Tecnologia dialup: Visões gerais e explicações

Contents

Introduction

Este capítulo apresenta e explica algumas das tecnologias usadas em redes de discagem. Você encontrará dicas de configuração e interpretações de alguns dos comandos **show**, que são úteis para verificar a operação correta da rede. Os procedimentos de solução de problemas estão além do escopo deste documento e podem ser encontrados no documento *Troubleshooting de Discagem*.

Antes de Começar

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas

técnicas Cisco.

Prerequisites

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Operações de modem

Esta seção explica problemas relacionados especificamente à configuração, verificação e uso de modems com roteadores Cisco.

Usando o comando Modem Autoconfigure

Se estiver usando o Cisco Internetwork Operating System (Cisco IOS) versão 11.1 ou posterior, você pode configurar seu roteador Cisco para se comunicar e configurar seu modem automaticamente.

Use o procedimento a seguir para configurar um roteador Cisco para tentar descobrir automaticamente que tipo de modem está conectado à linha e, em seguida, configurar o modem:

1. Para descobrir o tipo de modem conectado ao roteador, use o comando de configuração de linha **modem autoconfigure discovery**.
2. Quando o modem for descoberto com êxito, configure-o automaticamente usando o comando de configuração de linha **modem autoconfigure type** ***modem-name***.

Se quiser exibir a lista de modems para os quais o roteador tem entradas, use o comando **show modemcap** ***modem-name*** . Se desejar alterar um valor de modem retornado do comando **show modemcap**, use o comando de configuração de linha **modemcap edit** ***modem-name attribute value***.

Para obter informações completas sobre o uso desses comandos, consulte o *Guia de Configuração de Soluções de Discagem de Documentação do Cisco IOS e a Referência de Comandos de Soluções de Discagem*.

Observação: *não* insira **&W** na entrada modemcap que é usada para a configuração automática. Isso faz com que a NVRAM seja regravada toda vez que uma configuração automática de modem for executada e destruirá o modem.

Estabelecendo uma sessão de Telnet reversa para um modem

Para fins de diagnóstico, ou para configurar inicialmente o modem se estiver executando o Cisco

IOS versão 11.0 ou anterior, você deve estabelecer uma sessão Telnet reversa para configurar um modem para se comunicar com um dispositivo Cisco. Desde que você bloqueie a velocidade do modem lateral do equipamento terminal de dados (DTE), o modem sempre se comunicará com o servidor de acesso ou roteador na velocidade desejada. Consulte a Tabela 16-5 para obter informações sobre como travar a velocidade do modem. Certifique-se de que a velocidade do dispositivo Cisco esteja configurada antes de emitir comandos para o modem através de uma sessão Telnet reversa. Novamente, consulte a Tabela 16-5 para obter informações sobre como configurar a velocidade do servidor de acesso ou roteador.

Para configurar o modem para uma sessão Telnet reversa, use o comando de configuração de linha **transport input telnet**. Para configurar um grupo rotativo (nesse caso, na porta 1), insira o comando de configuração de linha **rotary 1**. Colocar esses comandos na configuração de linha faz com que o IOS aloque ouvintes IP para conexões de entrada em intervalos de portas começando com os seguintes números básicos:

2000	protocolo Telnet
3000	Protocolo Telnet com rotação
4000	protocolo TCP bruto
5000	Protocolo TCP bruto com rotação
6000	protocolo Telnet, modo binário
7000	protocolo Telnet, modo binário com rotação
9000	protocolo Xremote
10000	Protocolo XRemote com rotação

Para iniciar uma sessão Telnet reversa no modem, execute as seguintes etapas:

1. Em seu terminal, use o comando **telnet ip-address 20yy** onde *ip-address* é o endereço IP de qualquer interface ativa conectada no dispositivo Cisco e yy é o número da linha à qual o modem está conectado.Por exemplo, o comando a seguir conectaria você à porta auxiliar em um roteador Cisco 2501 com o endereço IP 192.169.53.52: **telnet 192.169.53.52 2001**. Geralmente, um comando Telnet desse tipo pode ser emitido de qualquer lugar na rede, se puder **fazer ping** no endereço IP em questão.**Observação:** na maioria dos roteadores Cisco, a porta 01 é a porta auxiliar. Em um servidor de acesso Cisco, a porta auxiliar é o último TTY +1. Por exemplo, a porta auxiliar em um 2511 é a porta 17 (16 portas TTY + 1). Use sempre o comando exec **show line** para localizar o número de porta auxiliar - particularmente nas séries 2600 e 3600, que usam números de porta não contíguos para acomodar tamanhos de módulo assíncrono variáveis.
2. Se a conexão for recusada, pode indicar que não há ouvinte no endereço e na porta especificados ou que alguém já está conectado a essa porta. Verifique o endereço da conexão e o número da porta. Além disso, certifique-se de que o comando **modem inout** ou **modem DTR-ative**, assim como **transport input all**, apareçam sob a configuração de linha para as linhas que estão sendo alcançadas.Se estiver usando a função de rotação, verifique se o comando *rotary n* também aparece na configuração de linha onde n é o número do grupo de rotação. Para verificar se alguém já está conectado, faça telnet para o roteador e use o comando **show line *n*** . Procure um asterisco para indicar que a linha está em uso. Verifique se o CTS está alto e se o DSR não está. Use o comando **clear line *n*** para desconectar a sessão atual na porta número n. Se a conexão ainda for recusada, o modem

pode estar afirmando Carrier Detect (CD) o tempo todo. Desconecte o modem da linha, estabeleça uma sessão Telnet reversa e conecte o modem.

3. Depois de fazer a conexão Telnet com êxito, digite AT e certifique-se de que o modem responde com OK.
4. Se o modem não estiver respondendo, consulte a tabela a seguir.

A Tabela 16-1 abaixo descreve as possíveis causas dos sintomas de problemas de conectividade de modem para roteador e descreve as soluções para esses problemas.

Tabela 16-1: Sem conectividade entre modem e roteador

Possíveis causas	Ações sugeridas

O controle do modem não está ativado no servidor de acesso ou roteador	1. Use o comando exec **show line** no servidor de acesso ou roteador. A saída da porta auxiliar deve mostrar **InOut** ou **RIisCD** na coluna Modem. Isso indica que o controle do modem está ativado na linha do servidor de acesso ou roteador. Para obter uma explicação da saída da **linha show**, consulte "Using Debug Commands" (Usando Comandos de Depuração) no capítulo 15.
	2. Configure a linha para controle de modem usando o comando de configuração de linha **modem inout**. O controle do modem agora está ativado no servidor de acesso.
	Exemplo: O exemplo a seguir ilustra como configurar uma linha para chamadas de entrada e saída:
	`line 5`
	`modem inout`
	Nota: Certifique-se de usar o comando **modem inout** e não o comando **modem dialin** enquanto a conectividade do modem estiver em questão. Este último comando permite que a linha aceite apenas chamadas de entrada. As chamadas efetuadas serão recusadas e será impossível estabelecer uma sessão Telnet com o modem para configurá-las. Se quiser usar o comando **modem dialin**, faça isso somente depois de ter certeza de que o modem está funcionando corretamente.

O modem pode estar configurado incorret	Insira **AT&FE1Q0** para retornar aos padrões de fábrica e verificar se o modem está definido como caracteres de eco e saída de retorno. O modem pode ter uma sessão suspensa. Use **"^U"** para limpar a linha e **"^Q"** para abrir o controle de fluxo (XON). Verifique as configurações de paridade.

amente ou ter uma sessão suspensa.	
Cabeamento incorreto	1. Verifique o cabeamento entre o modem e o servidor de acesso ou roteador. Confirme se o modem está conectado à porta auxiliar no servidor de acesso ou roteador com um cabo RJ-45 enrolado e um adaptador MMOD DB-25. Essa configuração de cabeamento é recomendada e suportada pela Cisco para portas RJ-45. (Esses conectores são tipicamente denominados "Modem".) 2. Use o comando exec **show line** para verificar se o cabeamento está correto. Veja a explicação da saída do comando **show line** na seção intitulada "Using Debug Commands" (Usando Comandos de Depuração) no capítulo 15.
Problema de hardware	1. Verifique se você está usando o cabeamento correto e se todas as conexões estão boas. 2. Verifique se há danos em todo o hardware, incluindo cabeamento (fios quebrados), adaptadores (pinos soltos), portas do servidor de acesso e modem. 3. Consulte o Capítulo 3, "Troubleshooting Hardware and Booting Problems" (Solução de problemas de hardware e inicialização) para obter mais informações sobre como solucionar problemas de hardware.

Usando grupos giratórios

Para alguns aplicativos, os modems em um determinado roteador precisam ser compartilhados por um grupo de usuários. O Cisco Dialout Utility é um exemplo desse tipo de aplicativo. Basicamente, os usuários se conectam a uma porta que os conecta a um modem disponível. Para adicionar uma linha assíncrona a um grupo rotativo, basta inserir **rotary *n*** onde *n* é o número do grupo rotativo na configuração da linha assíncrona. Consulte o exemplo abaixo.

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

```
 flowcontrol hardware
```

A configuração de linha acima permitiria que os usuários se conectassem ao grupo giratório inserindo **telnet 192.169.53.52 3001** para telnet normal. As alternativas incluem as portas 5001 para Raw TCP, 7001 para binary telnet (que o Cisco Dialout Utility usa) e 10001 para conexões Xremote.

Observação: para verificar a configuração do Cisco Dialout Utility, clique duas vezes no ícone do utilitário de discagem na parte inferior direita da tela e pressione o botão More>. Em seguida, pressione o botão Configure Ports> (Configurar portas). Verifique se a porta está no intervalo 7000, se estiver usando grupos giratórios, e no intervalo 6000, se o utilitário Dialout estiver direcionando um modem individual. Você também deve ativar o registro de modem no PC. Isso é feito selecionando-se a seguinte sequência: **Iniciar->Painel de Controle-> modems**->(escolha o modem de discagem da Cisco)->**Propriedades**->**Conexão**->**Avançado**...->**Gravar um arquivo de log**.

Interpretando a Saída do Show Line

A saída do comando exec **show line** ***line-number*** é útil ao Troubleshoot um servidor de modem para acesso ou uma conexão de roteador. Abaixo está a saída do 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#
```

Quando ocorrem problemas de conectividade, uma saída importante é exibida nos campos Estado do modem e Estado do hardware do modem.

Observação: o campo Modem hardware state não aparece na saída **show line** para cada plataforma. Em alguns casos, as indicações para estados de sinal serão exibidas no campo Modem state (Estado do modem).

A Tabela 16-2 mostra as strings típicas de estado do modem e de estado do hardware do modem da saída do comando **show line**. Também explica o significado de cada estado.

Tabela 16-2: Estado do modem e do hardware do modem na saída show line

Estado do modem	Estado do hardware do modem	Significado
Ocioso	CTS noDSR DTR RTS	Esses são os estados de modem apropriados para conexões entre um servidor de acesso ou roteador e um modem (quando não há chamada recebida). A saída de qualquer outro tipo geralmente indica um problema.
Pronto	-	Se o estado do modem for Ready (Pronto), em vez de Idle (Ocioso), considere o seguinte: 1. O controle do modem não está configurado no servidor de acesso ou roteador. Configure o servidor de acesso ou roteador com o comando de configuração de linha **modem inout**. 2. Existe uma sessão na linha. Use o comando exec **show users** e use o comando exec privilegiado **clear line** para interromper a sessão, se desejado. 3. O DSR é alto. Há duas razões possíveis para isso: Problemas de cabeamento. Se o seu conector usa DB-25 pinos 6 e não tem pino 8, você deve mover o pino de 6 para 8 ou obter o conector apropriado.O modem configurado para DCD está sempre alto. O modem deve ser reconfigurado para ter DCD alto apenas com um CD(1). Isso geralmente é feito com o comando modem **&C1**, mas verifique a documentação do modem para saber a sintaxe exata do modem.

		Se o software não suportar o controle de modem, você deve configurar a linha do servidor de acesso à qual o modem está conectado com o comando de configuração de linha **no exec**. Limpe a linha com o comando exec privilegiado **clear line**, inicie uma sessão Telnet reversa com o modem e reconfigure o modem para que o DCD esteja alto apenas no CD. Termine a sessão Telnet inserindo **disconnect** e reconfigure a linha do servidor de acesso com o comando exec line configuration.
Pronto	noCTS noDSR DTR RTS (2)	A string noCTS aparece no campo Estado do hardware do modem por um dos quatro motivos a seguir: 1. O modem está desligado. 2. O modem não está conectado corretamente ao servidor de acesso. Verifique as conexões de cabeamento do modem para o servidor de acesso. 3. Cabeamento incorreto (MDCE enrolado ou MDTE direto, mas sem os pinos movidos). A configuração de cabeamento recomendada é fornecida anteriormente nesta tabela. 4. O modem não está configurado para controle de fluxo de hardware. Use o comando de configuração de linha **no flowcontrol hardware** para desativar o controle de fluxo de hardware no servidor de acesso. Em seguida, ative o controle de fluxo de hardware no modem por meio de uma sessão Telnet reversa. (Consulte a documentação do modem e consulte a seção "Estabelecendo uma Sessão Telnet Reversa para um Modem" no início deste capítulo.) Reative o controle de fluxo de hardware no servidor de acesso com o comando de configuração de linha **flowcontrol hardware**.
Pronto	CTS DSR DTR RTS	A string DSR (em vez da string noDSR) aparece no campo Estado do hardware do modem por um dos seguintes motivos: 1. Cabeamento incorreto (MDCE enrolado ou MDTE direto, mas sem os pinos

	(2)	movidos). A configuração de cabeamento recomendada é fornecida anteriormente nesta tabela. 2. O modem está configurado para DCD sempre alto. Reconfigure o modem para que o DCD esteja alto apenas no CD. Isso geralmente é feito com o comando modem **&C1**, mas verifique a documentação do modem para saber a sintaxe exata do modem. Configure a linha do servidor de acesso à qual o modem está conectado com o comando de configuração de linha **no exec**. Limpe a linha com o comando exec privilegiado **clear line**, inicie uma sessão Telnet reversa com o modem e reconfigure o modem para que o DCD esteja alto apenas no CD. Encerre a sessão Telnet inserindo **disconnect**. Reconfigure a linha do servidor de acesso com o comando exec line configuration.
Pronto	CTS* DSR* DTR RTS (2)	Se essa string aparecer no campo Modem hardware state, o controle do modem provavelmente não está ativado no servidor de acesso. Use o comando de configuração de linha **inout de modem** para ativar o controle de modem na linha. Informações adicionais sobre como configurar o controle de modem em um servidor de acesso ou linha de roteador são fornecidas anteriormente nesta tabela.

(1) CD = Detecção da portadora

(2) Uma * ao lado de um sinal indica uma de duas coisas: O sinal mudou nos últimos segundos ou o sinal não está sendo usado pelo método de controle de modem selecionado.

Reunindo informações de desempenho do modem

Esta seção explica os métodos para coletar dados de desempenho nos modems digitais MICA encontrados na família de servidores de acesso Cisco AS5x00. Os dados de desempenho podem ser usados para análise de tendências e são úteis na solução de problemas de desempenho que possam ser encontrados. Ao olhar para os números apresentados abaixo, tenha em mente que a perfeição não é possível no mundo real. A taxa de sucesso de chamada de modem (CSR) é uma função da qualidade dos circuitos, da base de usuário do modem cliente e do conjunto de modulações em uso. Uma porcentagem típica de CSR para chamadas V.34 é de 95%. Espera-se que as chamadas V.90 se conectem com êxito 92% do tempo. Quedas prematuras devem acontecer 10% do tempo.

Utilize os seguintes comandos para obter uma visão geral do comportamento do modem no

servidor de acesso:

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

As informações a seguir são úteis na solução de problemas de uma conexão de modem individual ou na coleta de dados para análise de tendência:

- debug modem csm
- modem call-record terse
- show modem op (MICA) / AT@E1 (Microcom) quando conectado
- show modem log para a sessão de interesse após a desconexão
- ANI (número do chamador)
- Hora do dia
- Revisão de hardware/firmware de modem cliente
- Informações interessantes do cliente (após desconexão)-ATI6, ATI11, AT&V, AT&V1 e assim por diante
- Um registro de áudio (arquivo .wav) da tentativa de trainup do modem cliente

Nas seções a seguir, os comandos serão explicados mais adiante e algumas tendências comuns serão discutidas.

Show Modem / Show Modem Summary

O comando **show modem** fornece uma visualização de modems individuais. A partir desses números, a integridade de modems individuais pode 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 os números agregados de todos os modems no roteador, use o 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%
```

