguientes, los comandos serán explicados más lejos y algunas tendencias comunes serán discutidas.

Muestre el módem/el modem summary de la demostración

El comando show modem da una vista de los módems individuales. De estos números la salud de los módems individuales puede ser vista.

```
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 totales 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%
```

Cuadro 16-3: muestre los campos del módem

Campos	Descripciones
Llamadas entrante y saliente	Módem de las llamadas que marcan en y de los. • Uso - Porcentaje del uptime del sistema total que todos los módems son funcionando. • Succ - Totales de llamada conectados con éxito. • Fall - Totales de llamada que no conectaron con éxito. • Resultado - Módems totales disponibles para el uso en el sistema.
Busied hacia fuera	El número total de épocas los módems fue tomado el Out Of Service con el **comando modem busy** o el **comando modem shutdown**.
Dial fallado	Número total de tentativas que los módems no colgaron para arriba o había no hay tono de marcado.
Ninguna American National Standard	El número total de tono de timbre de llamada de las épocas fue detectado, pero las llamadas no fueron contestadas por un módem.
El PCT del Succ.	Porcentaje de la conexión satisfactoria de los módems disponibles totales.

Muestre la salida del modem call-stats

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

Cuadro 16-4: muestre los campos del modem call-stats

rmt Link	Esta demostración que la corrección de errores estaba en efecto, y la llamada fueron colgadas para arriba por el sistema del cliente asociado al módem remoto.
hos tDr op	Esto muestra que la llamada fue colgada para arriba por el sistema del host IOS. Algunas razones comunes incluyen: tiempo de inactividad, un circuito claro de la compañía telefónica, o un termreq PPP LCP del cliente. La mejor manera de determinar la razón de la caída para arriba está usando el registro de llamada del módem conciso o las estadísticas AAA.

Los otros motivos de desconexión deben alcanzar hasta menos el de 10% del total.

Muestre la salida de las Conectar-velocidades del módem

```
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
```

Espere ver una distribución de las velocidades V.34. Debe haber un pico en 26.4, si el Señalización asociada al canal (CAS) del uso del T1s. Para el T1s ISDN (PRI), el pico debe estar en 31.2. También, busque algún K56Flex, las velocidades V.90. Si no hay conexiones del v.90 puede haber un problema de la topología de red.

Comprensión del comando conciso del registro de llamada del módem (11.3AA/12.0T)

Bastante que un comando exec, esto es comando configuration puesto en el nivel del sistema del servidor de acceso en la pregunta. Cuando desconexiones de un usuario, un mensaje similar a las visualizaciones siguientes:

```
*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 modem operational-status del exec command show muestra los parámetros actuales (o la mayoría del reciente) referente a la conexión de módem.

La entrada de documentación para este comando se encuentra en el *Dial Solutions Command Reference del Cisco IOS Release 12.0*. **el modem operational-status de la demostración** está solamente para los módems MICA. El comando equivalente para los módems Microcom es **módem en-MODE/AT@E1**. Utilice el **comando modem at-mode <slot>/<port>** de conectar con el módem, después publique el comando de **AT@E1**. La documentación completa para el **comando modem at-mode** se puede encontrar en la *guía de configuración de software del Cisco AS5300*, y la documentación para el comando de **AT@E1** está en *EN el comando set y el resumen de registro para la referencia de comandos de los módulos del módem Microcom*.

Utilice los pasos siguientes para determinar en los cuales los módems un usuario están viniendo adentro:

1. Publique el comando show user y busque el TTY con el cual están conectados.
2. Utilice el comando show line y busque los slots de módem/número de puerto.

Recopilar los datos de rendimiento del lado del cliente

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

- modelo/versión de firmware del hardware del cliente (alcanzable con el comando ATI3I7 en el módem del cliente)
- motivos de desconexión cliente-señalados (uso **ATI6** o **AT&V1**)

La otra información disponible en el extremo del cliente incluye modemlog.txt y ppplog.txt PC. Usted debe configurar específicamente su PC para generar estos archivos.

Analice los Datos del rendimiento

Una vez que usted ha recogido y ha entendido los Datos del rendimiento para su sistema de módem, usted necesita mirar cualesquiera modelos y componente restantes que puedan necesitar la mejora.

Problemas con los módems del servidor determinado

Utilice el **módem de la demostración** o **muestre el modem call-stats** para identificar cualquier módems con anormalmente las altas velocidades de la falla de preparación de conexión o de las malas tarifas de la desconexión (MICA). Si los pares de módems adyacentes están teniendo problemas, el problema es probable colgado/absolutamente DSP. Utilice **copy flash modem al** HMM afectado para recuperarse. Aseegurese los módems están funcionando con la última versión del portware. Para verificar que todos los módems estén configurados correctamente, utilice el configuration command modem **autoconfigure la mica/el microcom_server del tipo** en la configuración de línea. Para aseegurarse los módems autoconfigured siempre que una llamada se cuelgue para arriba, utilizan el **confmodem del debug del** comando exec. Para reparar los módems que se configuran mal gravemente, usted puede necesitar establecer a una sesión telnet reversa.

Problemas con DS0s determinado

Los problemas del DS0 son raros, pero posibles. Para localizar DS0s que funciona incorrectamente, utilice el comando show controller t1 call-counters y busque cualquier DS0s con

anormalmente las Llamadas totales altas y TotalDuration anormalmente bajo. Para apuntar sospechó DS0s, usted puede necesitar ocupado hacia fuera el otro DS0s con el **servicio dsl del** configuration command ISDN**, busyout del ds0** bajo interfaz serial para el T1. La salida del **show controller t1 call-counters** parece esto:

```
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 sospechado en este caso.

Tendencias adicionales del campo común

Abajo están algunas de las tendencias mas comunes vistas por el TAC de Cisco.

1. Malos trayectos del circuitoUsted puede ser que consiga los malos trayectos del circuito con el Public Switched Telephone Network (PSTN) si usted tiene los problemas siguientes:las llamadas de larga distancia tienen problemas, pero el local no hace (o vice versa)las llamadas a veces del día tienen problemaslas llamadas de los intercambios remotos específicos tienen problemas
2. Problemas con las llamadas de larga distanciaSi no está funcionando su servicio de larga distancia correctamente o en absoluto (solamente el servicio local está muy bien):Esté seguro que la Línea digital conecta en un switch digital, no un banco de canales.Dé instrucciones las compañías telefónicas para examinar los trayectos del circuito usados para la larga distancia.
3. Problemas con las llamadas de las áreas de llamada específicas.Si las llamadas de las regiones geográficas/de los intercambios específicos tienden a tener problemas, usted debe obtener la topología de red de la compañía telefónica.Si se requieren las conversiones de analógico a digital múltiples, el módem V.90/K56flex conecta no será posible y el V.34 puede ser degradado algo. Las conversiones de analógico a digital se requieren en las áreas que son servidas por los switches digitales NON-integrados o por el Switches analogico.

Operaciones ISDN

El ISDN refiere a un conjunto de los servicios digitales que están disponibles para los usuarios finales. El ISDN implica la numeración de la red telefónica para poder proporcionar la Voz, los datos, el texto, los gráficos, la música, el vídeo, y el otro material fuente a los usuarios finales de un solo, terminal del usuario final sobre el cableado del teléfono existente. Los autores del ISDN se imaginan una red global como la actual red telefónica, pero con la transmisión digital y una variedad de nuevos servicios.

El ISDN es un esfuerzo para estandardizar los servicios para suscriptores, usuario/las interfaces de la red, y red y las capacidades entre redes. Estandardizar los servicios para suscriptores intenta asegurar un nivel de compatibilidad internacional. Estandardizar el usuario/la interfaz de la red estimula el desarrollo y la comercialización de estas interfaces por los fabricantes de tercera persona. Estandardizando las ayudas de la red y de las capacidades entre redes alcance la meta del conectividad en todo el mundo asegurándose de que las redes ISDN comunican fácilmente el uno con el otro.

Las aplicaciones ISDN incluyen las aplicaciones de imagen de alta velocidad (tales como facsímil

del grupo IV), las líneas telefónicas adicionales en los hogares para servir la industria de la teleconmutación, la transferencia de archivos de alta velocidad, y la videoconferencia. Voz, por supuesto, isl también una aplicación popular para el ISDN.

El mercado de acceso local se está dividiendo para arriba entre diversas Tecnologías. En las áreas cuando sea nuevo menos tecnologías costosas tales como DSL y cable están disponibles el mercado local se están moviendo lejos del ISDN. Los negocios, sin embargo, continúan utilizando el ISDN bajo la forma de PRI T1/E1 para llevar una gran cantidad de datos o para proporcionar el acceso del dialin del v.90.

Componentes de ISDN

Los Componentes de ISDN incluyen las terminales, los adaptadores de terminal (TA), los dispositivos de terminación de la red, el equipo de terminación de línea, y el equipo de la terminación del intercambio. Las terminales ISDN vienen en dos tipos. Las terminales especializadas ISDN se refieren como tipo 1 del equipo de terminal (TE1). Las terminales del no ISDN, tales como DTE que preceden los estándares de ISDN, se refieren como tipo-2 del equipo de terminal (TE2). Los TE1 conectan con la red ISDN a través de un link digital de cuatro cables, de conductor doble retorcido. Los TE2 conectan con la red ISDN a través de un adaptador de terminal. El ISDN TA puede ser un dispositivo autónomo o una tarjeta dentro del TE2. Si el TE2 se implementa como dispositivo autónomo, conecta con el TA vía una interfaz de capa física estándar. Los ejemplos incluyen EIA/TIA-232-C (antes RS-232-C), el V.24, y el V.35.