Tabela 16-3: show modem Fields

Campos	Descrições
Chamadas de entrada e saída	Chamadas discando para dentro e para fora do modem. • Uso - percentual do tempo de atividade total do sistema durante o qual todos os modems estão em uso. • Êxito - Total de chamadas conectadas com êxito. • Falha - total de chamadas que não foram conectadas com êxito. • Disponível - total de modems disponíveis para uso no sistema.
Ocupado	Número total de vezes que os modems foram removidos do serviço com o comando **modem busy** ou o comando **modem shutdown**.
Falha na discagem	Número total de tentativas que os modems não desligaram ou não houve tom de discagem.
No Ans	Número total de vezes que o toque de chamada foi detectado, mas as chamadas não foram atendidas por um modem.
Succ Pct.	Porcentagem de conexão bem-sucedida do total de modems disponíveis.

[Saída Show Modem Call-Stats]

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

Tabela 16-4: show modem call-stats Fields

rmt Link	Isso mostra que a correção de erros estava em vigor e a chamada foi desligada pelo sistema cliente conectado ao modem remoto.
hostDrop	Isso mostra que a chamada foi desligada pelo sistema host do IOS. Alguns motivos comuns incluem: timeout de ociosidade, uma limpeza de circuito da companhia telefônica ou um termreq LCP PPP do cliente. A melhor maneira de determinar o motivo do desligamento é usando o

	modem call-record terse ou contabilidade AAA.

Os outros motivos de desconexão devem somar menos de 10% do total.

Saída Show Modem Connect-Speed

```
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
```

Esperamos ver uma distribuição de velocidades V.34. Deve haver um pico em 26,4, se os T1s usarem a sinalização associada ao canal (CAS). Para T1s ISDN (PRI), o pico deve ser 31.2. Além disso, procure algumas velocidades K56Flex, V.90. Se não houver conexões V.90, pode haver um problema de topologia de rede.

Entendendo o comando modem Call-Record Terse (11.3AA/12.0T)

Em vez de um comando exec, este é um comando de configuração colocado no nível do sistema do servidor de acesso em questão. Quando um usuário se desconecta, uma mensagem semelhante a esta é exibida:

```
*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

O comando exec **show modem operational-status** mostra os parâmetros atuais (ou mais recentes) relativos à conexão do modem.

A entrada de documentação para esse comando está na *Referência de Comandos de Soluções de Discagem do Cisco IOS versão 12.0*. **show modem operational-status** é apenas para modems MICA. O comando equivalente para modems Microcom é **modem at-mode / AT@E1**. Use o **comando modem at-mode <slot>/<port>** para conectar ao modem e execute o comando **AT@E1**. A documentação completa do comando **modem at-mode** pode ser encontrada no *Guia de Configuração do Software Cisco AS5300*, e a documentação do **AT@E1** está no *Conjunto de Comandos AT e no Resumo do Registro para Referência de Comandos dos Módulos de Modem Microcom*.

Execute as seguintes etapas para determinar em quais modems um usuário está entrando:

1. Emita o comando **show user** e procure o TTY ao qual eles estão conectados.
2. Use o comando **show line** e procure os números de slot/porta do modem.

Coletando dados de desempenho do lado do cliente

Para a análise de tendências, é muito importante coletar dados de desempenho do cliente. Tente sempre obter as seguintes informações:

- versão de firmware/modelo de hardware cliente (alcançável com o comando **ATI3I7** no modem do cliente)
- motivos de desconexão relatados pelo cliente (use **ATI6** ou **AT&V1**)

Outras informações disponíveis na extremidade do cliente incluem o modemlog.txt e o ppplog.txt do PC. Você deve configurar especificamente seu PC para gerar esses arquivos.

Analise os dados de desempenho

Depois de coletar e entender os dados de desempenho do seu sistema de modem, você precisará examinar os padrões e componentes restantes que possam precisar de aprimoramento.

Problemas com modems de servidor específicos

Use **show modem** ou **show modem call-stats** para identificar quaisquer modems com taxas anormalmente altas de falha de trainup ou taxas de desconexão defeituosas (MICA). Se os pares adjacentes de modems estiverem com problemas, o problema é provavelmente um DSP suspenso/inoperante. Use **copy flash modem** para recuperar o HMM afetado. Verifique se os modems estão executando a versão mais recente do portware. Para verificar se todos os modems estão configurados corretamente, use o comando de configuração **modem autoconfigure type mica/microcom_server** na configuração de linha. Para verificar se os modems estão sendo configurados automaticamente sempre que uma chamada é desligada, use o comando exec **debug confmodem**. Para corrigir modems mal configurados, talvez seja necessário estabelecer uma sessão Telnet reversa.

Problemas com DS0s específicos

Os problemas de DS0 são raros, mas possíveis. Para localizar DS0s com mau funcionamento, use o comando **show controller t1 call-counters** e procure quaisquer DS0s com TotalCalls anormalmente alto e TotalDuration anormalmente baixo. Para direcionar DS0s suspeitos, talvez seja necessário ocupar outros DS0s com o comando de configuração **isdn service dsl, ds0 busyout** na interface serial para o T1. A saída de **show controller t1 call-counters** é assim:

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

Obviamente, o timeslot 3 é o canal suspeito neste caso.

Tendências comuns adicionais

Abaixo estão algumas das tendências mais comuns vistas pelo Cisco TAC.

1. Caminhos de circuito defeituososVocê pode estar recebendo caminhos de circuito defeituosos através da PSTN (Public Switched Telephone Network) se tiver os seguintes problemas:chamadas de longa distância têm problemas, mas locais não (ou vice-versa)as chamadas em determinadas horas do dia apresentam problemasas chamadas de trocas remotas específicas têm problemas
2. Problemas com chamadas de longa distânciaSe o serviço de longa distância não estiver funcionando corretamente ou de forma alguma (mas o serviço local está bom):Certifique-se de que a linha digital se conecta a um switch digital, não a um banco de canais .Instrua as companhias telefônicas a examinar os caminhos de circuito usados para longa distância.
3. Problemas com chamadas de áreas de chamada específicas.Se as chamadas de regiões/trocas geográficas específicas tendem a ter problemas, você deve obter a topologia de rede da companhia telefônica.Se forem necessárias várias conversões analógicas para digitais, as conexões de modem V.90/K56flex não serão possíveis e o V.34 pode estar um pouco degradado. As conversões analógico-digital são necessárias em áreas atendidas por switches digitais não integrados ou por switches analógicos.

Operações ISDN

ISDN refere-se a um conjunto de serviços digitais que estão disponíveis para os usuários finais. A ISDN envolve a digitalização da rede telefônica de modo que voz, dados, texto, gráficos, música, vídeo e outro material de origem possam ser fornecidos aos usuários finais de um único terminal de usuário final sobre a fiação telefônica existente. Os proponentes da ISDN imaginam uma rede mundial muito parecida com a atual rede telefônica, mas com transmissão digital e uma variedade de novos serviços.

A ISDN é um esforço para padronizar os serviços de assinantes, as interfaces de usuário/rede e os recursos de rede e internetwork. A padronização dos serviços aos assinantes tenta garantir um nível de compatibilidade internacional. A padronização da interface usuário/rede estimula o desenvolvimento e a comercialização dessas interfaces por fabricantes terceirizados. A padronização dos recursos de rede e internetwork ajuda a alcançar o objetivo da conectividade mundial, garantindo que as redes ISDN se comuniquem facilmente entre si.

Os aplicativos de ISDN incluem aplicativos de imagem de alta velocidade (como o fac-símile Group IV), linhas telefônicas adicionais em residências para atender ao setor de telecomutação, transferência de arquivos de alta velocidade e videoconferência. A voz, é claro, também é um aplicativo popular para ISDN.

O mercado de acesso residencial está sendo dividido entre diferentes tecnologias. Nas áreas em que tecnologias mais recentes e mais baratas, como DSL e cabo, estão disponíveis, o mercado doméstico está se afastando da ISDN. As empresas, no entanto, continuam a usar a ISDN na forma de PRI T1/E1s para transportar grandes quantidades de dados ou para fornecer acesso de discagem v.90.

Componentes ISDN

Os componentes ISDN incluem terminais, adaptadores terminais (TAs), dispositivos de terminação de rede, equipamentos de terminação de linha e equipamentos de terminação de troca. Os terminais ISDN são fornecidos em dois tipos. Terminais ISDN especializados são

chamados de equipamento terminal tipo 1 (TE1). Terminais não ISDN, como DTE que precedem os padrões ISDN, são chamados de TE2 (terminal equipment type 2, equipamento terminal tipo 2). Os TE1s se conectam à rede ISDN por meio de um link digital de quatro fios e par trançado. Os TE2s se conectam à rede ISDN através de um adaptador de terminal. O TA ISDN pode ser um dispositivo autônomo ou uma placa dentro do TE2. Se o TE2 é implementado como um dispositivo autônomo, ele se conecta ao TA através de uma interface de camada física padrão. Os exemplos incluem EIA/TIA-232-C (anteriormente RS-232-C), V.24 e V.35.

Além dos dispositivos TE1 e TE2, o próximo ponto de conexão na rede ISDN é o dispositivo de terminação de rede tipo 1 (NT1) ou terminação de rede tipo 2 (NT2). Esses são dispositivos de terminação de rede que conectam o cabeamento de quatro fios do assinante ao loop local de dois fios convencional. Na América do Norte, o NT1 é um dispositivo CPE (Customer Premises Equipment, equipamento das instalações do cliente). Na maioria das outras partes do mundo, a NT1 faz parte da rede fornecida pela operadora. O NT2 é um dispositivo mais complicado, normalmente encontrado em PBXs (Digital Private Branch Exchange), que executa funções de protocolo das camadas 2 e 3 e serviços de concentração. Também existe um dispositivo NT1/2; é um único dispositivo que combina as funções de um NT1 e de um NT2.

Vários pontos de referência são especificados na ISDN. Esses pontos de referência definem interfaces lógicas entre agrupamentos funcionais, como TAs e NT1s. Os pontos de referência ISDN incluem:

- R-O ponto de referência entre equipamentos não ISDN e um TA
- S-O ponto de referência entre terminais de usuários e o NT2
- T-O ponto de referência entre os dispositivos NT1 e NT2
- U-O ponto de referência entre dispositivos NT1 e equipamento de terminação de linha na rede da operadora. O ponto de referência U é relevante apenas na América do Norte, onde a função NT1 não é fornecida pela rede da operadora

Veja a seguir um exemplo de configuração de ISDN. Este exemplo mostra três dispositivos conectados a um switch ISDN no escritório central. Dois desses dispositivos são compatíveis com ISDN, portanto podem ser conectados por meio de um ponto de referência S a dispositivos NT2. O terceiro dispositivo (um telefone padrão não ISDN) se conecta através do ponto de referência R a um TA. Qualquer um desses dispositivos também pode se conectar a um dispositivo NT1/2, que substituiria o NT1 e o NT2. E, embora não sejam mostradas, estações de usuário semelhantes são conectadas ao switch ISDN da extrema direita.

Um exemplo de configuração ISDN

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

Current configuration:
!
version 11.1
service timestamps debug datetime msec
service udp-small-servers
service tcp-small-servers
!
hostname 2503B
!
!
username 2503A password
ip subnet-zero
```

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

2503B#
```

Serviços ISDN

O serviço BRI (Basic Rate Interface Interface de Taxa Básica) da ISDN oferece dois canais B e um canal D (2B+D). O serviço BRI canal B opera a 64 kbps e destina-se a transportar dados do utilizador; O serviço de canal D BRI opera a 16 kbps e tem o objetivo de transportar informações de controle e sinalização, embora possa suportar a transmissão de dados do usuário em determinadas circunstâncias. O protocolo de sinalização do canal D compreende as camadas 1 a 3 do modelo de referência OSI. A BRI também oferece controle de enquadramento e outras despesas gerais, elevando sua taxa de bits total para 192 kbps. A especificação da camada física BRI é o ITU-T (International Telecommunication Union Telecommunications Standardization Setor, Setor de Padronização de Telecomunicações da União Internacional de Telecomunicações); anteriormente Comitê Consultivo para Telégrafo Internacional e Telefone [CCITT]) I.430.

O serviço ISDN PRI (Primary Rate Interface Interface de Taxa Primária) oferece 23 canais B e um canal D na América do Norte e no Japão, resultando em uma taxa de bits total de 1,544 Mbps (o canal D da PRI é executado a 64 kbps). A ISDN PRI na Europa, Austrália e em outras partes do mundo fornece 30 B mais um canal D de 64 kbps e uma taxa total de interface de 2,048 Mbps. A especificação da camada física PRI é ITU-T I.431.

Camada 1

Os formatos de quadro da camada física ISDN (Camada 1) diferem dependendo se o quadro é de

saída (do terminal para a rede) ou de entrada (da rede para o terminal). As duas interfaces da camada física são mostradas na Figura 16-1.

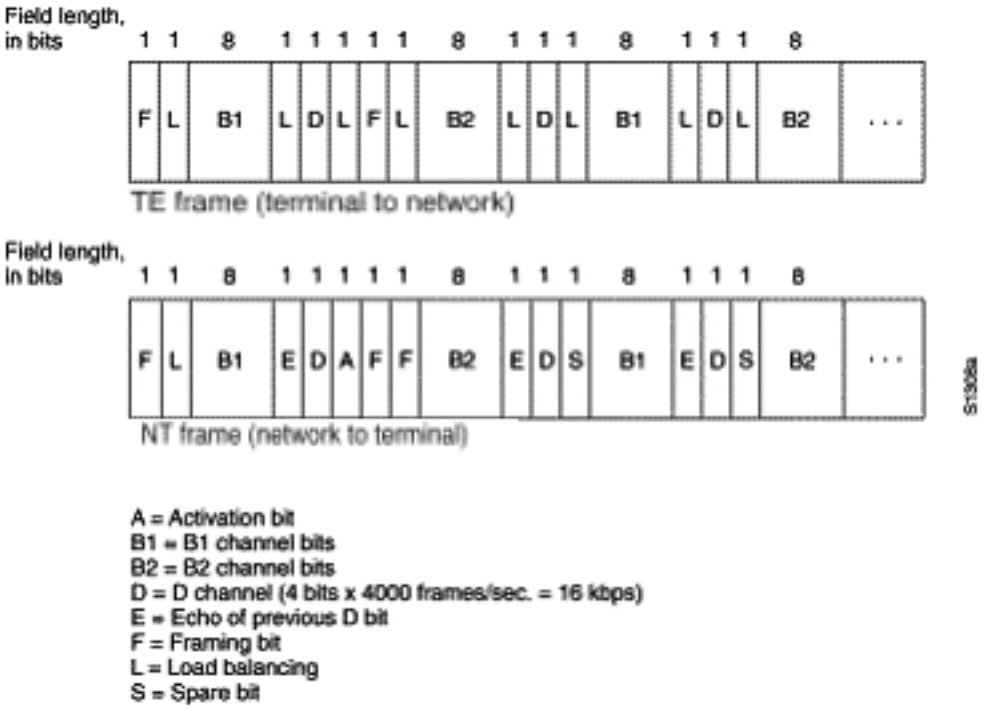

Figura 16-1: Formatos de quadros de camada física ISDN

Os quadros têm 48 bits de comprimento, dos quais 36 bits representam dados. Os bits de um quadro da camada física ISDN são usados da seguinte maneira:

- F - Fornece sincronização.
- L - Ajusta o valor médio do bit.
- E - Usado para resolução de contenção quando vários terminais em um barramento passivo disputam um canal.
- A - Ativa dispositivos.
- S - Não atribuído.
- B1, B2 e D - Para dados do usuário.

Vários dispositivos de usuário ISDN podem ser fisicamente conectados a um circuito. Nessa configuração, podem ocorrer colisões se dois terminais transmitirem simultaneamente. Portanto, a ISDN fornece recursos para determinar a contenção de link. Quando um NT recebe um bit D do TE, ele ecoa o bit na próxima posição do E-bit. O TE espera que o próximo bit E seja o mesmo do último bit D transmitido.

Os terminais não podem transmitir para o canal D a menos que detectem primeiro um número específico de uns (indicando "nenhum sinal") correspondente a uma prioridade pré-estabelecida. Se o TE detectar um bit no canal de eco (E) diferente de seus bits D, ele deverá parar de transmitir imediatamente. Essa técnica simples garante que apenas um terminal possa transmitir sua mensagem D de cada vez. Após a transmissão bem-sucedida da mensagem D, o terminal tem sua prioridade reduzida por ser necessário detectar mais mensagens contínuas antes da transmissão. Os terminais não podem aumentar sua prioridade até que todos os outros dispositivos na mesma linha tenham tido a oportunidade de enviar uma mensagem D. As conexões telefônicas têm prioridade mais alta do que todos os outros serviços, e as informações

de sinalização têm uma prioridade mais alta do que as informações de não sinalização.

Camada 2

A camada 2 do protocolo de sinalização ISDN é o Link Access Procedure no canal D, também conhecido como LAPD. O LAPD é semelhante ao HDLC (High-Level Data Link Control) e ao LAPB (Link Access Procedure, Balanced). Como a expansão da abreviação LAPD indica, ela é usada no canal D para garantir que o controle e a sinalização de informações fluam e sejam recebidos corretamente. O formato do quadro LAPD (consulte a Figura 16-2) é muito semelhante ao do HDLC e, como o HDLC, o LAPD usa supervisão, informações e quadros não numerados. O protocolo LAPD é formalmente especificado em ITU-T Q.920 e ITU-T Q.921.

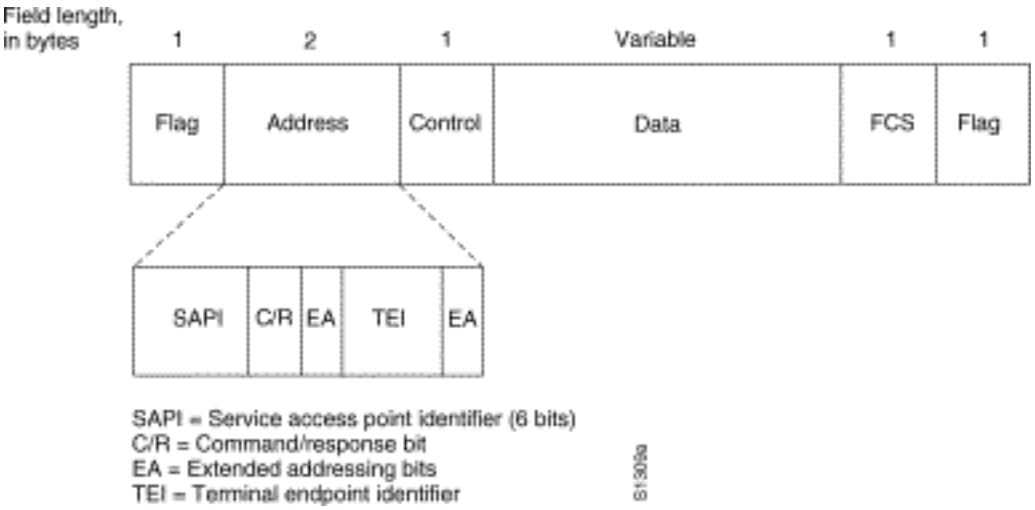

Figura 16-2: Formato de quadro LAPD

Os campos Flag e Controle de LAPD são idênticos aos do HDLC. O campo Endereço LAPD pode ter 1 ou 2 bytes de comprimento. Se o bit de endereço estendido do primeiro byte for definido, o endereço será de 1 byte; se não estiver definido, o endereço será 2 bytes. O primeiro byte do campo de endereço contém o Service Access Point Identifier (SAPI), que identifica o portal no qual os serviços LAPD são fornecidos à Camada 3. O bit C/R indica se o quadro contém um comando ou uma resposta. O campo do identificador de ponto final de terminal (TEI) identifica um único terminal ou vários terminais. Um TEI de todos os uns indica um broadcast.

Camada 3

Duas especificações de Camada 3 são usadas para sinalização ISDN: ITU-T (antigo CCITT) I.450 (também conhecido como ITU-T Q.930) e ITU-T I.451 (também conhecido como ITU-T Q.931). Juntos, esses protocolos oferecem suporte a conexões de usuário para usuário, comutadas por circuito e comutadas por pacotes. Várias mensagens de estabelecimento de chamada, encerramento de chamada, informações e diversas são especificadas, incluindo SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS e DISCONNECT.

Essas mensagens são funcionalmente semelhantes às fornecidas pelo protocolo X.25 (consulte o Capítulo 19, "Troubleshooting X.25 Connections", para obter mais informações). A Figura 16-3, da ITU-T I.451, mostra os estágios típicos de uma chamada comutada por circuito ISDN.

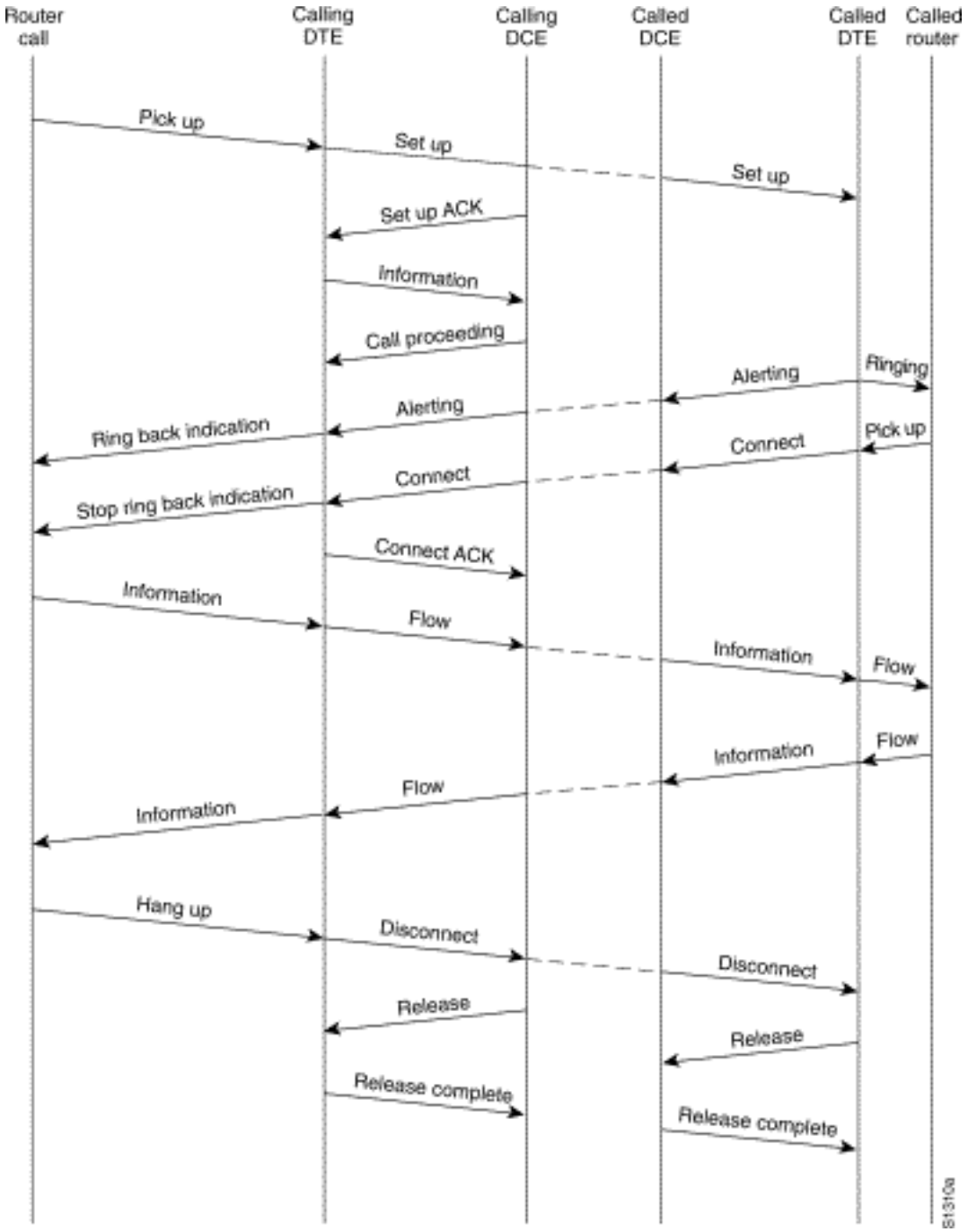

Figura 16-3 Estágios de chamada comutada por circuito ISDN

Interpretando a Saída do Show ISDN Status

Para descobrir qual é a condição atual da conexão ISDN entre o roteador e o switch da companhia telefônica, use o comando **show isdn status**. Os dois tipos de interfaces suportadas por este comando são a BRI e a 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
```

Tabela 16-5:- show isdn status for BRI

Campo	Importância
Status da camada 1: DESATIVADO	Isso indica que a interface BRI não está vendo um sinal na linha. Há cinco razões possíveis para essa condição. • A interface BRI está desligada. Verifique a configuração para o comando **shutdown** na interface BRI ou procure uma indicação administrativamente down no comando **show interface**. Use o utilitário de configuração e insira **no shutdown** na interface BRI. Insira o comando **clear interface bri** no prompt exec para verificar se a interface BRI foi reiniciada. • Existe um problema com o cabeamento. Você precisará substituir o cabo. Certifique-se de usar um cabo RJ-45 straight-through. Para verificar o cabo, segure as extremidades do cabo RJ-45 lado a lado. Se os pinos estiverem na mesma ordem, o cabo é direto. Se a ordem dos pinos for invertida, o cabo será enrolado. Substitua o cabo. • A porta ISDN BRI de um roteador pode exigir um dispositivo NT1. Na ISDN, o NT1 é um dispositivo que fornece a interface entre o equipamento das instalações do cliente e o equipamento de comutação da central. Se o roteador não tiver uma NT1 interna, obtenha e conecte uma NT1 à porta BRI. Verifique se a BRI ou o adaptador de terminal está conectado à porta S/T do NT1. Consulte a documentação do fabricante para verificar o funcionamento correto do NT1 externo. • A linha pode não estar funcionando. Entre em contato com a transportadora para confirmar a operação da conexão e

	verificar as configurações de tipo de switch. • Verifique se o roteador está funcionando corretamente. Se houver hardware defeituoso ou defeituoso, substitua-o conforme necessário.

Status da camada 2: Estado = TEI_ASSIGNED	Verifique a configuração do tipo de switch e SPIDS. A configuração do switch ISDN específico da interface substituirá a configuração do switch global. O status do SPID indicará se o switch aceitou o SPIDS (válido ou inválido). Entre em contato com o provedor de serviços para verificar a configuração configurada no roteador. Para alterar as configurações de SPID, use o comando de configuração da interface **isdn *spidn.*** Onde *n* é 1 ou 2, dependendo do canal em questão. Use a forma **no** desse comando para remover o SPID especificado.
	`isdn spidn spid-number [ldn]`
	`no isdn spidn spid-number [ldn]`
	Descrição da sintaxe:
	`spid-number`
	O número que identifica o serviço ao qual você se inscreveu. Esse valor é atribuído pelo provedor de serviços ISDN e geralmente é um número de telefone de 10 dígitos com dígitos adicionais.
	`ldn`
	(Opcional) Número de diretório local (LDN), que é um número de 7 dígitos atribuído pelo provedor de serviços. O switch na mensagem de configuração de entrada fornece essas informações. Se você não incluir o acesso do diretório local ao switch, ele será permitido, mas o outro canal B poderá não receber chamadas. Para ver as negociações da camada 2 entre o switch e o roteador, use o comando exec privilegiado **debug isdn q921**. As depurações q921 estão documentadas na *Referência de Comando de Depuração*. As depurações dependem muito dos recursos da CPU, portanto, tenha cuidado ao utilizá-las.

```
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#
```

Se o comando **show isdn status** não funcionar ou não mostrar o PRI, tente usar o comando **show isdn service**. Verifique se o comando **pri-group** aparece na configuração sob o controlador T1/E1 na configuração. Se o comando não estiver presente, configure o controlador com o comando **pri-group**.