Más allá de los dispositivos TE1 y TE2, el punto de conexión siguiente en la red ISDN es el tipo 1 de la terminación de la red (NT1) o dispositivo del tipo-2 de la terminación de la red (NT2). Éstos son los dispositivos de terminación de la red que conectan al suscriptor de cuatro cables que ata con alambre con el local loop de dos hilos convencional. En Norteamérica, el NT1 es un dispositivo del Customer Premises Equipment (CPE). En la mayoría de las otras partes del mundo, el NT1 es parte de que la red proporcionó por el portador. El NT2 es un dispositivo más complicado, encontrado típicamente en los intercambios de central privada digitales (PBX), que lleva a cabo los servicios de la concentración de la capa 2 y 3 funciones del protocolo y. Un dispositivo NT1/2 también existe; es un único dispositivo que combina las funciones de un NT1 y de un NT2.

Varios puntos de referencia se especifican en el ISDN. Estos puntos de referencia definen las interfaces lógicas entre las agrupaciones funcionales tales como TA y los NT1. Los puntos de referencia ISDN incluyen el siguiente:

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

Lo que sigue es una configuración de ISDN de ejemplo. Esta muestra muestra tres dispositivos asociados a un switch ISDN en la oficina central. Dos de estos dispositivos son ISDN-compatibles, así que pueden ser asociados a través de un punto de referencia S a los dispositivos NT2. Los terceros attaches del dispositivo (un estándar, un teléfono del no ISDN) a través del punto de referencia R a un TA. Ninguno de estos dispositivos podrían también asociar a un dispositivo NT1/2, que substituiría el NT1 y el NT2. Y, aunque no se muestren, las estaciones de usuario similares se asocian al switch ISDN del extremo derecho.

Una configuración de ISDN de ejemplo

```
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 del Basic Rate Interface (BRI) ISDN ofrece dos canales B y uno canal D (2B+D). El servicio del Canal B BRI actúa en 64 kbps y se significa llevar los datos del usuario; El servicio del canal D BRI actúa en 16 kbps y se significa llevar el control y la información de señalización, aunque pueda soportar la transmisión de datos del usuario en determinadas circunstancias. El protocolo de señalización del canal D comprende las capas 1 a 3 del OSI Reference Model. El BRI también prevé el control de alineación de tramas y el otro de arriba, trayendo su velocidad total de bit a 192 kbps. La especificación de la capa física BRI está sector de normalización de telecomunicaciones de la Unión internacional de telecomunicaciones (ITU-T; antes el Comité de consulta para la telegrafía y telefonía internacional [CCITT]) I.430.

El servicio de la Interfaz de velocidad primaria ISDN (PRI) ofrece 23 canales B y uno canal D en Norteamérica y Japón, rindiendo una velocidad total de bit de 1.544 Mbps (el PRI canal D se ejecuta en 64 kbps). El ISDN PRI en Europa, Australia, y otras partes del mundo proporciona 30 B más un 64-kbps canal D y una tarifa de la interfaz total del 2.048 Mbps. La especificación de la capa física PRI es ITU-T I.431.

Layer 1

La Capa física ISDN (formatos de trama de la capa 1) diferencia dependiendo de si la trama es saliente (de la terminal a la red) o entrante (de la red a la terminal). Ambas interfaces de capa física se muestran en el cuadro 16-1.

Cuadro 16-1: Formatos de la trama de capa física ISDN

Las tramas son 48 bits de largo, cuyo 36 bits representan los datos. Los bits de una trama de capa física ISDN se utilizan como sigue:

- F - Provee sincronización.
- L - Ajusta el valor en bits medio.
- E - Utilizado para la resolución de contención cuando varias terminales en un bus pasivo afirman para un canal.
- A - Activa los dispositivos.
- S - No asignado.
- B1, B2, y D - Para los datos del usuario.

Los dispositivos del usuario del ISDN múltiple se pueden asociar físicamente a un circuito. En esta configuración, las colisiones pueden resultar si dos terminales transmiten simultáneamente. Por lo tanto, el ISDN proporciona las características para determinar la contención del link. Cuando NT recibe una D mordida del TE, produce eco detrás el bit en la posición siguiente del E-bit. El TE espera que el bit siguiente E sea lo mismo que su bit transmitido último D.

Las terminales no pueden transmitir en canal D a menos que primero detecten un número específico de unos (indicación sin señal) correspondiente a una prioridad preestablecida. Si el TE detecta un bit en el canal de la generación de eco (e) que es diferente de sus bits D, debe parar el transmitir inmediatamente. Esta técnica simple se asegura de que solamente una terminal pueda transmitir su mensaje D al mismo tiempo. Después de la transmisión acertada del mensaje D, la terminal tiene su prioridad reducida por ser requerido para detectar los más continuos antes de transmitir. Las terminales no pueden aumentar su prioridad hasta que todos los otros dispositivos en la misma línea hayan tenido una oportunidad de enviar un mensaje D. Las conexiones de teléfono tienen prioridad más alta que todos los otros servicios, y la información de señalización tiene una prioridad más alta que información de no señalización.

Capa 2

La capa 2 del protocolo de señalización ISDN es procedimiento de acceso a link en canal D, también conocido como LAPD. El LAPD es similar al High-Level Data Link Control (HDLC) y al link de Proceso de Acceso a link Balanceado (LAPB). Mientras que la extensión de la abreviatura LAPD indica, se utiliza a través del canal D para asegurarse de que los flujos del control y de información de señalización y se recibe correctamente. El formato de trama LAPD (véase el cuadro 16-2) es muy similar al del HDLC y, como el HDLC, del LAPD utiliza supervisor, la información, y las tramas sin numeración. El protocolo LAPD se especifica formalmente en ITU-T Q.920 y ITU-T Q.921.

Cuadro 16-2: Formato de trama LAPD

El indicador y los Campos de control LAPD son idénticos a los del HDLC. El campo de dirección LAPD puede ser 1 o 2 bytes de largo. Si el bit de dirección extendido del primer byte se fija, el direccionamiento es 1 byte; si no se fija, el direccionamiento es 2 bytes. El primer byte del campo de dirección contiene el Identificador del punto de acceso al servicio (SAPI), que identifica el portal en el cual proporcionan los servicios LAPD para acodar 3. El bit C/R indica si la trama contiene un comando o una respuesta. El campo del identificador de punto final de terminal (TEI) identifica una sola terminal o los Terminales múltiples. Un TEI todos los indica un broadcast.

Capa 3

Dos especificaciones de la capa 3 se utilizan para la señalización ISDN: ITU-T (antes CCITT) I.450 (también conocido como ITU-T Q.930) y ITU-T I.451 (también conocido como q.931 ITU-T). Junto, conexiones individuales, con conmutador de circuito, y conmutadas por paquetes del soporte de estos protocolos. Especifican, incluyendo la CONFIGURACIÓN, CONECTAN, LIBERAN a una variedad de establecimiento de llamada, de terminación de llamada, de información, y de mensajes misceláneos, INFORMACIÓN DEL USUARIO, CANCELACIÓN, ESTATUS, y DESCONEXIÓN.

Estos mensajes son funcionalmente similares a ésos proporcionados por el protocolo x.25 (véase el capítulo 19, “resolviendo problemas las conexiones X.25,” para más información). El cuadro 16-3, de ITU-T I.451, muestra las etapas típicas de un ISDN Circuit-Switched Call.

Cuadro 16-3 etapas del ISDN Circuit-Switched Call

Interpretando la demostración isdn status output

Para descubrir cuál está la condición actual de la conexión ISDN entre el router y el Switch de la

compañía telefónica, utilice el comando show isdn status. Las dos clases de interfaces que sean soportadas por este comando son el BRI y el 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
```

Isdn status de la demostración del cuadro 16-5:- para el BRI

Campo	Significación
Estado de la capa 1: DESACTIVADO	Esto indica que la interfaz BRI no está considerando una señal en la línea. Hay cinco razones posibles de esta condición. • La interfaz BRI es apaga. Marque la configuración para el comando shutdown bajo interfaz BRI, o busque administrativo abajo una indicación del **comando show interface**. Utilice la utilidad de configuración y ingrese **ningún apagan** bajo interfaz BRI. Ingrese el comando clear interface bri en el prompt exec de aseegurarse la interfaz BRI se recomienza. • Un problema existe con el cableado. Usted necesitará substituir el cable. Aseegurese le utilizar un cable continuo RJ-45. Para marcar el cable, lleve a cabo los extremos del cable RJ-45 de lado a lado. Si los contactos están en la misma orden, el cable es continuo. Si se invierte la orden de los pines, se rueda el cable. Reemplazar el cable • El puerto del ISDN BRI de un router pudo requerir un dispositivo NT1. En el ISDN, el NT1 es un dispositivo que proporciona la interfaz entre el Customer Premises Equipment y el equipo de Switching de la oficina central. Si el router no tiene un NT1 interno, obtenga y conecte un NT1 con el puerto BRI. Aseegurese que el BRI o el adaptador de terminal está asociado al puerto S/T del NT1. Refiera a la documentación del fabricante para verificar la operación correcta del externo NT1. • La línea no pudo funcionar. Entre en contacto el portador para confirmar la operación de la conexión y para verificar

	las configuraciones del tipo de switch. • Aseegurese al router está funcionando correctamente. Si hay defectuoso o hardware en mal funcionamiento, substituya cuanto sea necesario.
Estado de la capa 2: Estado = TEI_ASSIGNED	Marque el ajuste de tipo de switch y el SPIDS. La configuración de switch ISDN específico de la interfaz reemplazará la configuración de switch global. El Estado de SPID indicará si el Switch validó el SPIDS (válido o inválido). Entre en contacto su proveedor de servicio para verificar la configuración configurada en el router. Para cambiar las configuraciones SPID, utilice el comando interface configuration del **spidn isdn**. Donde está 1 o 2 *n*, dependiendo del canal en la pregunta. No utilice la **ninguna** forma de este comando de 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 cual usted ha inscrito. Este valor es asignado por el proveedor del servicio ISDN y es generalmente un número de teléfono 10-digit con los dígitos adicionales. `ldn`El Número de directorio local (LDN) (opcional), que es un número de 7 dígitos asignó por el proveedor de servicio. El Switch en el mensaje de CONFIGURACIÓN entrante entrega esta información. Si usted no incluye el acceso del directorio local al Switch se permite, pero el otro canal B puede no poder recibir las llamadas entrantes. Para ver las negociaciones de la capa 2 entre el Switch y el router, utilice el **debug isdn q921 del** comando privileged exec. Los debugs q921 se documentan en la *referencia del comando Debug*. Los debugs confían pesadamente en los recursos de la CPU, así que tenga cuidado al emplearlos.

```
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 trabaja ni muestra el PRI, intente usar el **comando show isdn service**. Aseegurese el **comando pri-group** aparece en la configuración bajo el regulador T1/E1 en la configuración. Si el comando no está presente, configure el regulador con el **comando pri-group**.

Lo que sigue es un ejemplo de una configuración para un router Cisco con un controlador de T1/PRI canalizado:

```
controller t1 0
```

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

Cuadro 16-6: muestre el isdn status para el PRI

Campo	Significación
Estado de la capa 1: DESACTIVADO	Esto indica que la interfaz PRI no está considerando el T1/E1 el enmarcar en la línea. Considere las posibles causas siguientes para esta condición: • La interfaz PRI es apaga. Marque la configuración para el comando shutdown bajo interfaz serial0:23 o busque administrativo abajo una indicación del **comando show interface**. Utilice la utilidad de configuración y ingrese **ningún apagan** bajo interfaz en la pregunta. Ingrese el comando clear controller T1/E1 n en el prompt exec de aseegurarse la interfaz PRI se recomienza. • Un problema existe con el cableado. Usted necesitará substituir el cable. Aseegurese le utilizar un cable continuo RJ-45. Para marcar el cable, lleve a cabo los extremos del cable RJ-45 de lado a lado. Si los contactos están en la misma orden, el cable es continuo. Si se invierte la orden de los pines, se rueda el cable. Reemplazar el cable • La línea no pudo funcionar. Entre en contacto el portador para confirmar la operación de la conexión, y para verificar las configuraciones del tipo de switch. • Aseegurese al router está funcionando correctamente. Si hay defectuoso o hardware en mal funcionamiento, substituya cuanto sea necesario.
Estado de la capa 2: Estado = TEI_ASSIGNED	Marque el ajuste de tipo de switch. La configuración de switch ISDN específico de la interfaz reemplazará la configuración de switch global. Verifique el T1/E1 se configura para hacer juego el Switch del proveedor (los problemas T1/E1 se discuten en el capítulo 15). Para ver las negociaciones de la capa 2 entre el Switch y el router, utilice el **debug isdn q921 del** comando privileged exec. Los debugs q921 se documentan en la *referencia del comando Debug*. Los debugs confían pesadamente en los recursos de la CPU, así

	que tenga cuidado al emplearlos.
El número de llamadas/ de Bloqueos de control de llamada funcionando/total afectó un aparato los bloqueos de control de la llamada ISDN	Estos números indican cuántas llamadas están en curso, y el número de recursos que se afectan un aparato para soportar esas llamadas. Si el número de CCB afectados un aparato es más alto que el número de CCB que son utilizados, considere que pudo haber un problema en liberar los CCB. Aseegurese allí son CCB disponibles para las llamadas entrantes.

On-Demand Routing del dial: Operaciones de la interfaz del dialer

El On-Demand Routing del dial (DDR) es un método para la provisión de conectividad WAN sobre una base económica, del según se necesite, como link principal o como respaldo para un link de los seriales sin marcado.

Una interfaz del dialer se define como cualquier interfaz del router capaz de poner o de recibir una llamada. Este término genérico debe ser distinguido de la **interfaz del dialer del** término (con una D) capital, que refiere 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 marcador X. de la interfaz. De esta punta adelante, salvo que se indique lo contrario, utilizaremos el marcador del término en su sentido genérico.

La configuración de la interfaz del dialer viene en dos sabores: correspondencia basada del marcador (designada a veces el DDR heredado), y Perfiles de marcado. Qué método usted utiliza depende de las circunstancias bajo las cuales usted necesita la Conectividad del dial. La correspondencia basada DDR del marcador primero fue introducida en la versión de IOS 9.0, los Perfiles de marcado en la versión de IOS 11.2.

Accionar un dial

En su corazón, el DDR es apenas *paquetes interesantes de una* extensión de ruteo en donde se rutea a una interfaz del dialer, accionando un intento de marcado. Las secciones siguientes explican los conceptos implicados en la definición del tráfico interesante y explican la encaminamiento usada para las conexiones DDR.

Paquetes interesantes

Interesante es el término usado para describir los paquetes o traficar que o accionarán un intento

de marcado o, si un link de marcado es ya activo, reajustará el temporizador de inactividad en la interfaz del dialer. Para que un paquete sea considerado interesante:

- el paquete debe cumplir los criterios del “permiso” definidos por una lista de acceso
- la lista de acceso se debe referir por la marcador-lista o el paquete debe estar de un protocolo que sea permitido universal por la marcador-lista
- la lista del dialer se debe asociar a una interfaz del dialer por medio de un marcador-grupo

Los paquetes nunca se consideran automáticamente ser interesantes (por abandono). Las definiciones de paquete interesante se deben declarar explícitamente en un router o una configuración del Access Server.

Grupo de dialer

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

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

El número de grupo es el número del grupo de acceso de dialer a quien la interfaz específica pertenece. Definen a este grupo de acceso con el **comando dialer-list**. Los valores aceptables son no-cero, enteros positivos entre 1 y 10.

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

Paquetes que hacen juego el activador del grupo del dialer especificado un pedido de conexión.

Evalúan a la dirección destino del paquete contra la lista de acceso especificada en el comando associated dialer-list. Si pasa, o se inicia una llamada (si no se ha establecido ninguna conexión ya) o se reajusta el temporizador de inactividad (si una llamada está conectada actualmente).

Lista del dialer

El protocolo utiliza al **comando dialer-list global configuration** de definir una lista del dialer de DDR para controlar la marca, o por una combinación del protocolo y de la lista de acceso. Los paquetes interesantes son los que hacen juego el permiso del nivel del protocolo o que son permitidas por la lista en el **comando dialer-list**: **dialer-list dialer-group protocol protocol-name {permit | niegue | list access-list-number | acceso-grupo}**

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

el protocolo-nombre es una de las palabras claves de protocolo siguientes: APPLETALK, Bridge, clns, clns_es, clns_is, DECNet, decnet_router-L1, decnet_router-L2, decnet_node, IP, IPX, vides, o XNS.

acceso de los permisos del **permiso a un** protocolo completo.

niegue niega el acceso a un protocolo completo.

la lista especifica que una lista de acceso será utilizada para definir un granularity más fino que un protocolo completo.

access-list-number - Números de lista de acceso especificados en cualquier DECNet, Banyan VINES, IP, Novell IPX, o estándar XNS o listas de acceso ampliadas, incluyendo las Listas de acceso y los tipos de Bridging del punto de acceso del servicio extendido del Novell IPX (SAP). Vea el cuadro 16-7 para los tipos y los números soportados de la lista de acceso.

nombre de la lista de filtros del acceso-*grupo* usado en los **comandos clns filter-set y clns access-group**.

Cuadro 16-7: Enumeración de la lista de acceso por el protocolo

Tipo de la lista de acceso	Rango del número de lista de acceso (decimal)
AppleTalk	600-699
Banyan VINES (estándar)	1-100
Banyan VINES (extendido)	101-200
DECNet	300-399
IP (estándar)	1-99
IP (extendido)	100-199
Novell IPX (estándar)	800-899
Novell IPX (ampliado)	900-999
Uso de puente transparente	200-299
XNS	500-599

Lista de acceso

Para cada Networking Protocol que debe ser enviada a través de la conexión de marcado, una lista de acceso puede ser configurada. Con objeto del control de costos, es generalmente deseable configurar una lista de acceso para evitar que cierto tráfico, tal como actualizaciones de ruteo, sacar a colación o continúe una conexión. Observe que cuando creamos las Listas de acceso con el fin de la definición interesante y del tráfico no interesante, nosotros no están declarando que los paquetes no interesantes no pueden cruzar el link de marcado. Apenas estamos indicando que no reajustarán el temporizador de inactividad, ni sacarán a colación una conexión en sus los propio. Mientras la conexión de marcado esté para arriba, los paquetes no interesantes todavía serán permitidos fluir a través del link.

Por ejemplo, un EIGRP corriente del router como su Routing Protocol puede tener una lista de acceso configurada para declarar los paquetes EIGRP sin interés 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 pudieron cruzar el link

de marcado. Recuerde que para cualquier protocolo, el comportamiento predeterminado en ausencia de una declaración del **access-list permit** es negar todo el tráfico. Si no hay lista de acceso y ningún **comando dialer-list** permitiendo el protocolo, después que el protocolo será sin interés. En la práctica real, si no hay lista del dialer para un protocolo, esos paquetes no fluirán a través del link en absoluto.

Ejemplo - Juntándolo todo

Con todos los elementos en el lugar, usted puede examinar el proceso completo por el cual el estatus “interesante” de un paquete es determinado. En este ejemplo, el IP y el IPX son los protocolos que pueden cruzar el link de marcado. El usuario quiere evitar que los broadcasts y las actualizaciones de ruteo la iniciación de una llamada o guarden el link para arriba.