A seguir está um exemplo de configuração para um roteador Cisco com um controlador T1/PRI canalizado:

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

Tabela 16-6: show isdn status para PRI

Campo	Importância
Status da camada 1: DESATIVADO	Isso indica que a interface PRI não está vendo o enquadramento T1/E1 na linha. Considere as seguintes possíveis causas para esta condição: • A interface PRI está desligada. Verifique a configuração do comando **shutdown** na interface serial0:23 ou procure uma indicação administrativamente inativa no comando **show interface**. Use o utilitário de configuração e insira **no shutdown** na interface em questão. Insira o comando **clear controller T1/E1** *n* no prompt exec para verificar se a interface PRI foi reiniciada. • Existe um problema com o cabeamento. Você precisará substituir o cabo. Certifique-se de usar um cabo RJ-45 straight-through. Para verificar o cabo, segure as extremidades do cabo RJ-45 lado a lado. Se os pinos estiverem na mesma ordem, o cabo é direto. Se a ordem dos pinos for invertida, o cabo será enrolado. Substitua o cabo. • A linha pode não estar funcionando. Entre em contato com a transportadora para confirmar a operação da conexão e verificar as configurações de tipo de switch. • Verifique se o roteador está funcionando

	corretamente. Se houver hardware defeituoso ou defeituoso, substitua-o conforme necessário.
Status da camada 2: Estado = TEI_ASSIGNED	Verifique a configuração do tipo de switch. A configuração do switch ISDN específico da interface substituirá a configuração do switch global. Verifique se T1/E1 está configurado para corresponder ao switch do provedor (problemas T1/E1 são discutidos no Capítulo 15). Para ver as negociações da camada 2 entre o switch e o roteador, use o comando exec privilegiado **debug isdn q921**. As depurações q921 estão documentadas na *Referência de Comando de Depuração*. As depurações dependem muito dos recursos da CPU, portanto, tenha cuidado ao utilizá-las.
Número de chamadas / Blocos de controle de chamadas em uso / Total de blocos de controle de chamadas ISDN alocados	Esses números indicam quantas chamadas estão em andamento e o número de recursos alocados para suportar essas chamadas. Se o número de BCC atribuídos for superior ao número de BCC que estão a ser utilizados, considere que pode haver um problema na publicação de BCC. Verifique se há CCBs disponíveis para chamadas recebidas.

Roteamento de discagem por demanda: Operações da interface do discador

O Roteamento de Discagem sob Demanda (DDR - Dial on Demand Routing) é um método de fornecer conectividade de WAN de forma econômica, conforme a necessidade, como um link principal ou como backup para um link serial não discado.

Uma **interface de discador** é definida como qualquer interface de roteador capaz de fazer ou receber uma chamada. Esse termo genérico deve ser diferenciado do termo **interface do discador** (com um D maiúsculo), que se refere a uma interface lógica configurada para controlar uma ou mais interfaces físicas de um roteador e que é vista em uma configuração de roteador como interface Dialer X. A partir deste ponto, salvo indicação em contrário, usaremos o termo discador no seu sentido genérico.

A configuração da interface do discador tem dois tipos: dialer map-based (às vezes chamado de DDR legado) e dialer files (perfis de discador). O método usado depende das circunstâncias em que você precisa de conectividade de discagem. O DDR baseado em mapa de discador foi introduzido pela primeira vez no IOS versão 9.0, perfis de discador na versão 11.2 do IOS.

Discagem

No fundo, o DDR é apenas uma extensão de roteamento em que *pacotes interessantes* são roteados para uma interface de discador, acionando uma tentativa de discagem. As seções a seguir explicam os conceitos envolvidos na definição de tráfego interessante e explicam o roteamento usado para conexões DDR.

Pacotes interessantes

Interessante é o termo usado para descrever pacotes ou tráfego que disparará uma tentativa de discagem ou, se um link de discagem já estiver ativo, redefinirá o temporizador de ociosidade na interface do discador. Para que um pacote seja considerado interessante:

- o pacote deve atender aos critérios de "permissão" definidos por uma lista de acesso
- a lista de acesso deve ser referenciada pela lista de discadores ou o pacote deve ser de um protocolo universalmente permitido pela lista de discadores
- a lista de discadores deve ser associada a uma interface de discador usando um dialer-group

Os pacotes nunca são automaticamente considerados interessantes (por padrão). As definições de pacotes interessantes devem ser explicitamente declaradas em uma configuração de roteador ou servidor de acesso.

Grupo de Discadores

Na configuração de cada interface de discador no roteador ou no servidor de acesso, deve haver um comando **dialer-group**. Se o comando **dialer-group** não estiver presente, não há um link lógico entre as definições de pacotes interessantes e a interface. A sintaxe do comando:

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

O número do grupo é o número do grupo de acesso do discador ao qual a interface específica pertence. Esse grupo de acesso é definido com o comando **dialer-list**. Os valores aceitáveis são diferentes de zero, inteiros positivos entre 1 e 10.

Uma interface pode ser associada somente a um único grupo de acesso de discador; atribuição de grupo de discador múltiplo não permitida. Uma segunda atribuição de grupo de acesso de discador substituirá a primeira. Um grupo de acesso de discador é definido com o comando **dialer-group**. O comando **dialer-list** associa uma lista de acesso a um grupo de acesso de discador.

Os pacotes que correspondem ao grupo de discadores especificado disparam uma solicitação de conexão.

O endereço de destino do pacote é avaliado em relação à lista de acesso especificada no comando **dialer-list** associado. Se ela passar, uma chamada é iniciada (se nenhuma conexão já tiver sido estabelecida) ou o temporizador de ociosidade é redefinido (se uma chamada estiver

conectada no momento).

Lista de discadores

O comando de configuração global **dialer-list** é usado para definir uma lista de discadores DDR para controlar a discagem por protocolo ou por uma combinação de protocolo e lista de acesso. Pacotes interessantes são aqueles que correspondem à permissão de nível de protocolo ou que são permitidos pela lista no comando **dialer-list**: **dialer-list dialer-group protocol protocol-name {permit | negar | list** *access-list number* **| grupo de acesso}**

dialer-group é o número de um grupo de acesso de discador identificado em qualquer comando de configuração de interface dialer-group.

protocol-name é uma das seguintes palavras-chave de protocolo: appletalk, bridge, clns, clns_es, clns_is, decnet, decnet_router-L1, decnet_router-L2, decnet_node, ip, ipx, vines ou xns.

permit permite o acesso a um protocolo inteiro.

deny nega o acesso a um protocolo inteiro.

list especifica que uma lista de acesso será usada para definir uma granularidade mais fina que um protocolo inteiro.

access-list-number - números de lista de acesso especificados em qualquer DECnet, Banyan VINES, IP, Novell IPX ou listas de acesso estendidas ou padrão XNS, incluindo listas de acesso e tipos de bridging do Novell IPX Extended Service Access Point (SAP). Consulte a Tabela 16-7 para obter os tipos e números da lista de acesso suportados.

nome da lista de filtros *do grupo de acesso* usado nos comandos **clns filter-set** e **clns access-group**.

Tabela 16-7: Numeração Da Lista De Acesso Por Protocolo

Tipo de lista de acesso	Intervalo de números da lista de acesso (decimal)
Apple Talk	600-699
Banyan VINES (standard)	1-100
Banyan VINES (estendido)	101-200
DECnet	300-399
IP (padrão)	1-99
IP (estendido)	100-199
Novell IPX (padrão)	800-899
IPX Novell (estendido)	900-999
Bridging Transparente	200-299
XNS	500-599

Lista de acesso

Para cada protocolo de rede a ser enviado através da conexão de discagem, uma lista de acesso pode ser configurada. Para fins de controle de custos, geralmente é desejável configurar uma lista de acesso para impedir que certos tráfegos, como atualizações de roteamento, ativem ou mantenham uma conexão. Observe que quando criamos listas de acesso com o objetivo de definir tráfego interessante e desinteressante, não declaramos que pacotes desinteressantes não podem cruzar o link de discagem. Estamos apenas indicando que eles não reinicializarão o temporizador de ociosidade, nem trarão uma conexão por conta própria. Enquanto a conexão de discagem estiver ativa, os pacotes não interessantes ainda poderão fluir pelo link.

Por exemplo, um roteador que executa o EIGRP como seu protocolo de roteamento pode ter uma lista de acesso configurada para declarar os pacotes EIGRP desinteressantes e todos os outros tráfegos IP interessantes:

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

As listas de acesso podem ser configuradas para todos os protocolos que podem atravessar o link de discagem. Lembre-se de que, para qualquer protocolo, o comportamento padrão na ausência de uma instrução **de permissão da lista de acesso** é negar todo o tráfego. Se não houver uma lista de acesso e nenhum comando **dialer-list** permitindo o protocolo, esse protocolo não será interessante. Na prática real, se não houver uma lista de discadores para um protocolo, esses pacotes não fluirão pelo link.

Exemplo - Juntando tudo

Com todos os elementos no lugar, você pode examinar o processo completo pelo qual o status "interessante" de um pacote é determinado. Neste exemplo, IP e IPX são os protocolos que podem atravessar o link de discagem. O usuário deseja impedir que broadcasts e atualizações de roteamento iniciem uma chamada ou mantenham o link ativo.

```
!
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
!
```

Um pacote deve ser permitido pelas instruções **access-list 121**, antes de atravessar a **interface assíncrona 1**, para ser considerado *interessante*. Nesse caso, os pacotes EIGRP são negados, assim como qualquer outro pacote de broadcast, enquanto todo o tráfego IP restante é permitido. Lembre-se de que isso não impede que os pacotes EIGRP transitem pelo link. Isso significa apenas que esses pacotes não reiniciarão o temporizador de ociosidade ou iniciarão uma

tentativa de discagem.

Da mesma forma, a **lista de acesso 903** declara as solicitações IPX RIP, SAPs e GNS como não interessantes, enquanto todo o tráfego IPX restante é interessante. Sem essas instruções de negação, a conexão de discagem provavelmente nunca cairia e uma conta de telefone muito grande resultaria, já que os pacotes desses tipos fluem constantemente em uma rede IPX.

Com **dialer-group 7** configurado na interface assíncrona, sabemos que **dialer-list 7** é necessário para ligar os filtros de tráfego interessantes (ou seja, listas de acesso) à interface. Uma instrução **dialer-list** é necessária (e *apenas* uma pode ser configurada) para cada protocolo, certificando-se de que o número da lista do discador é igual ao número do grupo do discador na interface.

Mais uma vez, é importante lembrar que as instruções *deny* nas listas de acesso configuradas para definir o tráfego interessante ***não*** impedem que os pacotes negados cruzem o link.

Usando o comando **debug dialer**, você pode ver a atividade que disca:

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

Aqui vemos que o tráfego IP com um endereço de origem 172.16.1.111 e um endereço de destino 172.16.2.22 disparou uma tentativa de discagem na interface assíncrona1.

Roteamento

Depois de definidos, os pacotes interessantes devem ser roteados corretamente para que uma chamada seja iniciada. O processo de roteamento depende de duas coisas: entradas da tabela de roteamento e uma interface "up" sobre a qual rotear pacotes.

Interfaces - up/up (falsificação)

Para que os pacotes sejam roteados para e através de uma interface, essa interface deve ser up/up conforme visto em uma saída **show interfaces**:

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

O que acontece com uma interface de discador que não está conectada? Se o protocolo não estiver ativo e em execução na interface, a implicação é que a interface em si não estará ativa. As rotas que dependem dessa interface serão liberadas da tabela de roteamento e o tráfego não será roteado para essa interface. O resultado é que nenhuma chamada seria iniciada pela interface.

A solução para combater essa possibilidade é permitir o estado **up/up (spoofing)** para interfaces de discador. Qualquer interface pode ser configurada como uma interface de discador. Por exemplo, uma interface serial ou assíncrona pode ser transformada em um discador adicionando o comando **dialer in-band** ou **dialer dtr** à configuração da interface. Essas linhas são desnecessárias para interfaces que são, por natureza, uma interface de discador (BRIs e PRIs). A saída de um comando show interface será semelhante a esta:

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

Em outras palavras, a interface "finge" ser **up/up** para que as rotas associadas permaneçam em vigor e para que os pacotes possam ser roteados para a interface.

Há circunstâncias em que uma interface de discador não será **up/up (spoofing)**. A saída **show interface** pode mostrar a interface como administrativamente inativa:

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

Administrativamente desativado significa apenas que a interface foi configurada com o comando **shutdown**. Esse é o estado padrão de qualquer interface de roteador quando o roteador é inicializado pela primeira vez. Para corrigir isso, use o comando de configuração de interface **no shutdown**.

A interface também pode ser vista como estando no modo de espera:

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

Esse estado indica que a interface foi configurada como backup para outra interface. Quando uma conexão exige redundância em caso de falha, uma interface de discador pode ser configurada como backup. Isso é feito adicionando os seguintes comandos à interface da conexão principal:

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

Depois que o comando **backup interface** tiver sido configurado, a interface usada como backup será colocada no modo de espera até que a interface primária atinja um estado de **inatividade/inatividade**. Nesse momento, a interface do discador configurada como um backup irá para um estado de **up/up (spoofing)** pendente de um evento de discagem.

Rotas estáticas e rotas estáticas flutuantes

A maneira mais segura de rotear pacotes para uma interface de discador é com o roteamento estático. Essas rotas são inseridas manualmente na configuração do roteador ou do servidor de acesso com o comando:

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

prefixo: Prefixo de rota IP para o destino.

máscara: Máscara de prefixo para o destino.

endereço: Endereço IP do próximo salto que pode ser usado para acessar a rede de destino.

interface: Interface de rede a ser usada para tráfego de saída.

distância : (Opcional) Uma distância administrativa. Este argumento é usado em rotas estáticas flutuantes.

As rotas estáticas são usadas em situações em que o link de discagem é a única conexão com o local remoto. Uma rota estática tem um valor de distância administrativa de um (1), o que a torna preferida sobre rotas dinâmicas para o mesmo destino.

Por outro lado, as rotas estáticas flutuantes - isto é, rotas estáticas com uma distância administrativa predefinida - são normalmente usadas em cenários DDR de backup. Nesses cenários, um protocolo de roteamento dinâmico, como RIP ou EIGRP, roteia pacotes pelo link primário.

Uma rota estática normal (distância administrativa = 1) é preferível ao EIGRP (distância administrativa = 90) ou ao RIP (distância administrativa = 120). A rota estática faz com que os pacotes sejam roteados através da linha de discagem, mesmo que o principal esteja ativo e seja capaz de passar tráfego. Se, no entanto, a rota estática for configurada com uma distância administrativa superior à de qualquer um dos protocolos de roteamento dinâmico em uso no roteador, a rota estática flutuante será usada somente na ausência de uma rota "melhor" - uma com uma distância administrativa mais baixa.

Se o Backup DDR estiver sendo invocado pelo uso do comando **backup interface**, a situação é um pouco diferente. Como a interface do discador permanece no modo de espera enquanto o primário está **ativo**, uma rota estática ou uma rota estática flutuante pode ser configurada. A interface do discador não tentará se conectar até que a interface primária fique **inativa/inativa**.

Para uma determinada conexão, o número de rotas estáticas (ou estáticas flutuantes) necessárias é uma função do endereçamento nas interfaces do discador. Nos casos em que as duas interfaces de discador (uma em cada um dos dois roteadores) compartilham uma rede ou sub-rede comum, normalmente é necessária apenas uma rota estática. Ele aponta para a LAN remota usando o endereço da interface do discador do roteador remoto como o endereço do próximo salto.

Examples

Exemplo 1: Discar é a única conexão que usa interfaces numeradas. Uma rota é suficiente.

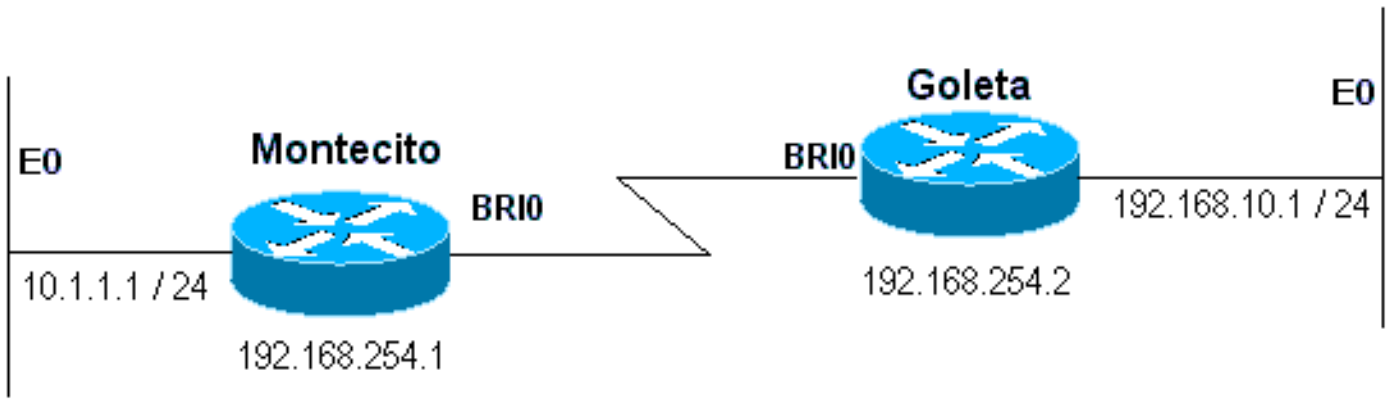

Figura 16-4: Discar usando interfaces numeradas

```
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
```

Exemplo 2: Discar é a única conexão que usa interfaces não numeradas. Isso pode ser configurado com apenas uma rota, mas é comum configurar duas rotas: uma rota de host para a interface LAN no roteador remoto e uma rota para a LAN remota através da interface LAN remota. Isso é feito para evitar problemas de mapeamento de Camada3 para Camada2, que podem resultar em falhas de encapsulamento.

Esse método também é usado se as interfaces do discador nos dois dispositivos estiverem numeradas, mas não na mesma rede ou sub-rede.

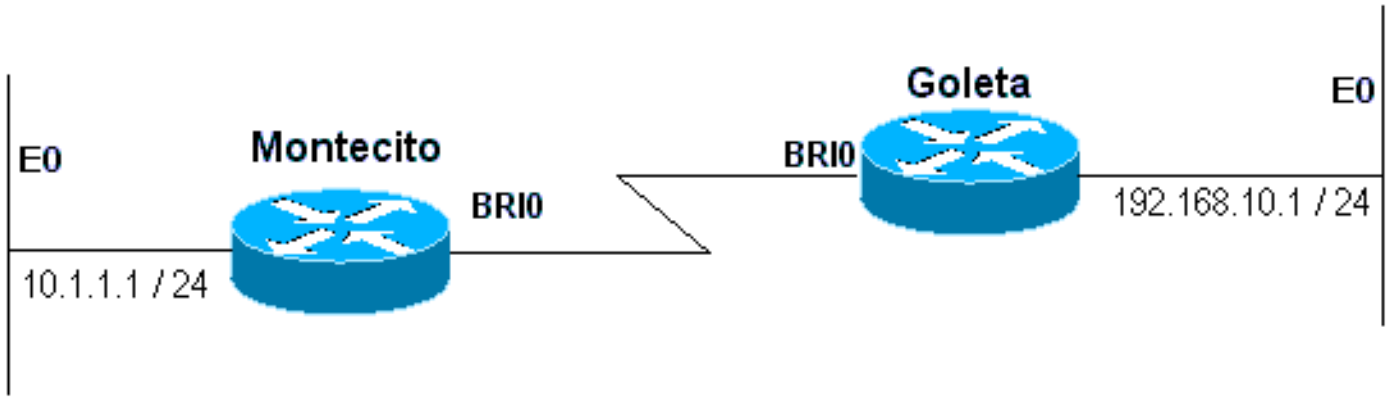

Figura 16-5: Discar usando interfaces não numeradas

```
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
```

Exemplo 3: Discar é uma conexão de backup usando interfaces numeradas. É necessária uma rota estática flutuante.

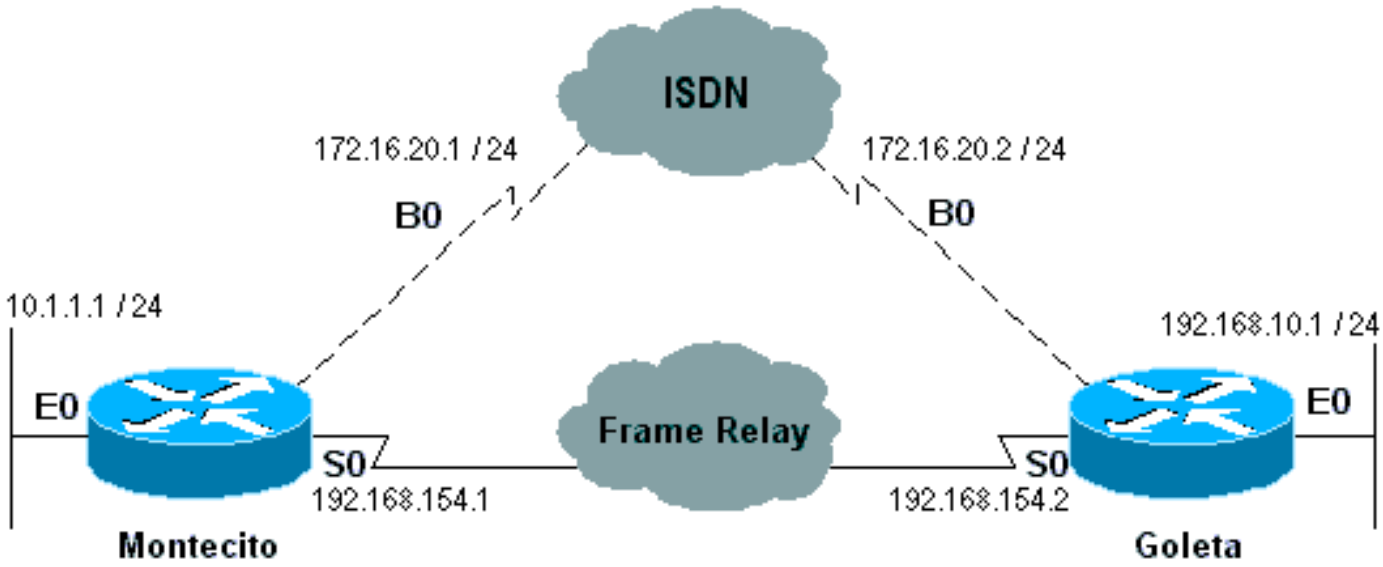

Figura 16-6: Backup usando interfaces numeradas

```
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
```

Exemplo 4: Discar é uma conexão de backup usando interfaces não numeradas. Como no Exemplo 2 acima, esse método também é usado se as interfaces do discador nos dois dispositivos forem numeradas, mas não na mesma rede ou sub-rede.

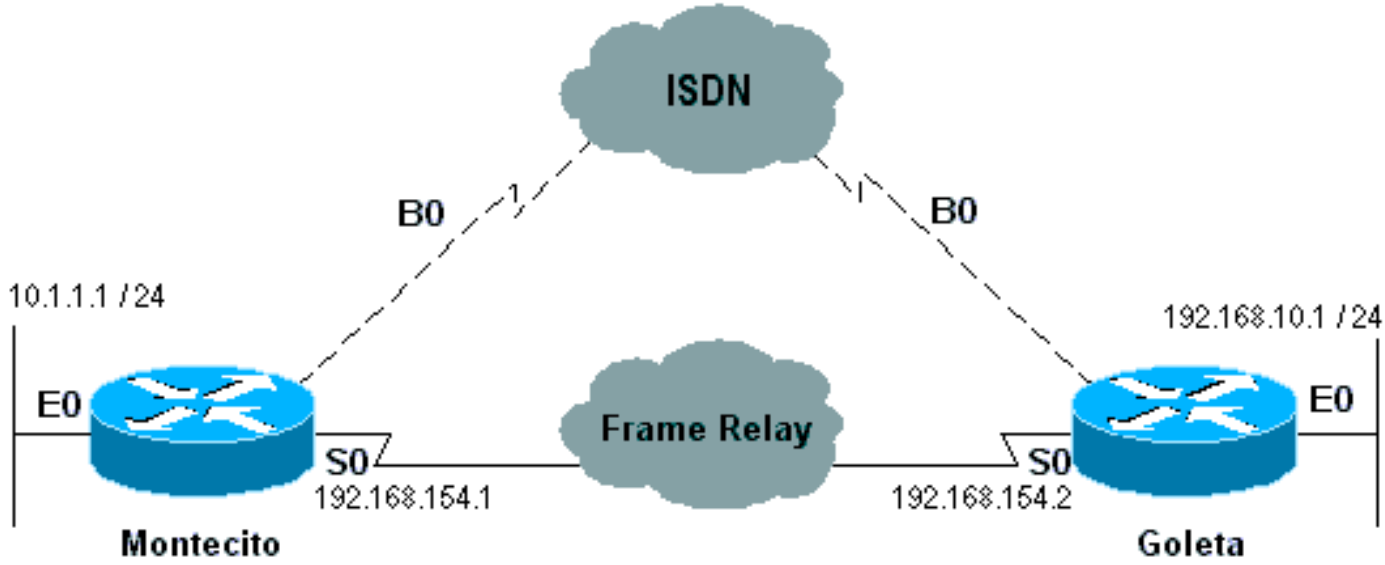

Figura 16-7: Backup usando interfaces não numeradas

```
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 do discador

O DDR baseado em mapa de discador (legado) é poderoso e abrangente, mas suas limitações afetam o dimensionamento e a extensibilidade. O DDR baseado em mapa de discador é baseado em um enlace estático entre a especificação de chamada por destino e a configuração da interface física.

No entanto, o DDR baseado em mapa de discador também tem muitos pontos fortes. Suporta Frame Relay, CLNS ISO, LAPB, roteamento de instantâneos e todos os protocolos roteados suportados nos roteadores Cisco. Por padrão, o DDR baseado em mapa de discador suporta comutação rápida.

Ao configurar uma interface para chamada de saída, um mapa de discador deve ser configurado para cada destino remoto e para cada número chamado diferente no destino remoto. Por exemplo, se você quiser uma conexão PPP Multilink ao discar de uma BRI ISDN para outra interface BRI ISDN que tenha um número de diretório local diferente para cada um de seus canais B, precisará de um mapa de discador para cada um dos 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
!
```

A ordem na qual os mapas de discador são configurados pode ser importante. Se dois ou mais comandos dialer map se referirem ao mesmo endereço remoto, o roteador ou o servidor de acesso tentará um após o outro, em ordem, até que ele estabeleça uma conexão com êxito

Observação: o IOS pode criar dinamicamente mapas de discadores em um roteador que recebe uma chamada. O mapa do discador é criado com base no nome de usuário autenticado e no endereço IP negociado do chamador. Os mapas de discador dinâmico só podem ser vistos na saída do comando **show dialer map**. Você não pode exibi-los na configuração atual do roteador ou do servidor de acesso.

Sintaxe do comando

Use a seguinte forma do comando de configuração de interface **dialer map** para:

- configurar uma interface serial ou uma interface ISDN para ligar para um ou vários locais, ou
- receber chamadas de vários sites.