```
!
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 se debe permitir por las declaraciones del **access-list 121**, antes de cruzar el **interface async 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 evita que los paquetes EIGRP transiten el link. Significa solamente que estos paquetes no reajustarán el temporizador ocioso ni iniciarán un intento de marcado.

Semejantemente, el **access-list 903** declara el RIP IPX, las savias y las peticiones GNS de ser sin interés, mientras que el resto del tráfico IPX es interesante. Sin estos enunciados de negación, la conexión de marcado nunca bajaría probablemente y una factura telefónica muy grande resultaría puesto que los paquetes de estos tipos fluyen constantemente a través de una red IPX.

Con el **dialer-group 7** configurado en la interfaz asincrónica, sabemos que la marcador-**lista 7** es necesaria atar los filtros de tráfico interesante (es decir, Listas de acceso) a la interfaz. Una declaración de la marcador-**lista** se requiere (y *solamente* una puede ser configurado) para cada protocolo, aseegurandose que el número de la lista del dialer es lo mismo que el número de grupo de dialer en la interfaz.

De nuevo, es importante recordar que los *enunciados de negación* en las Listas de acceso configuradas para definir el tráfico interesante no evitarán que los paquetes negados crucen el link.

Usando el comando debug dialer, usted puede ver la actividad que acciona 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 destino de 172.16.2.22 ha accionado un intento de marcado en el Async1 de la interfaz.

Ruteo

Una vez que están definidos, los paquetes interesantes se deben rutear correctamente para que una llamada sea iniciada. El proceso de ruteo depende de dos cosas: entradas de la tabla de ruteo y “encima” de la interfaz sobre la cual a los paquetes de Routes.

Interfaces - up/up (spoofing)

Para que los paquetes sean ruteados y a través de una interfaz, esa interfaz debe estar up/up como se ve en las **interfaces de una demostración** hechas salir:

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

¿Qué sucede a una interfaz del dialer que no esté conectada? Si el protocolo no es en servicio en la interfaz, la implicación es que la interfaz sí mismo no estará para arriba. Rutea que confían en esa interfaz serán vaciadas de la tabla de ruteo, y el tráfico no será ruteado a esa interfaz. El resultado es que no se iniciaría ningunas llamadas por la interfaz.

La solución para contradecir esta posibilidad es permitir el **up/up (spoofing) del** estado para las interfaces del dialer. Cualquier interfaz se puede configurar como interfaz del dialer. Por ejemplo, un serial o una interfaz asincrónica se podía hacer 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 son por naturaleza una interfaz del dialer (los BRI y los PRI). La salida para una interfaz de la demostración parecerá esto:

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

Es decir la interfaz “finge” ser **up/up** de modo que siga habiendo las rutas asociadas en vigor y para poder rutear los paquetes a la interfaz.

Hay las circunstancias bajo las cuales una interfaz del dialer no será **up/up (spoofing)**. **La salida de la interfaz de la demostración** puede mostrar la interfaz como siendo administrativo abajo:

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

Administrativo abajo de simplemente significa que la interfaz se ha configurado con el comando shutdown. Éste es el estado predeterminado de cualquier interfaz del router cuando inician al router por el primer tiempo. Para remediar esto, utilice el comando interface configuration **ningún apagan**.

La interfaz se puede también considerar para estar en el modo de reserva:

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

Este estado indica que se ha configurado la interfaz pues el respaldo para otra interfaz. Cuando una conexión requiere la Redundancia en caso del error, una interfaz del dialer se puede configurar como el respaldo. Esto es lograda agregando los siguientes comandos a la interfaz de la conexión primaria:

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

Una vez que han configurado al **comando backup interface**, la interfaz usada como el respaldo será puesta en el modo de reserva hasta que la interfaz primaria vaya a un estado de

abajo/abajo. En aquella època, la interfaz del dialer configurada como respaldo, irá a un estado up/up (simulación) hasta que finalice un evento del dial.

Static rutas y Rutas estáticas flotantes

La forma más segura a los paquetes de Routes a una interfaz del dialer está con el Static Routing. Estas rutas se ingresan manualmente en la configuración del router o del servidor de acceso con el comando:

máscara del prefijo de la **ruta de IP {***direccionamiento* **| interface} [distance]**

prefijo: Prefijo de la ruta de IP para el destino.

máscara: Máscara del prefijo para el destino.

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

interfaz: Interfaz de la red a utilizar para el tráfico saliente.

distancia: (Opcional) una distancia administrativa. Este argumento se utiliza en las Rutas estáticas flotantes.

Las Static rutas se utilizan en las situaciones donde está la única conexión el link de marcado al sitio remoto. Una Static ruta tiene un valor de la distancia administrativa de un (1), que lo hace preferido sobre las rutas dinámico al mismo destino.

Por otra parte, las Rutas estáticas flotantes - es decir, las Static rutas con una distancia administrativa predefinida - se utilizan típicamente en los escenarios DDR de reserva. En estos escenarios un Dynamic Routing Protocol, tal como RIP o EIGRP, rutea los paquetes a través del link principal.

Una Static ruta normal (la distancia administrativa = 1) es preferible al EIGRP (distancia administrativa = 90) o al RIP (distancia administrativa = 120). La Static ruta hace los paquetes ser ruteada a través del Dial Line (Línea de marcado), incluso si el primario es ascendente y capaz de pasar el tráfico. Si, sin embargo, la Static ruta se configura con una distancia administrativa más alta que la de los Dynamic Routing Protocol uces de los funcionando en el router, las Rutas estáticas flotantes serán utilizadas solamente en ausencia de una “mejor” ruta - una con una distancia administrativa menor.

Si el respaldo DDR se está invocando por medio del **comando backup interface**, la situación es algo diferente. Porque sigue habiendo la interfaz del dialer en el modo de reserva mientras que el primario está **para arriba**, una Static ruta o las Rutas estáticas flotantes puede ser configurada. La interfaz del dialer no intentará conectar hasta después de que la interfaz primaria vaya **abajo de/abajo**.

Para una conexión dada, el número (o la estática flotante) de rutas estáticas necesarias es una función de la dirección en las interfaces del dialer. En caso de que las dos interfaces del dialer (una en cada uno del dos Routers) compartan una red común o una subred, se requiere típicamente solamente una Static ruta. Señala al LAN remoto usando el direccionamiento de la interfaz del dialer del router remoto como la dirección del salto siguiente.

Ejemplos

Ejemplo 1: El dial es la única conexión usando las interfaces numeradas. Una ruta es suficiente.

Cuadro 16-4: Dial usando las 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: El dial es la única conexión usando las interfaces sin numerar. Esto se puede configurar con apenas una ruta, pero es común configurar dos rutas: una host-ruta a la interfaz LAN en el router remoto y una ruta al LAN remoto vía el LAN remoto interconectan. Esto se hace para prevenir los problemas de asignación Layer3-to-Layer2, que pueden dar lugar a las fallas de encapsulación.

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

Cuadro 16-5: Dial usando las 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: El dial es una conexión de respaldo usando las interfaces numeradas. Se requieren una Rutas estáticas flotantes.

Cuadro 16-6: Respaldo usando las 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: El dial es una conexión de respaldo usando las interfaces sin numerar. Como en el ejemplo 2 antedicho, este método también se utiliza si las interfaces del dialer en los dos dispositivos se numeran, pero no en la misma red o subred.

Cuadro 16-7: Respaldo usando las interfaces de Unumbered

```
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 de marcado

La correspondencia basada del marcador (herencia) DDR es extensibilidad potentes y su de las limitaciones de la influencia escalamiento completos, pero y. La correspondencia basada DDR del marcador se basa en una vinculación estática entre la especificación de la llamada del por destino y la configuración de interfaz física.

Sin embargo, la correspondencia basada DDR del marcador también tiene muchas fuerzas. Soporta el Frame Relay, ISO CLNS, el LAPB, el Snapshot Routing, y todos los protocolos de routing que se soporten en los routeres Cisco. Por abandono, la correspondencia basada DDR del marcador soporta la transferencia rápida.

Al configurar una interfaz para la Llamada saliente, un mapa de marcado se debe configurar para cada destino remoto, y para cada uno diferente número al que se llamó en el destino remoto. Por ejemplo, si usted quiere una conexión PPP de links múltiples al marcar de un ISDN BRI en otra interfaz del ISDN BRI que tiene un diverso Número de directorio local para cada uno de sus Canales B, usted necesita un mapa de marcado 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
!
```

La orden en la cual se configuran los Mapas de marcado puede ser importante. Si dos o más comandos dialer map refieren a la misma dirección remota, el router o el servidor de acceso los intentará uno tras otro, en la orden, hasta que establezca con éxito una conexión

Nota: El IOS puede construir dinámicamente los Mapas de marcado en un router que recibe una llamada. El mapa de marcado se construye sobre la base del nombre de usuario autenticado y de la dirección IP negociada del llamador. Los mapas de marcado dinámico se pueden considerar solamente en la salida del comando show dialer map. Usted no puede verlos en la configuración corriente del router o del servidor de acceso.

Sintaxis del comando

Utilice la forma siguiente del **comando dialer map interface configuration** a:

- configure una interfaz serial o una interfaz de ISDN para llamar uno o los sitios múltiples, o
- reciba las llamadas de los sitios múltiples.