Todas as opções são exibidas nessa primeira forma do comando. Para excluir uma entrada de mapa de discador específica, use uma forma **no** desse 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]]
```

Use a seguinte forma do comando **dialer map** para:

- configurar uma interface serial ou uma interface ISDN para fazer uma chamada para vários locais e
- para autenticar chamadas de vários sites.

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

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

Use a seguinte forma do comando **dialer map** para configurar uma interface serial ou uma interface ISDN para suportar bridging.

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

Use a seguinte forma do comando **dialer map** para configurar uma interface assíncrona para fazer uma chamada para:

- um único site que requer um script do sistema ou que não tem um script de modem atribuído, ou
- vários locais em uma única linha, em várias linhas ou em um grupo rotativo de discador.

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

Descrição da sintaxe

- *protocol* **-** Palavras-chave do protocolo. Use uma das seguintes opções: **appletalk, bridge, clns, decnet, ip, ipx, novell, snapshot, vines ou xns.**
- *next-hop-address* - O endereço do protocolo usado para corresponder aos endereços para os quais os pacotes são destinados. Este argumento não é usado com a palavra-chave **bridge** protocol.
- **name** - (Opcional) Indica o sistema remoto com o qual o roteador ou servidor de acesso local se comunica. Usado para autenticar o sistema remoto em chamadas recebidas.
- *hostname* - (Opcional) Nome sensível a maiúsculas e minúsculas ou ID do dispositivo remoto (geralmente o nome do host). Para roteadores com interfaces ISDN, o campo *hostname* pode conter o número que a ID da linha chamadora fornece (nos casos em que a identificação da linha chamadora, também conhecida como *CLI* , *identificador de chamada* e *identificação automática de número (ANI), está disponível).*
- **spc** - (Opcional) Especifica uma conexão semipermanente entre o equipamento do cliente e a troca. É usado somente na Alemanha para circuitos entre um ISDN BRI e um switch ISDN 1TR6 e na Austrália para circuitos entre um ISDN PRI e um switch TS-014.
- **velocidade 56 | 64** - (Opcional) Palavra-chave e valor que indicam a velocidade da linha em kilobits por segundo a utilizar. Usado somente para ISDN. A velocidade padrão é 64 kbps.
- **broadcast** - (Opcional) Indica que os broadcasts devem ser encaminhados para esse endereço de protocolo.
- **modem-script** - (Opcional) Indica o script de modem a ser usado para a conexão (para interfaces assíncronas).
- *modem-regexp* - (Opcional) Expressão regular à qual um script de modem será correspondido (para interfaces assíncronas).
- **system-script** - (Opcional) Indica o script do sistema a ser usado para a conexão (para interfaces assíncronas).
- *system-regexp* - (Opcional) Expressão regular à qual um script de sistema será correspondido (para interfaces assíncronas).
- *dial-string[:isdn-subaddress]* (Opcional) Número de telefone enviado ao dispositivo de discagem no reconhecimento de pacotes com um endereço de próximo salto especificado

que corresponda à lista de acesso definida (e o número de subendereço opcional usado para conexões multiponto ISDN). A sequência de discagem e o subendereço ISDN, se usados, devem ser o último item na linha de comando.

Perfis de discagem

Observação: nesta seção, o termo "interface do discador" refere-se à interface configurada; não a uma interface física no roteador ou no servidor de acesso.

A implementação de perfis de discador do DDR, introduzida no IOS versão 11.2, é baseada em uma separação entre a configuração de interface lógica e física. Os perfis de discador também permitem que as configurações lógicas e físicas sejam vinculadas dinamicamente por chamada.

A metodologia de perfis de discador é vantajosa quando você deseja:

- compartilhe uma interface (ISDN, serial assíncrona ou síncrona) para fazer ou receber chamadas
- alterar qualquer configuração por usuário (exceto o encapsulamento na primeira fase dos perfis de discador)
- bridge para muitos destinos
- evitar problemas de split horizon

Os perfis de discador permitem que a configuração de interfaces físicas seja separada da configuração lógica necessária para uma chamada e também permitem que as configurações lógicas e físicas sejam vinculadas dinamicamente por chamada.

Um perfil do Dialer consiste nos seguintes elementos:

- Uma configuração de *interface do discador* (uma entidade lógica), incluindo uma ou mais cadeias de discagem (cada uma delas é usada para acessar uma sub-rede de destino)
- Uma classe de *mapa de discador* que define todas as características de qualquer chamada para a cadeia de discagem especificada
- Um *pool de discadores* ordenado de interfaces físicas a serem usadas pela interface do discador

Todas as chamadas que vão de ou para a mesma sub-rede de destino usam o mesmo perfil de discador.

Uma configuração de interface do Discador inclui todas as configurações necessárias para acessar uma sub-rede de destino específica (e todas as redes alcançadas por ela). É possível especificar várias cadeias de discagem para a mesma interface do Discador; cada sequência de discagem pode ser associada a uma classe de mapa de discador diferente. A dialer map-class define todas as características de qualquer chamada para a sequência de discagem especificada. Por exemplo, a map-class para um destino pode especificar uma velocidade ISDN de 56 kbps. A classe de mapa para um destino diferente pode especificar uma velocidade ISDN de 64 kbps.

Cada interface do Discador usa um pool de discadores, que é um pool de interfaces físicas ordenadas com base na prioridade atribuída a cada interface física. Uma interface física pode pertencer a vários pools de discadores, com a contenção sendo resolvida por prioridade. As interfaces ISDN BRI e PRI podem definir um limite para o número mínimo e máximo de canais B reservados por quaisquer pools de discadores. Um canal reservado por um pool de discadores permanece ocioso até que o tráfego seja direcionado para o pool.

Quando os perfis de discador são usados para configurar o DDR, uma interface física não tem configurações exceto encapsulamento e os pools de discadores aos quais a interface pertence.

Nota: O parágrafo anterior tem uma exceção. Os comandos que se aplicam antes da conclusão da autenticação devem ser configurados na interface física (ou BRI ou PRI) e não no Perfil do discador. Os perfis de discador não copiam comandos de autenticação PPP (ou comandos LCP) para a interface física.

A Figura 16-8 mostra uma aplicação típica de perfis de discador. O Roteador A tem a interface 1 do discador para o roteamento de discagem por demanda com a sub-rede 1.1.1.0 e a interface 2 do discador para o roteamento de discagem por demanda com a sub-rede 2.2.2.0. O endereço IP da interface 1 do discador é seu endereço como um nó na rede 1.1.1.0. Ao mesmo tempo, esse endereço IP serve como o endereço IP das interfaces físicas usadas pela interface do discador 1. Da mesma forma, o endereço IP da interface de discador 2 é seu endereço como um nó na rede 2.2.2.0.

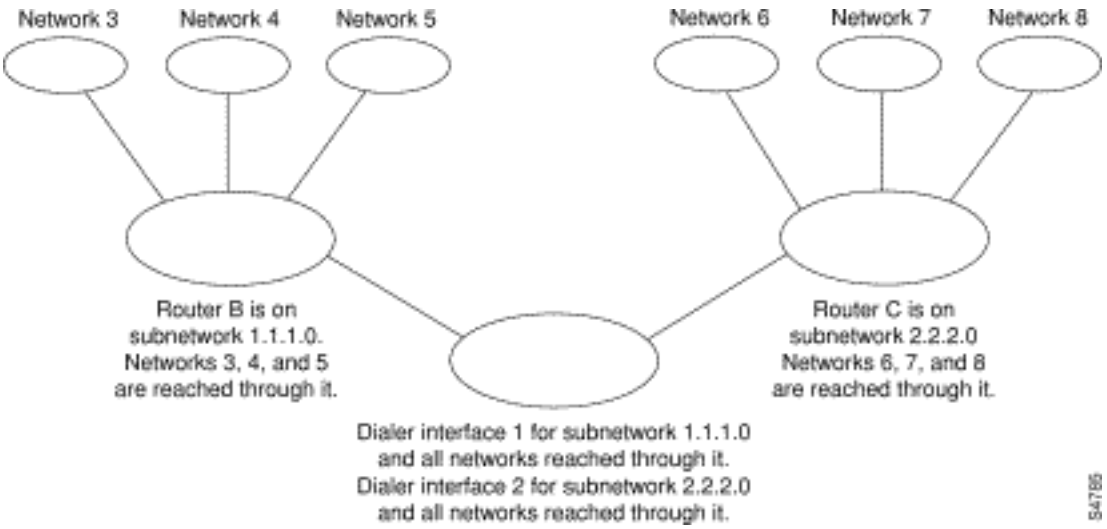

Figura 16-8: Aplicativo de Perfis de Discador Típico

Uma interface de discador usa apenas um pool de discadores. Uma interface física, no entanto, pode ser membro de um ou vários pools de discadores e um pool de discadores pode ter várias interfaces físicas como membros.

A Figura 16-9 ilustra as relações entre os conceitos de interface de discador, pool de discadores e interfaces físicas. A interface 0 do discador usa o conjunto de discadores 2. A interface física BRI 1 pertence ao pool de discadores 2 e tem uma prioridade específica no pool. A interface física BRI 2 também pertence ao conjunto de discadores 2. Como a contenção é resolvida com base nos níveis de prioridade das interfaces físicas no pool, a BRI 1 e a BRI 2 devem receber prioridades diferentes no pool. Talvez a BRI 1 tenha a prioridade 100 e a BRI 2 tenha a prioridade 50 no conjunto de discadores 2 (uma prioridade de 50 é maior que uma prioridade de 100). A BRI 2 tem uma prioridade mais alta no pool e suas chamadas serão feitas primeiro.

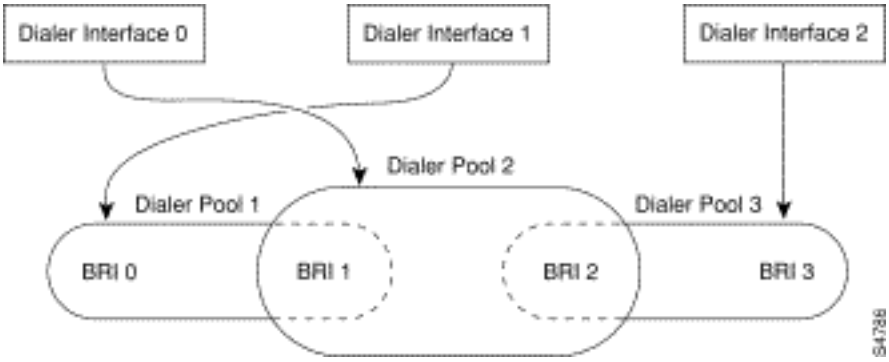

Figura 16-9: Relações entre interfaces de discador, pools de discadores e interfaces físicas

Etapas de configuração do perfil do discador

Comando	Propósito
interface dialer number	Crie uma interface do Dialer.
máscara **de endereço IP**	Especifique o endereço IP e a máscara da interface do discador como um nó na rede de destino a ser chamada.
encapsulamento ppp	Especifique o encapsulamento PPP.
dialer remote-name username	Especifique o nome de autenticação CHAP do roteador remoto.
dialer string dial-string class class-name	Especifique o destino remoto a ser chamado e a classe de mapa que define as características das chamadas a este destino.
dialer *poolnumber*	Especifique o pool de discagem a ser usado para chamadas para esse destino.
dialer-group group-number	Atribua a interface do Dialer a um grupo de discadores.
dialer-list dialer-group protocol protocol-name {permit | negar | list *access-list-number*}	Especifique uma lista de acesso por número da lista ou por protocolo e número da lista para definir os pacotes "interessantes" que podem disparar uma chamada.

Operações do PPP

O Point-to-Point Protocol (PPP) é de longe o protocolo de transporte de camada de enlace mais comum, tendo o SLIP completamente utilizado como o protocolo preferido para conexões seriais síncronas e assíncronas de discagem (e, em muitos casos, não discadas). O PPP foi originalmente definido em 1989 pelo RFC 1134, que desde então se tornou obsoleto por uma série de RFCs que culminaram (a partir dessa gravação) no RFC1661. Há também vários RFCs que definem elementos do protocolo, como RFC1990 (o PPP Multilink Protocol), RFC2125 (o

PPP Bandwidth Allocation Protocol) e muitos outros. Um repositório on-line de RFCs pode ser encontrado em:

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

Talvez a melhor definição de PPP possa ser encontrada no RFC1661, que afirma:

O protocolo de ponto a ponto (PPP) proporciona um método padrão para transporte de datagramas sobre links de ponto a ponto. O PPP é composto de três componentes principais:

1. Um método para encapsular datagramas multiprotocolo.
2. Um LCP (Link Control Protocol) para estabelecer, configurar e testar a conexão de enlace de dados.
3. Uma família de Network Control Protocols (NCPs) para estabelecer e configurar diferentes protocolos da camada de rede.

Fases da negociação de PPP

A negociação do PPP consiste em três fases: Link Control Protocol (LCP), autenticação e Network Control Protocol (NCP). Cada uma é processada na ordem, após o estabelecimento da conexão assíncrona ou ISDN.

LCP

O PPP não segue um modelo cliente/servidor. Todas as conexões são ponto-a-ponto. Portanto, quando há um chamador e um receptor, ambas as extremidades da conexão ponto-a-ponto devem concordar com os protocolos e parâmetros negociados.

Quando a negociação começa, cada um dos peers que deseja estabelecer uma conexão PPP deve enviar uma Solicitação de Configuração (vista na **negociação de ppp de depuração** e, em seguida, chamada CONFREQ). Estão incluídas na CONFREQ todas as opções que não são o padrão do link. Essas opções geralmente incluem Unidade de recepção máxima (MRU), Mapa de caracteres de controle assíncrono (ACCM), Protocolo de autenticação (AuthProto) e Número mágico. Também são vistas a Maximum Receive Reconstructed Unit (MRRU) e o Endpoint Discriminator (EndpointDisc), usados para PPP Multilink.

Há três respostas possíveis para qualquer CONFREQ:

- Configure-Acknowledge (CONFACK) deve ser emitido se o peer reconhecer as opções e concordar com os valores vistos no CONFREQ.
- Um Configure-Reject (CONFREJ) deve ser enviado se alguma das opções no CONFREQ não for reconhecida (por exemplo, algumas opções específicas do fornecedor) ou se os valores para qualquer uma das opções tiverem sido explicitamente despermitidos na configuração do peer.
- Um Configure-Negative-Acknowledge (CONFNAK) deve ser enviado se todas as opções no CONFREQ forem reconhecidas, mas os valores não forem aceitáveis para o peer.

Os dois peers continuam a trocar CONFREQs, CONFREJs e CONFNAKs até que cada um envie um CONFACK, até que a conexão de discagem seja interrompida ou até que um ou ambos os peers indiquem que a negociação não pode ser concluída.

Autenticação

Após a conclusão bem-sucedida da negociação de LCP e a obtenção de um acordo sobre AuthProto, a próxima etapa é a autenticação. A autenticação, embora não obrigatória por RFC1661, é altamente recomendada em todas as conexões de discagem. Em alguns casos, é um requisito para o funcionamento adequado; Perfis de discador sendo um caso em questão.

Os dois principais tipos de autenticação no PPP são o Password Authentication Protocol (PAP) e o Challenge Handshake Authentication Protocol (CHAP), definidos pelo RFC1334 e atualizados pelo RFC1994.

O PAP é o mais simples dos dois, mas é menos seguro porque a senha de texto simples é enviada através da conexão de discagem. O CHAP é mais seguro porque a senha de texto simples nunca é enviada pela conexão de discagem.

O PAP pode ser necessário em um dos seguintes ambientes:

- Uma grande base instalada de aplicativos clientes que não suportam CHAP
- Incompatibilidades entre as implementações de diferentes fornecedores de CHAP

Ao discutir a autenticação, é útil usar os termos "solicitante" e "autenticador" para distinguir as funções desempenhadas pelos dispositivos em cada extremidade da conexão, embora qualquer um dos pares possa atuar em qualquer função. "Requerente" descreve o dispositivo que solicita acesso à rede e fornece informações de autenticação; o "autenticador" verifica a validade das informações de autenticação e permite ou despermite a conexão. É comum que ambos os pares ajam em ambas as funções quando uma conexão DDR está sendo feita entre os roteadores.

PAP

O PAP é bastante simples. Após a conclusão bem-sucedida da negociação de LCP, o solicitante envia repetidamente sua combinação de nome de usuário/senha pelo link até que o autenticador responda com uma confirmação ou até que o link seja quebrado. O autenticador pode desconectar o link se determinar que a combinação nome de usuário/senha não é válida.

CHAP

O CHAP é um pouco mais complicado. O autenticador envia um desafio ao solicitante, que responde com um valor. Esse valor é calculado usando uma função de "hash unidirecional" para hash do desafio e da senha de CHAP juntos. O valor resultante é enviado ao autenticador junto com o nome de host CHAP do solicitante (que pode ser diferente do nome de host real) em uma mensagem de *resposta.*

O autenticador lê o nome do host na mensagem de resposta, procura a senha esperada para esse nome de host e, em seguida, calcula o valor que espera que o solicitante envie em sua resposta executando a mesma função de hash executada pelo solicitante. Se os valores resultantes corresponderem, a autenticação será bem-sucedida. A falha deve levar a uma desconexão.

AAA

Um serviço de autenticação, autorização e contabilização (AAA), como TACACS+ ou RADIUS, pode ser usado para realizar PAP ou CHAP.

NCP

Após a autenticação bem-sucedida, a fase NCP é iniciada. Como no LCP, os colegas trocam CONFREQs, CONFREJs, CONFNAKs e CONFACKs. No entanto, nessa fase de negociação, os elementos que estão sendo negociados têm a ver com protocolos de camada mais alta - IP, IPX, Bridging, CDP, etc. Um ou mais desses protocolos podem ser negociados. Como é o mais usado, e como outros protocolos operam da mesma maneira, o Internet Protocol Control Protocol (IPCP), definido em RFC1332, é o foco desta discussão. Outros RFCs pertinentes incluem, mas não se limitam a:

- RFC1552 (IPX Control Protocol)
- RFC1378 (AppleTalk Control Protocol)
- RFC1638 (Bridging Control Protocol)
- RFC1762 (DECnet Control Protocol)
- RFC1763 (Vines Control Protocol)

Além disso, o Cisco Discovery Protocol Control Protocol (CDPCP) pode ser negociado durante o NCP, embora isso não seja comum. Os engenheiros do Cisco TAC geralmente aconselham que o comando no cdp enable seja configurado em qualquer interface de discador e em todas as interfaces para evitar que os pacotes CDP mantenham uma chamada ativa indefinidamente.

O elemento principal negociado no IPCP é cada endereço de peer. Cada um dos pares está em um de dois estados possíveis; tem um endereço IP ou não. Se o peer já tiver um endereço, ele enviará esse endereço em um CONFREQ para o outro peer. Se o endereço for aceitável para o outro peer, um CONFACK será retornado. Se o endereço não for aceitável, a resposta será um CONFNAK contendo um endereço para o peer usar.

Se o peer não tiver endereço, ele enviará um CONFREQ com o endereço 0.0.0.0. Isso instrui o outro peer a atribuir um endereço, que é realizado pelo envio de um CONFNAK com o endereço correto.

Outras opções podem ser negociadas em IPCP. Geralmente vistos, são os endereços principal e secundário do Servidor de Nomes de Domínio e do Servidor de Nomes NetBIOS, conforme descrito em RFC1877 Informativo. O IP Compression Protocol (RFC1332) também é comum.

Metodologias alternativas de PPP

Metodologias alternativas de PPP incluem PPP multilink, PPP multichassi e perfis virtuais.

Multilink PPP

O recurso Multilink Point-to-Point Protocol (MLP) fornece funcionalidade de balanceamento de carga em vários links de WAN. Ao mesmo tempo, ele oferece interoperabilidade de vários fornecedores, fragmentação de pacotes e sequenciamento adequado e cálculo de carga no tráfego de entrada e saída. A implementação do PPP Multilink da Cisco suporta as especificações de fragmentação e sequenciamento de pacotes no RFC1717.

O PPP multilink permite que os pacotes sejam fragmentados. Esses fragmentos podem ser enviados ao mesmo tempo através de vários links ponto-a-ponto para o mesmo endereço remoto. Os vários links surgem em resposta a um limite de carga de discador que você define. A carga pode ser calculada no tráfego de entrada, de saída ou em qualquer um, conforme necessário para o tráfego entre os locais específicos. O MLP oferece largura de banda sob demanda e reduz

a latência de transmissão entre links de WAN.

O PPP multilink funciona nos seguintes tipos de interface (único ou múltiplo) configurados para suportar grupos giratórios de discagem sob demanda e encapsulamento PPP:

- interfaces seriais assíncronas
- BRIs
- PRI

Configuração

Para configurar o PPP Multilink em interfaces assíncronas, você configura as interfaces assíncronas para suportar o encapsulamento DDR e PPP. Em seguida, você configura uma interface do Discador para suportar encapsulamento PPP, largura de banda sob demanda e PPP Multilink. Em algum momento, no entanto, adicionar mais interfaces assíncronas não melhora o desempenho. Com o tamanho padrão de MTU, o PPP Multilink deve suportar três interfaces assíncronas usando modems V.34. No entanto, os pacotes podem ser descartados ocasionalmente se o MTU for pequeno ou se ocorrerem grandes rajadas de quadros curtos.

Para habilitar o PPP Multilink em uma única interface ISDN BRI ou PRI, você não precisa definir um grupo rotativo de discador separadamente porque as interfaces ISDN são grupos rotativos de discador por padrão. Se você não usar procedimentos de autenticação PPP, seu serviço de telefone deverá passar as informações de ID do chamador.

Énecessário um número de limite de carga. Para obter um exemplo de configuração do PPP Multilink em uma única interface BRI ISDN, consulte o *Exemplo de PPP Multilink em uma Interface ISDN* abaixo.

Quando o PPP Multilink estiver configurado e você quiser que um pacote multilink seja conectado indefinidamente, use o comando **dialer idle-timeout** para definir um temporizador de ociosidade muito alto. O comando **dialer-load threshold 1** não mantém um pacote multilink de *n* links conectados indefinidamente, e o comando **dialer-load threshold 2** não mantém um pacote multilink de dois links conectados indefinidamente.

Para habilitar o PPP Multilink em várias interfaces ISDN BRI ou PRI, você configura uma interface giratória do Discador e a configura para o PPP Multilink. Em seguida, você configura as BRIs separadamente e as adiciona ao mesmo grupo rotativo. Veja o *exemplo de PPP Multilink em várias interfaces ISDN* abaixo.

Exemplo de PPP Multilink em uma interface ISDN

O exemplo a seguir ativa o PPP Multilink na interface BRI 0. Quando uma BRI é configurada, nenhuma configuração de grupo rotativo de discador é necessária (a interface ISDN é um grupo rotativo por padrão).

```
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
```

Exemplo de PPP multilink em várias interfaces ISDN

O exemplo a seguir configura vários BRIs ISDN para pertencerem ao mesmo grupo rotativo de discador para PPP Multilink. Use o comando **dialer rotary-group** para atribuir cada uma das BRIs ISDN a esse grupo rotativo de discador, que deve corresponder ao número da interface do Discador (neste caso, o número 0).

```
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
```

PPP multilink multichassi

O PPP multilink fornece a capacidade de dividir e recombinar pacotes em um único sistema final através de um pipe lógico (também chamado de *pacote*) formado por vários links. O PPP multilink fornece largura de banda sob demanda e reduz a latência de transmissão entre links de WAN.

O Multilink PPP (MMP) multichassi, por outro lado, fornece a capacidade adicional para que os links terminem em vários roteadores com endereços remotos diferentes. O MMP também pode lidar com tráfego analógico e digital.

Esta funcionalidade destina-se a situações em que há grandes pools de usuários de discagem, nos quais um único servidor de acesso não pode fornecer portas de discagem suficientes. O MMP permite que as empresas forneçam um único número de discagem para seus usuários e apliquem a mesma solução para chamadas analógicas e digitais. Esse recurso permite que os provedores de serviços de Internet, por exemplo, aloquem um único número rotativo ISDN a várias PRIs ISDN em vários roteadores.

Para obter uma descrição completa dos comandos MMP aqui referenciados, consulte a *Referência de Comandos de Soluções de Discagem da Cisco*. Para localizar a documentação de outros comandos exibidos neste capítulo, use o comando reference master index ou pesquise on-line.

O MMP é suportado nas plataformas das séries Cisco 7500, 4500 e 2500 e nas interfaces serial

síncrona, serial assíncrona, BRI ISDN, PRI ISDN e Dialer.

O MMP não exige reconfiguração de switches da companhia telefônica.

Configuração

Os roteadores ou servidores de acesso são configurados para pertencer a grupos de pares, chamados de *grupos de pilha*. Todos os membros do grupo de pilhas são peers; os grupos de pilha não precisam de um roteador de lead permanente. Qualquer membro do grupo de pilha pode atender chamadas provenientes de um único número de acesso, que geralmente é um grupo de busca ISDN PRI. As chamadas podem ser recebidas de dispositivos de usuário remoto, como roteadores, modems, adaptadores de terminal ISDN ou placas de PC.

Quando uma conexão é estabelecida com um membro de um *grupo de pilha*, esse membro é proprietário da chamada. Se uma segunda chamada chegar do mesmo cliente e um roteador diferente atender a chamada, o roteador estabelece um túnel e encaminha todos os pacotes pertencentes à chamada para o roteador que possui a chamada. O processo de estabelecer um túnel e encaminhar chamadas através dele para o roteador proprietário da chamada é às vezes chamado de *projetar o link PPP para o mestre de chamada*.

Se um roteador mais potente estiver disponível, ele poderá ser configurado como um membro do grupo de pilhas e os outros membros do grupo de pilhas poderão estabelecer túneis e encaminhar todas as chamadas para ele. Nesse caso, os outros membros do grupo de pilhas estão apenas respondendo chamadas e encaminhando tráfego para o roteador mais potente de *descarregamento*.

Observação: as linhas WAN de alta latência entre os membros do grupo de pilha podem tornar a operação do grupo de pilha ineficiente.

As operações de tratamento de chamadas, ofertas e encaminhamento de Camada 2 do MMP no grupo da pilha prosseguem da seguinte maneira. Ele também é mostrado na Figura 16-10.

1. Quando a primeira chamada chega ao grupo de pilhas, o Roteador A responde.
2. No lance, o Roteador A vence porque já tem a chamada. O Roteador A torna-se o *call-master* dessa sessão com o dispositivo remoto. O Roteador A também pode ser chamado de *host para a interface do pacote mestre*.
3. Quando o dispositivo remoto que iniciou a chamada precisa de mais largura de banda, ele faz uma segunda chamada PPP Multilink para o grupo.
4. Quando a segunda chamada é recebida, o Roteador D a atende e informa o grupo da pilha. O Roteador A vence a licitação porque já está tratando a sessão com esse dispositivo remoto.
5. O Roteador D estabelece um túnel para o Roteador A e encaminha os dados brutos do PPP para o Roteador A.
6. O Roteador A reagrupa e resequencia os pacotes.
7. Se mais chamadas chegarem ao Roteador D e elas também pertencerem ao Roteador A, o túnel entre A e D se expande para lidar com o tráfego adicional. O roteador D não estabelece um túnel adicional para A.
8. Se mais chamadas chegarem e forem atendidas por qualquer outro roteador, esse roteador também estabelece um túnel para A e encaminha os dados brutos do PPP.
9. Os dados remontados são transmitidos na rede corporativa como se todos tivessem

passado por um link físico.

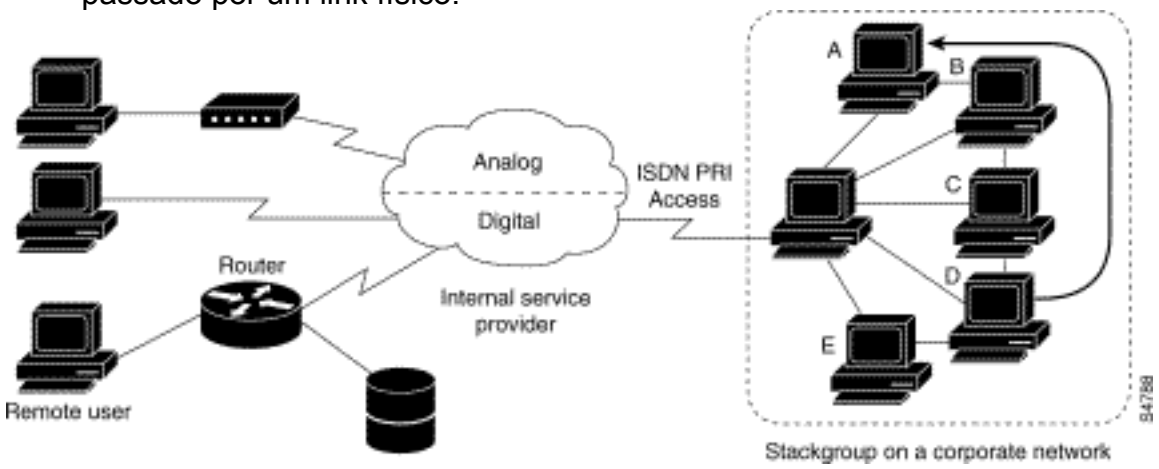

Figura 16-10: Cenário típico de PPP multilink de multichassi

Ao contrário da figura anterior, a Figura 16-11 apresenta um roteador de descarga. Os servidores de acesso que pertencem a um grupo de pilhas atendem chamadas, estabelecem túneis e encaminham chamadas para um roteador Cisco 4700 que ganha a licitação e é o call-master para todas as chamadas. O Cisco 4700 reagrupa e sequencia todos os pacotes que chegam através do grupo de pilha.

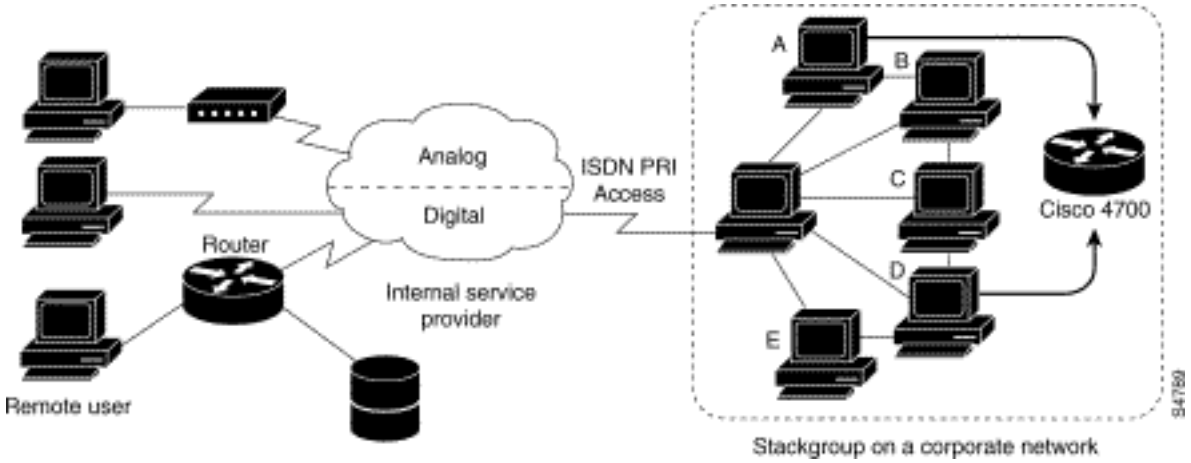

Figura 16-11: PPP multilink multichassi com um roteador de descarga como membro do grupo de pilha

Observação: você pode criar grupos de pilhas usando diferentes plataformas de servidor de acesso, switching e roteador. No entanto, servidores de acesso universal como o Cisco AS5200 não devem ser combinados com ISDN. Isso só deve ser feito com servidores de acesso, como a plataforma 4x00. Como as chamadas do escritório central são alocadas de forma arbitrária, essa combinação pode resultar na entrega de uma chamada analógica a um servidor de acesso somente digital, que não conseguiria lidar com a chamada.

O suporte a MMP em um grupo de roteadores exige que cada roteador seja configurado para suportar o seguinte:

- Multilink PPP
- Protocolo de oferta de grupo de pilha (SGBP)
- Modelo virtual usado para clonar a configuração de interface para suportar MMP

Perfis virtuais

Perfis virtuais é um aplicativo exclusivo do Point-to-Point Protocol (PPP) que pode criar e configurar uma interface de acesso virtual dinamicamente quando uma chamada de discagem é recebida e desativar a interface dinamicamente quando a chamada é encerrada. Os perfis virtuais funcionam com PPP direto e com PPP multilink (MLP).

As informações de configuração de uma interface de acesso virtual de perfis virtuais podem vir de uma interface de modelo virtual ou de uma configuração específica do usuário armazenada em um servidor de autenticação, autorização e contabilização (AAA), ou ambos.

A configuração AAA específica do usuário usada por Perfis virtuais é a configuração *da interface* e é baixada durante as negociações do LCP. Outro recurso, chamado Configuração por usuário, também usa informações de configuração obtidas de um servidor AAA. No entanto, a configuração por usuário usa a configuração *de rede* (como listas de acesso e filtros de rota) baixada durante as negociações do NCP.

Duas regras regem a configuração da interface de acesso virtual por interfaces de modelo virtual de perfis virtuais e configurações AAA:

- Cada aplicativo de acesso virtual pode ter, no máximo, um modelo do qual clonar. No entanto, ele pode ter várias configurações AAA a partir das quais clonar (informações AAA de perfis virtuais e Configuração AAA por usuário, que por sua vez pode incluir a configuração para vários protocolos).
- Quando os perfis virtuais são configurados pelo modelo virtual, seu modelo tem prioridade mais alta do que qualquer outro modelo virtual.

Consulte a seção "Interoperabilidade com outros recursos de discagem da Cisco" abaixo para obter uma descrição das possíveis sequências de configuração que dependem da presença ou ausência do MLP ou de outro recurso de acesso virtual que clona uma interface de modelo virtual.

Esse recurso é executado em todas as plataformas Cisco IOS que suportam MLP.

Para obter uma descrição completa dos comandos mencionados nesta seção, consulte o capítulo "Virtual Profiles Commands" (Comandos de Perfis Virtuais) na *Dial Solutions Command Reference* no conjunto de documentação do Cisco IOS. Para localizar a documentação de outros comandos exibidos neste capítulo, você pode usar o comando reference master index ou pesquisar on-line.

Informações de Apoio

Esta seção apresenta informações de fundo sobre Perfis virtuais para ajudá-lo a entender esse aplicativo antes de começar a configurá-lo.

Restrições

Recomendamos que endereços não numerados sejam usados em interfaces de modelo virtual para garantir que endereços de rede duplicados não sejam criados em interfaces de acesso virtual.

Prerequisites

O uso de informações de configuração de interface AAA específicas do usuário com Perfis

virtuais exige que o roteador seja configurado para AAA e exige que o servidor AAA tenha pares AV de configuração de interface específica do usuário. Os pares AV relevantes (em um servidor RADIUS) começam da seguinte maneira:

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

As informações que seguem o sinal de igual (=) podem ser qualquer comando de configuração de interface do Cisco IOS. Por exemplo, a linha pode ser a seguinte:

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