Todas las opciones se muestran en esta primera forma del comando. Para borrar una entrada del mapa de marcado determinada, no utilice una **ninguna** forma 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 forma siguiente del **comando dialer map** a:

- configure una interfaz serial o una interfaz de ISDN para poner una llamada a los sitios múltiples, y
- para autenticar las llamadas de los sitios múltiples.`dialer map protocol next-hop-address [name hostname] [spc] [speed 56 | 64]
  [broadcast] [dial-string[:isdn-subaddress]]`

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

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

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

- un solo sitio que requiere una secuencia de comandos de sistema o que no tiene ninguna

secuencia de comandos del módem asignada, o
- sitios múltiples en una sola línea, en las líneas múltiples, o en un grupo rotativo de dialers.`dialer map protocol next-hop-address [name hostname] [broadcast] [modem-script modem-regexp] [system-script system-regexp] [dial-string]`

Descripción de la Sintaxis

- palabras claves del *protocol protocol*. Utilice uno del siguiente: **APPLETALK**, **Bridge**, **clns**, **DECNet**, **IP**, **IPX**, **novell**, **foto**, **vides**, o **XNS**.
- *next-hop-address* - La dirección de protocolo usada para hacer juego contra los direccionamientos a los cuales los paquetes son destinados. Este argumento no se utiliza con la palabra clave del **Bridge Protocol**.
- **nombre** - (opcional) indica el sistema remoto con el cual el router local o el servidor de acceso comunica. Utilizado para autenticar el sistema remoto en las llamadas entrantes.
- *nombre de host* - (opcional) Nombre que distingue entre minúsculas y mayúsculas o ID del dispositivo remoto (generalmente el nombre del host). Para el Routers con las interfaces de ISDN, el campo del *nombre de host* puede contener el número que la línea de llamada ID proporciona (en caso de que Calling Line Identification, también designado el *CLI*, *Identificador de llamada*, y la *identificación de número automática* (ANI), está disponible).
- **proceso estadístico** - (opcional) especifica una conexión semipermanente entre el equipo del cliente y el intercambio. Se utiliza solamente en Alemania para los circuitos entre un ISDN BRI y un switch ISDN 1TR6 y en Australia para los circuitos entre un ISDN PRI y un Switch TS-014.
- **speed 56 | 64** - palabra clave (opcional) y valor que indican la velocidad de línea en los kilobites por segundo para utilizar. Utilizado para el ISDN solamente. La velocidad predeterminada es 64 kbps.
- **broadcast** - (opcional) indica que los broadcasts se deben remitir a esta dirección de protocolo.
- **secuencia de comandos del módem** - (opcional) indica la secuencia de comandos del módem que se utilizará para la conexión (para las interfaces asincrónicas).
- *módem-regexp* - expresión normal (opcional) a la cual una secuencia de comandos del módem será correspondida con (para las interfaces asincrónicas).
- **secuencia de comandos de sistema** - (opcional) indica la secuencia de comandos de sistema que se utilizará para la conexión (para las interfaces asincrónicas).
- *sistema-regexp* - expresión normal (opcional) a la cual una secuencia de comandos de sistema será correspondida con (para las interfaces asincrónicas).
- *dial-string [:* número de teléfono (opcional) de la *subdirección de ISDN]* enviado al dispositivo de marcado al reconocer los paquetes con una dirección del salto siguiente especificada que hace juego la lista de acceso definida (y el número opcional del subaddress usado para las conexiones multipunto ISDN). La cadena de marcado y la subdirección de ISDN, si está utilizada, deben ser el elemento más reciente de la línea de comando.

Perfiles de Marcador

Nota: En esta sección el término “interfaz del dialer” refiere a la interfaz configurada; no a una interfaz física en el router o el servidor de acceso.

La implementación de los Perfiles de marcado del DDR, introducida en la versión de IOS 11.2, se

basa en una separación entre lógico y la configuración de interfaz física. Los Perfiles de marcado también permiten que las configuraciones lógica y física estén limitadas juntas dinámicamente sobre por llamada una base.

La metodología de los Perfiles de marcado es ventajosa cuando usted quiere hacer el siguiente:

- comparta una interfaz (ISDN, asíncrono, o el sincro'nico serial) para poner o para recibir las llamadas
- cambie cualquier configuración sobre por usuario una base (excepto la encapsulación en la primera fase de Perfiles de marcado)
- Bridge a muchos destinos
- evite los problemas partidos del horizonte

Los Perfiles de marcado permiten la configuración de las interfaces físicas sea separada de la configuración lógica requerida para una llamada, y también permiten que las configuraciones lógica y física estén limitadas juntas dinámicamente sobre por llamada una base.

Un perfil de marcado consiste en los elementos siguientes:

- Una configuración de la *interfaz del dialer* (entidad lógica), incluyendo una o más cadenas de marcado (que se utiliza para alcanzar una subred de destino)
- *Una clase del mapa de marcado* que define todas las características para cualquier llamada a la cadena de marcado especificada
- *Recursos compartidos de dialers* pedidos de las interfaces físicas que se utilizarán por la interfaz del dialer

Todo llama yendo a o desde el mismo uso de la subred de destino el mismo perfil de marcado.

Una configuración de la interfaz del dialer incluye todas las configuraciones necesarias para alcanzar una subred de destino específica (y cualquier redes alcanzadas a través de ella). Las cadenas de marcado múltiples se pueden especificar para la misma interfaz del dialer; cada cadena de marcado se puede asociar a una diversa clase del mapa de marcado. La clase del mapa de marcado define todas las características para cualquier llamada a la cadena de marcado especificada. Por ejemplo, el map-class para un destino pudo especificar una velocidad 56-kbps ISDN. El map-class para un diverso destino pudo especificar una velocidad 64-kbps ISDN.

Cada interfaz del dialer utiliza a los recursos compartidos de dialers, que es recursos compartidos de la interfaz física pedidos en base de la prioridad asignada a cada interfaz física. Una interfaz física puede pertenecer a los recursos compartidos por múltiples dialers, con la contención que es resuelta por la prioridad. Las interfaces del ISDN BRI y PRI pueden establecer un límite en el mínimo y el número máximo de canales B reservados por cualquier recursos compartidos de dialers. Un canal reservado por los recursos compartidos de dialers sigue siendo ocioso hasta que el tráfico se dirija al pool.

Cuando los Perfiles de marcado se utilizan para configurar el DDR, una interfaz física no tiene ningún ajuste de la configuración excepto la encapsulación y los recursos compartidos de dialers a los cuales la interfaz pertenece.

Nota: El párrafo precedente tiene una excepción. Los comandos que se aplican antes de que la autenticación sea completa se deben configurar en la interfaz física (o BRI o PRI) y no en el perfil de marcado. Los Perfiles de marcado no hacen los comandos ppp authentication de copia (o los comandos LCP) a la interfaz física.

El cuadro 16-8 muestra una aplicación típica de los Perfiles de marcado. El router A tiene la interfaz del dialer 1 para el Dial-On-Demand Routing con el red secundario 1.1.1.0, y interfaz del dialer 2 para el Dial-On-Demand Routing con el red secundario 2.2.2.0. La dirección IP para la interfaz del dialer 1 es su direccionamiento como nodo en la red 1.1.1.0. Al mismo tiempo, esa dirección IP sirve como la dirección IP de las interfaces físicas usadas por la interfaz del dialer 1. Semejantemente, la dirección IP para la interfaz del dialer 2 es su direccionamiento como nodo en la red 2.2.2.0.

Cuadro 16-8: Aplicación típica de los Perfiles de marcado

Una interfaz del dialer utiliza a solamente un recursos compartidos de dialers. Una interfaz física, sin embargo, puede ser un miembro de un o mucho recursos compartidos de dialers, y los recursos compartidos de dialers pueden tener varias interfaces físicas como miembros.

El cuadro 16-9 ilustra las relaciones entre los conceptos de interfaz del dialer, de recursos compartidos de dialers, y de interfaces físicas. El BRI 1 de la interfaz física de los recursos compartidos de dialers 2. de las aplicaciones de la interfaz del dialer 0 pertenece a los recursos compartidos de dialers 2 y tiene una prioridad específica en el pool. La interfaz física BRI2 también pertenece a los recursos compartidos de dialers 2. Porque la contención se resuelve en base de los niveles de prioridad de las interfaces físicas en el pool, BRI 1 y el BRI2 tienen que ser asignados diversas prioridades en el pool. Quizás el BRI 1 es la prioridad asignada 100 y el BRI2 es la prioridad asignada 50 en los recursos compartidos de dialers 2 (una prioridad de 50 es más alta que una prioridad de 100). El BRI2 tiene una prioridad más alta en el pool, y sus llamadas serán puestas primero.

Cuadro 16-9: Relaciones entre las interfaces del dialer, los recursos compartidos de dialers, y las interfaces físicas

Pasos de la configuración del perfil de marcado

Comando	Propósito
número de marcador de interfaz	Cree una interfaz del dialer.
máscara de dirección del **IP Address**	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 la 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.
poolnumber del marcador	Especifique el grupo de marcado a utilizar para llamadas a este destino.
dialer-group group-number	Asigne la interfaz del dialer a un grupo de dialer.
dialer-list dialer-	Especifique una lista de acceso por

group protocol protocol-name {permit | niegue | list access-list-number}	el número de lista o por el protocolo y el número de lista para definir los paquetes “interesantes” que pueden accionar una llamada.