O uso de uma interface de modelo virtual com perfis virtuais exige que um modelo virtual seja definido especificamente para perfis virtuais.

Interoperabilidade com outros recursos de discagem da Cisco

Perfis virtuais interoperam com Cisco DDR, Multilink PPP (MLP) e discadores como ISDN.

Configuração DDR de interfaces físicas

Os perfis virtuais interoperam totalmente com interfaces físicas nos seguintes estados de configuração DDR quando nenhum outro aplicativo de interface de acesso virtual está configurado:

- Os perfis de discador são configurados para a interface. O perfil do discador é usado em vez da configuração de perfis virtuais.
- O DDR não está configurado na interface. Perfis virtuais substituem a configuração atual.
- O DDR legado é configurado na interface. Perfis virtuais substituem a configuração atual.

Observação: se uma interface de discador for usada (incluindo qualquer discador ISDN), sua configuração será usada na interface física em vez da configuração de Perfis virtuais.

Efeito PPP Multilink na configuração da interface de acesso virtual

Como mostrado na tabela 16-8, a configuração exata de uma interface de acesso virtual depende dos três fatores a seguir:

- Se os perfis virtuais estão configurados pelo modelo virtual, por AAA, por ambos ou por nenhum dos dois. Esses estados são mostrados como "VP VT apenas", "VP AAA apenas", "VP VT e VP AAA" e "No VP at all", respectivamente, na tabela.
- A presença ou ausência de uma interface de discador.
- A presença ou ausência de MLP. O rótulo de coluna "MLP" é um suporte para qualquer recurso de acesso virtual que suporte MLP e clones de uma interface de modelo virtual.

Na Tabela 16-8, "VT Multilink" significa que uma interface de modelo virtual é clonada *se* uma for definida para MLP ou um recurso de acesso virtual que usa MLP.

Tabela 16-8: Sequência de clonagem de configuração de perfis virtuais

Configur	Sem	Disca	Sem MLP sem	Nenhum

ação de perfis virtuais	discador MLP	dor MLP	discador	discador MLP
VP apenas VT	VP VT	VP VT	VP VT	VP VT
VP AAA apenas	VP AAA (Multilink VT)	VP AAA (Multilink VT)	VP AAA	VP AAA
VP VT e VP AAA	VP VT VP AAA	VP VT VP AAA	VP VT VP AAA	VP VT VP AAA
Nenhum VP	(VT Multilink)	Discador	Nenhuma interface de acesso virtual foi criada.	Nenhuma interface de acesso virtual foi criada.

A ordem dos itens em qualquer célula da tabela é importante. Onde o VP VT é mostrado acima do VP AAA, significa que primeiro o modelo virtual de perfis virtuais é clonado na interface e, em seguida, a configuração da interface AAA para o usuário é aplicada a ele. A configuração da interface AAA específica do usuário é adicionada à configuração e substitui qualquer interface física conflitante ou comandos de configuração de modelo virtual.

Interoperabilidade com outros recursos que usam modelos virtuais

Os perfis virtuais também interoperam com aplicativos de acesso virtual que clonam uma interface de modelo virtual. Cada aplicativo de acesso virtual pode ter, no máximo, um modelo do qual clonar, mas pode clonar de várias configurações AAA.

A interação entre perfis virtuais e outros aplicativos de modelo virtual é a seguinte:

- Se os perfis virtuais estiverem ativados e um modelo virtual for definido para ele, o modelo virtual de perfis virtuais será usado.
- Se os perfis virtuais forem configurados somente pelo AAA (nenhum modelo virtual é definido para perfis virtuais), o modelo virtual para outro aplicativo de acesso virtual (VPDN, por exemplo) poderá ser clonado na interface de acesso virtual.
- Um modelo virtual, se houver, é clonado para uma interface de acesso virtual antes da configuração de AAA de perfis virtuais ou da configuração de AAA por usuário. A AAA Per-User Configuration, se usada, é aplicada por último.

Terminology

Os termos novos ou incomuns a seguir são usados neste capítulo:

Par AV: Um parâmetro de configuração em um servidor AAA; parte da configuração do usuário que o servidor AAA envia ao roteador, em resposta a solicitações de autorização específicas do usuário. O roteador interpreta cada par AV como um comando de configuração do roteador Cisco IOS e aplica os pares AV em ordem. Neste capítulo, o termo par AV se refere a um parâmetro de

configuração de interface em um servidor RADIUS.

Um par AV de configuração de interface para Perfis virtuais pode assumir uma forma como esta:

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

clonagem: Criar e configurar uma interface de acesso virtual aplicando comandos de configuração a partir de um modelo virtual específico. O modelo virtual é a origem das informações genéricas do usuário e das informações dependentes do roteador. O resultado da clonagem é uma interface de acesso virtual configurada com todos os comandos no modelo.

interface de acesso virtual: Instância de uma interface virtual exclusiva que é criada dinamicamente e existe temporariamente. As interfaces de acesso virtual podem ser criadas e configuradas de forma diferente por diferentes aplicativos, como Perfis virtuais e redes de discagem virtual privada.

interface de modelo virtual: Configuração de interface genérica para determinados usuários ou para uma determinada finalidade, além de informações dependentes do roteador. Isso toma a forma de uma lista de comandos de interface do Cisco IOS a serem aplicados à interface virtual conforme necessário.

perfil virtual: Instância de uma interface de acesso virtual exclusiva que é criada dinamicamente quando determinados usuários entram e é interrompida dinamicamente quando a chamada é desconectada. O perfil virtual de um usuário específico pode ser configurado por uma interface de modelo virtual, configuração de interface específica do usuário armazenada em um servidor AAA ou por uma interface de modelo virtual e configuração de interface específica do usuário a partir do AAA.

A configuração de uma interface de acesso virtual começa com uma interface de modelo virtual (se houver), seguida pela aplicação de configuração específica do usuário para a sessão de discagem do usuário específico (se houver).

Exemplo anotado de negociação PPP

Neste exemplo, um ping ativa um link ISDN entre os roteadores *Montecito* e *Goleta*. Observe que, embora não haja timestamping neste exemplo, geralmente é recomendável que você use o comando de configuração global **service timestamps debug datetime msec**.

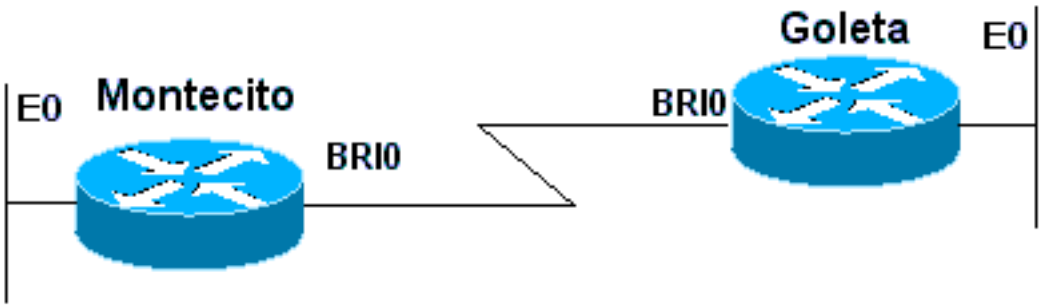

Figura 16-12: Roteador-ISDN-Roteador

Estas depurações são retiradas de *Montecito*; no entanto, a depuração no *Goleta* pareceria muito a mesma.

Observação: suas depurações podem aparecer em um formato diferente. Essa saída é o formato de saída de depuração PPP mais antigo, antes das modificações introduzidas no IOS versão 11.2(8). Consulte o Capítulo 17 para obter um exemplo de depuração de PPP em versões mais recentes do 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 - O tráfego é gerado para iniciar uma tentativa de discagem.

B - A conexão é estabelecida (depurações ISDN não usadas neste exemplo).

Iniciar LCP:

C - *Montecito* envia solicitações de configuração de LCP para AUTHTYPE e para MAGICNUMBER.

D - *Goleta* envia seus CONFREQs. Se o valor para MAGICNUMBER for o mesmo que o valor enviado por *Montecito*, há uma forte probabilidade de a linha estar em loop.

E - Indica que *Montecito* enviou reconhecimentos aos CONFREQs *de Goleta*.

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

Iniciar fase de autenticação:

G, H - *Montecito* e *Goleta* desafiam-se mutuamente para a autenticação.

J - *Goleta* responde ao desafio.

K, L - *Goleta* passa a autenticação com êxito.

M - Mensagem de *Goleta* a *Montecito*: autenticação bem-sucedida.

A negociação do NCP é iniciada:

N, P - Cada roteador envia seu endereço IP configurado em um CONFREQ.

Q, R - *Montecito* envia um CONFACK para o CONFREQ *de Goleta*.

S - ? e vice-versa.

T, U - Uma rota é instalada de *Montecito* a *Goleta* e o protocolo na interface é alterado para "ativado", indicando que as negociações do NCP foram concluídas com êxito.

Antes de ligar para a equipe do TAC da Cisco Systems

Antes de ligar para o Cisco Systems Technical Assistance Center (TAC), verifique se você leu este capítulo e concluiu as ações sugeridas para o problema do seu sistema.

Além disso, faça o seguinte e documente os resultados para que possamos auxiliá-lo melhor:

Para todos os problemas, colete a saída de **show running-config** e **show version**. Verifique se o comando **service timestamps debug datetime msec** está na configuração.

Para problemas de DDR, colete o seguinte:

- **show dialer map**
- **debug dialer**
- **negociação de debug ppp**
- **debug ppp authentication**

Se a ISDN estiver envolvida, colete:

- **show isdn status**
- **debug isdn q931**
- **debug isdn events**

Se houver modems envolvidos, colete:

- mostrar linhas
- show line [x]
- **show modem** (se modems integrados estiverem envolvidos)
- **show modem version** (se modems integrados estiverem envolvidos)
- **debug modem**
- **debug modem csm** (se modems integrados estiverem envolvidos)
- **debug chat** (se for um cenário DDR)

Se T1s ou PRIs estiverem envolvidos, colete:

- **show controller t1**

Informações Relacionadas

- Guia de soluções de discagem do Cisco IOS
- Visão geral sobre interfaces, controladores e linhas usados para acesso discado
- Roteamento através de linhas de modem

- Porta serial e configuração de tronco T1/E1
- Criação de Inter-redes DDR
- Decisão e Preparação para Configurar DDR
- Configurando o DDRtitle
- Visão geral da tecnologia PPP
- Projetando redes ISDN
- Tipos de Switch, códigos e valores ISDN
- Provisionamento da linha ISDN
- Suporte Técnico e Documentação - Cisco Systems