Operaciones PPP

El Point-to-Point Protocol (PPP) es con mucho el Transport Protocol más común de la capa de link, usurpando totalmente el SLIP como el protocolo de la opción para el dial (y en muchos casos, NON-dial) síncrono y las conexiones en serie asíncrona. El PPP fue definido originalmente en 1989 por el RFC 1134, que desde entonces ha sido hecho Obsoleto por una serie de RFC que culminaban (a partir de esta escritura) en el RFC1661. Hay también los RFC numerosos que definen los elementos del protocolo, tales como RFC1990 (el protocolo del multilink PPP), RFC2125 (el protocolo bandwidth allocation PPP), y muchos otros. Un repositorio en línea de los RFC se puede encontrar en:

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

Quizás la mejor definición del PPP se puede encontrar en el RFC1661, que estado:

El Point-to-Point Protocol (PPP) proporciona un método estándar para transportar los datagramas con protocolos múltiples sobre los enlaces punto a punto. El PPP se comprende de tres componentes principales:

1. Un método para encapsular los datagramas con protocolos múltiples.
2. Un (LCP) del Link Control Protocol para establecer, configurar, y probar la conexión de link de datos.
3. Una familia de los protocolos network control (NCP) para establecer y configurar diversos protocolos de capa de red.

Etapas de la negociación PPP

La negociación PPP consiste en tres fases: (LCP), autenticación, y protocolo network control del Link Control Protocol (NCP). Cada uno procede en la orden, siguiendo el establecimiento del async o de la conexión ISDN.

LCP (Protocolo de control de enlace)

El PPP no sigue un modelo cliente/servidor. Todas las conexiones son entre iguales. Por lo tanto, cuando hay un llamador y un receptor, los ambos extremos de la conexión Point-to-Point deben estar de acuerdo con los protocolos y los parámetros negociados.

Cuando la negociación comienza, cada uno de los pares que quieren establecer una conexión PPP debe enviar una petición de la configuración (véase en la **negociación ppp del debug** y designada en lo sucesivo el CONFREQ). Se incluye en el CONFREQ cualquier opción que no sea el valor por defecto del link. Éstos incluyen a menudo el Maximum Receive Unit (MRU), el Async Control Character Map (ACCM), el protocolo de autenticación (AuthProto), y el número mágico. También se consideran el Maximum Receive Reconstructed Unit (MRRU) y el discriminador de punto final (EndpointDisc), usado para el Multilink PPP.

Hay tres respuestas posibles a cualquier CONFREQ:

- Un Configuración-reconocimiento (CONFACK) debe ser publicado si el par reconoce las opciones y está de acuerdo los valores vistos en el CONFREQ.
- Un Configuración-rechazo (CONFREJ) debe ser enviado si las opciones unas de los en el CONFREQ no se reconocen (por ejemplo, algunas Opciones específicas del proveedor) o si los valores para las opciones unas de los se han rechazado explícitamente en la configuración del par.
- Un Configuración-Negativo-reconocimiento (CONFNAK) se debe enviar si todas las opciones en el CONFREQ se reconocen, solamente los valores no es aceptable por el par.

Los dos pares continúan intercambiando los CONFREQ, los CONFREJ y los CONFNAK hasta que cada uno envíe un CONFACK, hasta que la conexión de marcado esté quebrada, o hasta uno o ambos pares indica que la negociación no puede ser completada.

Autenticación

Después de la terminación satisfactoria de la negociación LCP y de alcanzar un acuerdo en el AuthProto, el siguiente paso es autenticación. La autenticación, mientras que es no obligatoria por el RFC1661, se recomienda altamente en todas las conexiones de marcado. A veces, es un requisito para la operación correcta; Perfiles de marcado que son un caso en cuestión.

Los dos tipos principales de autenticación en el PPP son el protocolo password authentication (PAP) y el Challenge Handshake Authentication Protocol (CHAP), definido por el RFC1334 y actualizado por el RFC1994.

El PAP es el más simple de los dos, pero es menos seguro porque la contraseña para texto sin formato se envía a través de la conexión de marcado. La GRIETA es más segura porque la contraseña para texto sin formato no se envía nunca a través de la conexión de marcado.

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

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

Al discutir la autenticación, es útil utilizar los términos “solicitante” y “authenticator” para distinguir los papeles desempeñados por los dispositivos en cualquier extremo de la conexión, aunque cualquier par puede actuar en cualquier papel. El “solicitante” describe el dispositivo que pide el acceso a la red y suministra la información de autenticación; el “authenticator” verifica la validez de la información de autenticación y permite o rechaza la conexión. Es común para que ambos pares actúen en ambos papeles cuando una conexión DDR se está haciendo entre el Routers.

PAP

El PAP es bastante simple. Después de la terminación satisfactoria de la negociación LCP, el solicitante envía en varias ocasiones su Combinación de nombre de usuario/contraseña a través del link hasta que el authenticator responda con un acuse de recibo o hasta que el link está quebrado. El authenticator puede desconectar el link si determina que la Combinación de nombre de usuario/contraseña es inválida.

GRIETA

La GRIETA es algo más complicada. El authenticator envía un desafío al solicitante, que entonces responde con un valor. Este valor se calcula usando una función del “troceo unidireccional” para desmenuzar el desafío y la contraseña de la GRIETA junto. El valor de resultado se envía al authenticator junto con el solicitante nombre de la computadora principal de CHAP (que puede ser diferente de su nombre del host real) en un *mensaje de respuesta*.

El authenticator lee el nombre de host en el mensaje de respuesta, mira para arriba la contraseña prevista para ese nombre de host, y después calcula el valor que cuenta con al solicitante enviado en su respuesta realizando la misma función de troceo el solicitante realizada. Si los valores de resultado hacen juego, la autenticación es acertada. El error debe llevar a una desconexión.

AAA

Un servicio de la autenticación, de la autorización y de las estadísticas (AAA), tal como TACACS+ o RADIUS, puede ser utilizado en lograr el PAP o la GRIETA.

NCP

Después de la autenticación satisfactoria, la fase NCP comienza. Como en el LCP, los pares intercambian los CONFREQ, los CONFREJ, los CONFNAK y los CONFACK. Sin embargo, en esta fase de negociación, los elementos que son negociados tienen que hacer con los protocolos de capa más altas - IP, IPX, bridging, CDP, y así sucesivamente. Uno o más de estos protocolos pueden ser negociados. Pues es el más de uso general, y porque otros protocolos actúan en mucho la misma moda, el Protocolo de control de Protocolo de Internet (IPCP), definido en el RFC1332, es el foco de esta discusión. Otros RFC pertinentes incluyen, pero no se limitan a:

- RFC1552 (IPX Control Protocol)
- RFC1378 (protocolo de control de APPLETALK)
- RFC1638 (protocolo bridging control)
- RFC1762 (Control Protocol del DECNet)
- RFC1763 (Control Protocol de las vides)

Además, el Control Protocol del protocolo cisco discovery (CDPCP) se puede negociar durante el NCP, aunque éste no es común. Los ingenieros de Cisco TAC aconsejarán generalmente que configuren al comando no cdp enable en cualquiera y todas las interfaces del dialer de prevenir los paquetes CDP que guardan un llamar indefinidamente.

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

Si el par no tiene ningún direccionamiento, enviará un CONFREQ con el direccionamiento 0.0.0.0. Esto dice al otro par asignar un direccionamiento, que es logrado por el envío de un CONFNAK con la dirección apropiada.

Las otras opciones se pueden negociar en el IPCP. Comúnmente - vista son el primarios y las direcciones secundarias para el Domain Name Server y el servidor de nombre de NetBIOS, según lo descrito en el RFC1877 informativo. El Compression Protocol IP (RFC1332) es también común.

Metodologías de PPP alternativo

Las metodologías de PPP alternativo incluyen el Multilink PPP, el multichassis PPP, y los Perfiles virtuales.

PPP de links múltiples

La característica del protocolo multilink point-to-point (MLP) proporciona la funcionalidad de balance de carga sobre los links de WAN múltiples. Al mismo tiempo proporciona la Interoperabilidad multi-vendor, fragmentación de paquetes y secuencia apropiada, y cálculo de la carga en ambos tráfico entrante y saliente. La implementación de Cisco del Multilink PPP soporta las especificaciones de la fragmentación y del establecimiento de secuencia de paquetes en el RFC1717.

El Multilink PPP permite que los paquetes sean hechos fragmentos. Estos fragmentos se pueden enviar al mismo tiempo sobre los links Point-to-Point múltiples a la misma dirección remota. Los links múltiples suben en respuesta a un umbral de carga del dialer que usted defina. 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 Multilink PPP trabaja sobre los tipos de interfaz siguientes que (solos o múltiples) se configuran para soportar los grupos rotativos y la encapsulación PPP del Marcado a pedido:

- interfaces seriales asincrónicas
- BRI
- PRI

Configuración

Para configurar el Multilink PPP en las interfaces asincrónicas, usted configura las interfaces asincrónicas para soportar el DDR y la encapsulación PPP. Usted entonces configura una interfaz del dialer para soportar la encapsulación PPP, el ancho de banda a pedido, y el Multilink PPP. En algún momento, sin embargo, agregar más interfaces asincrónicas no mejora el funcionamiento. Con el tamaño de MTU predeterminado, el Multilink PPP debe soportar tres interfaces asincrónicas usando los módems V.34. Sin embargo, los paquetes pudieron ser caídos de vez en cuando si el MTU es pequeño o si ocurren las explosiones grandes de las tramas cortas.

Para habilitar el Multilink PPP en una sola interfaz del ISDN BRI o PRI, le no requieren definir a un grupo rotativo de dialers por separado porque las interfaces de ISDN son grupos rotativos de dialers por abandono. Si usted no utiliza los procedimientos de la autenticación PPP, su servicio de telefonía debe pasar la información de identidad de la persona que llama.

Se requiere un número del umbral de carga. Por un ejemplo de configurar el Multilink PPP en una sola interfaz del ISDN BRI, vea el *ejemplo de Multilink PPP en una interfaz de ISDN* abajo.

Cuando se configura el Multilink PPP y usted quisiera que un agrupamiento de links múltiples fuera conectado indefinidamente, utilice el **comando dialer idle-timeout** de fijar un temporizador de inactividad muy alto. **El comando dialer-load threshold 1** no guarda un agrupamiento de links múltiples de los links *n* conectados indefinidamente, y el **comando dialer-load threshold 2** no guarda un agrupamiento de links múltiples de dos links conectados indefinidamente.

Para habilitar el Multilink PPP en el ISDN múltiple BRI o las interfaces PRI, usted configura una interfaz rotatoria del marcador y la configura para el Multilink PPP. Usted entonces configura los BRI por separado y los agrega cada uno al mismo grupo rotativo. Vea el *ejemplo de Multilink PPP en los interfaces ISDN múltiples* abajo.

Ejemplo de Multilink PPP en una interfaz de ISDN

El siguiente ejemplo habilita el Multilink PPP en la interfaz BRI 0. Cuando se configura un BRI, no se requiere ninguna configuración de grupo rotativo del marcador (la interfaz de ISDN es un grupo rotativo por abandono).

```
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 los interfaces ISDN múltiples

El siguiente ejemplo configura el ISDN múltiple BRI para pertenecer al mismo grupo rotativo de dialers para el Multilink PPP. Utilice el **comando dialer rotary-group** de asignar cada uno del ISDN BRI a ese grupo rotativo de dialers que deba hacer juego el número de la interfaz del dialer (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
```

Multilink de multichasis PPP

El Multilink PPP proporciona la capacidad de partir y de las recombinaciones de paquetes a un solo sistema final a través de un conducto lógico (también llamado un *conjunto*) formado por los links múltiples. El Multilink PPP proporciona el ancho de banda a pedido y reduce la latencia de la transmisión a través de los links PÁLIDOS.

El multilink de multichasis PPP (MMP), por otra parte, proporciona la capacidad adicional para que los links terminen en los routeres múltiples con diversas direcciones remotas. El MMP puede

también manejar ambo el tráfico analógico y digital.

Estas funciones se piensan para las situaciones en las cuales hay pools grandes de los usuarios de dial in, en quienes un único servidor de acceso no puede proporcionar bastantes puertos de acceso telefónico. El MMP permite que las compañías proporcionen un solo número de dialup a sus usuarios y que apliquen la misma solución a las llamadas analógica y digital. Esta característica permite que los proveedores de servicio de Internet, por ejemplo, afecten un aparato un solo número rotativo ISDN a varios ISDN PRI a través de vario Routers.

Para una descripción completa de los comandos mmp referidos adjunto, refiera a la *referencia del comando solutions del marcado 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 la serie del 7500, 4500 y 2500 de Cisco y en el sincro'nico serial, la serie asincrónica, el ISDN BRI, ISDN PRI, y las interfaces del dialer.

El MMP no requiere la reconfiguración de los Switch de la compañía telefónicas.

Configuración

Configuran al Routers o el Access Servers para pertenecer a los grupos de pares, llamados los *grupos de pila*. Todos los miembros del grupo de pila son pares; los grupos de pila no necesitan a un router principal permanente. Cualquier miembro del grupo Stack puede contestar a las llamadas que vienen de un solo número de acceso, que es generalmente un grupo Hunt ISDN PRI. Las llamadas pueden venir adentro de los dispositivos del usuario remoto, tales como Routers, módems, adaptadores de terminal ISDN, o placas de PC.

Una vez que una conexión se establece con un miembro de un *grupo de pila*, ese miembro posee la llamada. Si una segunda llamada viene adentro del mismo cliente y un diverso router contesta a la llamada, el router establece un túnel y adelante todos los paquetes que pertenecen a la llamada al router que posee la llamada. El proceso de establecer un túnel y del envío llama con él al router que posee la llamada se llama a veces *proyección del link PPP al master de la llamada*.

Si un más router potente está disponible, puede ser configurado como miembro del grupo de pila y los otros miembros del grupo Stack pueden establecer los túneles y delantero todas las llamadas a él. En tal caso, los otros miembros del grupo Stack apenas están contestando que las llamadas y el tráfico de reenvío al más potente *descargan al* router.

Nota: Las líneas PÁLIDAS de la Latencia alta entre los miembros del grupo Stack pueden hacer la operación del grupo de pila ineficaz.

El manejo de llamadas MMP, haciendo una oferta, y acoda 2 funcionamientos de reenvío en el grupo de pila sigue de la forma siguiente. También se muestra en el cuadro 16-10.

1. Cuando la primera llamada viene adentro al grupo de pila, las respuestas del router A.
2. En hacer una oferta, el router A gana porque tiene ya la llamada. El router A hace el llamada-*master* para esa sesión con el dispositivo remoto. El router A pudo también ser llamado el *host a la interfaz de conjunto principal*.
3. Cuando el dispositivo remoto que inició la llamada necesita más ancho de banda, hace una segunda llamada del Multilink PPP al grupo.
4. Cuando viene la segunda llamada adentro, el router D le contesta e informa al grupo de pila.

El router A gana hacer una oferta porque está manejando ya la sesión con ese dispositivo remoto.
5. El router D establece un túnel al router A y adelante los datos PPP no procesados al router A.
6. El router A vuelve a montar y las re-secuencias los paquetes.
7. Si más llamadas vienen adentro al router D y pertenecen también al router A, el túnel entre A y D agranda para manejar el tráfico agregado. El router D no establece un túnel adicional al A.
8. Si más llamadas vienen adentro y son contestadas por cualquier otro router, ese router también establece un túnel a A y adelante a los datos PPP no procesados.
9. Los datos vueltos a montar se pasan en la red corporativa como si hicieron que todos vinieran a través de un vículo físico.

Cuadro 16-10: Escenario PPP típico del multilink de multichasis

En contraste con la figura anterior, el cuadro 16-11 ofrece a un router de la descarga. El Access Servers que pertenece a las llamadas de una respuesta del grupo de pila, establece los túneles, y adelante llama a un Cisco 4700 Router que gane hacer una oferta y es el llamada-master para todas las llamadas. El Cisco 4700 vuelve a montar y las re-secuencias todos los paquetes que vienen adentro a través del grupo de pila.

Cuadro 16-11: Multilink de multichasis PPP con un router de la descarga como miembro del grupo Stack

Nota: Usted puede construir a los grupos de pila que usan diverso servidor de acceso, la transferencia, y las plataformas del router. Sin embargo, los Universal Access Servers tales como el Cisco AS5200 no se deben combinar con el ISDN. Esto se debe hacer solamente con el Access Servers tal como la plataforma 4x00. Porque las llamadas de la oficina central se afectan un aparato en un modo arbitrario, esta combinación podría dar lugar a una llamada analógica que era entregada a un servidor de acceso digital-solamente, que no podría manejar la llamada.

El soporte MMP en un grupo de Routers requiere que configuren a cada router para soportar el siguiente:

- PPP de links múltiples
- Protocolo stack group bidding (SGBP)
- Plantilla virtual usada para reproducir la configuración de la interfaz para soportar el MMP

Perfiles virtuales

Los Perfiles virtuales son una aplicación única del Point-to-Point Protocol (PPP) que puede crear y configura una interfaz de acceso virtual dinámicamente cuando se recibe una llamada entrante, y derribar la interfaz dinámicamente cuando la llamada termina. Los Perfiles virtuales trabajan con el PPP directo y con el Multilink PPP (MLP).

La información de la configuración para una interfaz de acceso virtual de los Perfiles virtuales puede venir de una interfaz de plantilla virtual, o de la configuración específica del usuario salvada en un servidor del Authentication, Authorization, and Accounting (AAA), o ambos.

La configuración del user-specific aaa usada por los Perfiles virtuales es *configuración de la interfaz* y se descarga durante las negociaciones LCP. Otra característica, llamada Configuración por usuario, también utiliza la información de la configuración ganada de un servidor de AAA. Sin

embargo, la Configuración por usuario utiliza la *configuración de red* (tal como Listas de acceso y filtros de la ruta) descargada durante las negociaciones NCP.

Dos reglas gobiernan la configuración de la interfaz de acceso virtual por las interfaces de plantilla virtual y las configuraciones AAA de los Perfiles virtuales:

- Cada aplicación de acceso virtual puede tener, a lo más, una plantilla de la cual a reproducirse. Sin embargo, puede tener configuraciones de AAA múltiples de las cuales reproducirse (la información AAA de los Perfiles virtuales y configuración por usuario de AAA, que a su vez pudo incluir los protocolos de la configuración de múltiples).
- Cuando los Perfiles virtuales son configurados por la plantilla virtual, su plantilla tiene prioridad más alta que cualquier otra plantilla virtual.

Vea “Interoperabilidad con la sección de otras funciones de marcado de Cisco” abajo para una descripción de las secuencias de la configuración posible que dependen de la presencia o de la ausencia por el MLP u otra función de acceso virtual que reproduzca una interfaz de plantilla virtual.

Esta característica se ejecuta en todas las plataformas de Cisco IOS que soporten el MLP.

Para una descripción completa de los comandos mencionados en esta sección, refiera a los “Perfiles virtuales ordena” el capítulo en el *Dial Solutions Command Reference* en el conjunto de la documentación sobre Cisco IOS. Para localizar la documentación de otros comandos que aparezcan en este capítulo, usted puede utilizar el índice principal de referencia de comandos o buscar en línea.

Antecedentes

Esta sección presenta la información previa sobre los Perfiles virtuales para ayudarle a entender esta aplicación antes de que usted comience a configurarla.

Restricciones

Recomendamos que los direccionamientos innumerables estén utilizados en las interfaces de plantilla virtual para asegurarse de que no crean a las direcciones de red duplicada en las interfaces de acceso virtual.

Prerrequisitos

El uso de la información de configuración de interfaz AAA específica del usuario con los Perfiles virtuales requiere al router ser configurado para el AAA y requiere al servidor de AAA tener Pares AV de la configuración de interfaz específica del usuario. Los Pares AV relevantes (en un servidor de RADIUS) comienzan como sigue:

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

La información que sigue el signo igual (=) podría ser cualquier comando configuration de la interfaz del Cisco IOS. Por ejemplo, la línea pudo ser los siguientes:

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

El uso de una interfaz de plantilla virtual con los Perfiles virtuales requiere una plantilla virtual ser definido específicamente para los Perfiles virtuales.

Interoperabilidad con otras funciones de marcado de Cisco

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

Configuración de DDR de las interfaces físicas

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

- Los Perfiles de marcado se configuran para la interfaz. El perfil de marcado se utiliza en vez de la configuración de los Perfiles virtuales.
- El DDR no se configura en la interfaz. Los Perfiles virtuales reemplazan la configuración actual.
- El DDR heredado se configura en la interfaz. Los Perfiles virtuales reemplazan la configuración actual.

Nota: Si se utiliza una interfaz del dialer (cualquier dialer ISDN incluyendo), su configuración se utiliza en la interfaz física en vez de la configuración de los Perfiles virtuales.

Efecto del Multilink PPP sobre la configuración de la interfaz de acceso virtual

Tal y como se muestra en del cuadro 16-8, la configuración exacta de una interfaz de acceso virtual depende de los tres factores siguientes:

- Si los Perfiles virtuales son configurados por la plantilla virtual, por el AAA, por ambos, o por ningunos. Estos estados se muestran como “VP VT solamente,” “VP AAA solamente,” “VP VT y VP AAA,” y “ningún VP en absoluto,” respectivamente, en la tabla.
- La presencia o la ausencia de una interfaz del dialer.
- La presencia o la ausencia de MLP. La escritura de la etiqueta “MLP” de la columna es una substitución cualquier función de acceso virtual que soporte el MLP y se reproduzca de una interfaz de plantilla virtual.

En el cuadro 16-8, el “Multilink VT” significa que una interfaz de plantilla virtual está reproducida *si* uno se define para el MLP o una función de acceso virtual que utilice el MLP.

Cuadro 16-8: Secuencia de la reproducción de la configuración de los Perfiles virtuales

Configuración de los Perfiles virtuales	MLP ningún marcador	Marcador MLP	Ningún MLP ningún marcador	Ningún marcador MLP
VP VT solamente	VP VT	VP VT	VP VT	VP VT
VP AAA solamente	(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 VP en absoluto	(Multilink VT)	Marcador	No se crea ninguna interfaz de acceso virtual.	No se crea ninguna interfaz de acceso virtual.

La pedido de los elementos en cualquier célula de la tabla es importante. Donde el VP VT se muestra arriba VP AAA, significa que primero la plantilla virtual de los Perfiles virtuales está reproducida en la interfaz, y entonces la configuración de la interfaz AAA para el usuario se aplica a ella. El configuración de interfaz AAA específica del usuario agrega a la configuración y reemplaza cualquier comando en conflicto de la interfaz física o de configuración de plantilla virtual.

Interoperabilidad con las otras funciones que utilizan las plantillas virtuales

Los Perfiles virtuales también interoperan con las aplicaciones de acceso virtual que reproducen una interfaz de plantilla virtual. Cada aplicación de acceso virtual puede tener, a lo más, una plantilla de la cual a reproducirse, pero puede reproducirse de las configuraciones de AAA múltiples.

La interacción entre los Perfiles virtuales y otras aplicaciones de la plantilla virtual es como sigue:

- Si se habilitan los Perfiles virtuales y una plantilla virtual se define para ella, se utiliza la plantilla virtual de los Perfiles virtuales.
- Si los Perfiles virtuales son configurados por el AAA solamente (no se define ninguna plantilla virtual para los Perfiles virtuales), la plantilla virtual para otra aplicación de acceso virtual (VPDN, por ejemplo) se puede reproducir sobre la interfaz de acceso virtual.
- Una plantilla virtual, eventualmente, se reproduce a una interfaz de acceso virtual antes de la configuración AAA de los Perfiles virtuales o configuración por usuario de AAA. Configuración por usuario de AAA, si está utilizado, es el último aplicado.

Terminología

Los nuevos o infrecuentes términos siguientes se utilizan en este capítulo:

Par AV: Un parámetro de la configuración en un servidor de AAA; parte de la configuración de usuario que el servidor de AAA envía al router, en respuesta a los pedidos de autorización específicos del usuario. El router interpreta cada par AV como Cisco IOS comando router configuration y aplica los pares AV en la orden. En este capítulo, el par AV del término refiere a un parámetro de configuración de interfaz en un servidor de RADIUS.

Un par AV de la configuración de la interfaz para los Perfiles virtuales puede tomar una forma tal como esto:

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

clonación: Creando y configurando una interfaz de acceso virtual aplicando los comandos configuration de una plantilla virtual específica. La plantilla virtual es la fuente de la información

del usuario y de la información dependiente del router genéricas. El resultado de la reproducción es una interfaz de acceso virtual configurada con todos los comandos en la plantilla.

interfaz de acceso virtual: Caso de una interfaz virtual única que se crea dinámicamente y existe temporalmente. Las interfaces de acceso virtual se pueden crear y configurar diferentemente por diversas aplicaciones, tales como Perfiles virtuales y Virtual Private Dialup Networks.

interfaz de plantilla virtual: Usuarios de la configuración de la interfaz genérica con certeza o para cierto propósito, más la información dependiente del router. Esto toma la forma de una lista de comandos de la interfaz del Cisco IOS de ser aplicado a la interfaz virtual según las necesidades.

perfil virtual: El caso de una interfaz de acceso virtual única que se cree dinámicamente cuando los ciertos usuarios llaman adentro, y se derriba dinámicamente cuando la llamada desconecta. El perfil virtual de un usuario específico se puede configurar por una interfaz de plantilla virtual, configuración de interfaz específica del usuario salvada en un servidor de AAA, o una interfaz de plantilla virtual y configuración de interfaz específica del usuario del AAA.

La configuración de una interfaz de acceso virtual comienza con una interfaz de plantilla virtual (eventualmente), seguida por la aplicación de la configuración específica del usuario para la sesión de dial in del usuario determinado (eventualmente).

Ejemplo con notas de la negociación de PPP

En este ejemplo, un ping saca a colación un link ISDN entre el *montecito del* Routers y el *Goleta*. Observe que, mientras que no hay el timestamping en este ejemplo, está recomendado generalmente que usted utiliza el **service timestamps debug datetime msec del** comando global configuration.

Cuadro 16-12: Router-ISDN-router

Estos debugs se toman del *montecito*; sin embargo, el debugging en el *Goleta* miraría mucho el lo mismo.

Nota: Sus debugs pueden aparecer en un diverso formato. Esta salida es el más viejo formato de salida del debugging de PPP, antes de las modificaciones introducidas en la versión de IOS 11.2(8). Vea el capítulo 17 para un ejemplo del debugging de 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 - Se establece la conexión (los debugs ISDN no usados en este ejemplo).

Comience el LCP:

C - *El montecito* envía los pedidos de configuración LCP para el AUTHTYPE y para el MAGICNUMBER.

D - *El Goleta* envía sus CONFREQ. Si el valor para el MAGICNUMBER es lo mismo que el valor enviado por el *montecito*, hay una fuerte probabilidad que la línea está colocada.

E - Esto indica que el *montecito* ha enviado los acuses de recibo a los CONFREQ de *Goleta*.

F - *El montecito* recibe los CONFACK del *Goleta*.

Comience fase de autenticación:

G, H - Desafío del *montecito* y del *Goleta* para la autenticación.

J - *El Goleta* responde al desafío.

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

M - Mensaje del *Goleta al montecito*: autenticación acertada.

La negociación NCP comienza:

N, P - Cada router envía su IP Address configurado en un CONFREQ.

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

¿S -? y viceversa.

T, U - Una ruta está instalada del *montecito al Goleta* y el protocolo en la interfaz cambia a “encima de”, indicando que las negociaciones NCP han completado con éxito.

Antes de llamar el Equipo del TAC de Cisco Systems

Antes de llamar el Centro de Asistencia Técnica (TAC) de Cisco Systems, aseegurese le haber leído con este capítulo y haber completado las acciones sugeridas para su problema de sistema.

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

Para todos los problemas, recoja la salida de los ejecutar-**config de la demostración** y **muestre la versión**. Asegúrese de que el comando service timestamps debug datetime msec esté en la configuración.

Por problemas de DDR, recoja el siguiente:

- **muestre el mapa de marcado**
- **debug dialer**
- **debug ppp negotiation**
- **debug ppp authentication**

Si el ISDN está implicado, recoja:

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

Si los módems están implicados, recoja:

- muestre las líneas
- muestre la línea [x]
- **muestre el módem** (si los módems integrados están implicados)
- **muestre el modem version** (si los módems integrados están implicados)
- **haga el debug del módem**
- **debug modem csm** (si los módems integrados están implicados)
- **charla del debug** (si un escenario DDR)

Si el T1s o los PRI está implicados, recoja:

- **muestre el T1 del regulador**

Información Relacionada

- Guía de las soluciones del dial del Cisco IOS
- Información general de interfaces, controladores y líneas utilizadas para el acceso por marcación
- Encaminamiento a través de las líneas del módem
- Configuración troncal del puerto serial y del T1/E1
- Diseño del internetworks DDR
- Decisión y preparación para configurar del DDR
- Configurar DDRtitle
- Reseña general de tecnología PPP
- Diseño del internetworks ISDN
- Tipos de switch, códigos y valores de ISDN
- Disposición de la línea ISDN
- Soporte Técnico y Documentación - Cisco Systems