

Tecnologia dialup: Visões gerais e explicações

Índice

[Introdução](#)

[Antes de Começar](#)

[Convenções](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Operações do modem](#)

[Usando o comando modem autoconfigure](#)

[Estabelecendo uma sessão de Telnet reversa para um modem](#)

[Usando grupos giratórios](#)

[Interpretando a linha saída da mostra](#)

[Reunindo informações de desempenho do modem](#)

[Operações de ISDN](#)

[Componentes ISDN](#)

[Saída da interpretando exibição de status de ISDN](#)

[Roteamento por encomenda do seletor: Operações de interface do discador](#)

[Provocando um seletor](#)

[Mapas de discagem](#)

[Perfis de discador](#)

[Operações PPP](#)

[Fases da negociação de PPP](#)

[Metodologias de PPP alternado](#)

[Exemplo anotado de negociação PPP](#)

[Antes de chamar o equipe tac do Cisco Systems](#)

[Informações Relacionadas](#)

[Introdução](#)

Este capítulo introduz e explica algumas das Tecnologias usadas nas redes dialup. Você encontrará pontas da configuração e interpretações de alguns dos **comandos show**, que são úteis para verificar a operação correta da rede. Os procedimentos de Troubleshooting são além do alcance deste documento e podem ser encontrados no documento autorizado *pesquisar defeitos o Dialup*.

[Antes de Começar](#)

[Convenções](#)

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas](#)

[técnicas Cisco.](#)

Pré-requisitos

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. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Operações do modem

Esta seção explica as edições relativas especificamente à instalação, à verificação, e ao uso do Modems com roteadores Cisco.

Usando o comando modem autoconfigure

Se você está usando a liberação 11.1 do sistema operacional inter-redes Cisco (Cisco IOS) ou mais atrasado, você pode configurar seu roteador Cisco para comunicar-se com e configurar automaticamente seu modem.

Use o seguinte procedimento para configurar um roteador Cisco para tentar automaticamente descobrir que tipo de modem é conectado à linha, e para configurar então o modem:

1. Para descobrir o tipo de modem anexado a seu roteador, use o **comando modem autoconfigure discovery line configuration**.
2. Quando o modem é descoberto com sucesso, configurar o modem que usa automaticamente o **comando modem autoconfigure type modem-name line configuration**.

Se você quer indicar a lista de Modems para que o roteador tem entradas, use o *modem-nome do modemcap da mostra*. Se você quer mudar um valor do modem que esteja retornado do **comando show modemcap**, use o **comando modemcap edit modem-name attribute value line configuration**.

Para obter informações completas sobre do uso destes comandos, refira o *manual de configuração e o Dial Solutions Command Reference das soluções do seletor da documentação IOS Cisco*.

Nota: Não incorpore o **&W** à entrada de modemcap que é usada para o autoconfigure. Isto faz com que o NVRAM seja reescrito cada vez que um modem autoconfigure é executado e destruirá o modem.

Estabelecendo uma sessão de Telnet reversa para um modem

Para propósitos de diagnóstico, ou para configurar inicialmente o modem se você está executando o Cisco IOS Release 11.0 ou Anterior, você deve estabelecer uma sessão de Telnet

reversa para configurar um modem para comunicar-se com um dispositivo Cisco. Enquanto você trava a velocidade do modem do lado do equipamento de terminal de dados (DTE), o modem comunicar-se-á sempre com o servidor de acesso ou o roteador na velocidade desejada. Refira a tabela 16-5 para obter informações sobre de travar a velocidade do modem. Esteja certo que a velocidade do dispositivo Cisco está configurada antes de emitir comandos ao modem através de uma sessão de Telnet reversa. Além disso, refira a tabela 16-5 para obter informações sobre de configurar a velocidade do servidor de acesso ou do roteador.

Para configurar o modem para uma sessão de Telnet reversa, use o telnet de entrada de transporte do comando de configuração de linha. Para estabelecer um grupo giratório (neste caso, na porta 1), inscreva o comando line configuration **1. giratório** que colocam estes comandos sob as causas IO da configuração de linha atribuir ouvintes IP para conexões recebidas nos intervalos de porta que começam com os seguintes números base:

2000	Protocolo telnet
3000	Protocolo telnet com giratório
4000	Protocolo de TCP bruto
5000	Protocolo de TCP bruto com giratório
6000	Protocolo telnet, modo binário
7000	Protocolo telnet, modo binário com giratório
9000	Protocolo de XRemote
10000	Protocolo de XRemote com giratório

Para iniciar uma sessão de Telnet reversa a seu modem, execute as seguintes etapas:

1. De seu terminal, use o comando telnet ip-address 20yy onde o *IP address* é o endereço IP de Um ou Mais Servidores Cisco ICM NT de todo o active, interface conectada no dispositivo Cisco, e o JJ é o número de linha a que o modem é conectado. Por exemplo, o comando seguinte conectá-lo-ia ao porto auxiliar em um Cisco 2501 Router com o endereço IP 192.169.53.52: **telnet 192.169.53.52 2001**. Geralmente, um comando telnet deste tipo pode ser emitido em qualquer lugar sobre da rede, se pode **sibilar** o endereço IP de Um ou Mais Servidores Cisco ICM NT na pergunta. **Nota:** Na maioria de roteadores Cisco, a porta 01 é o porto auxiliar. Em um Cisco access server, o porto auxiliar é o último TTY +1. Como um exemplo, o porto auxiliar em uns 2511 é a porta 17 (16 portas de TTY + 1). Use sempre o **comando show line exec** encontrar o número de porto auxiliar - particularmente no 2600 e 3600 Series, que usam números de porta NON-contíguos para acomodar tamanhos de variação do módulo do async.
2. Se a conexão é recusada, poderia indicar que não há ou nenhum ouvinte no endereço especificado e porta, ou que alguém está conectado já a essa porta. Verifique o endereço e o número de porta da conexão. Também, certifique-se do comando modem inout ou modem DTR-active, assim como da **entrada de transporte todos**, aparecem sob a configuração de linha para as linhas que estão sendo alcançadas. Se usando a função rotary (rotatória), certifique-se que o comando rotary n igualmente aparece na configuração de linha onde n é o número do grupo giratório. Para verificar se alguém é conectado já, o telnet ao roteador e usar o comando show line N. procura um asterisco para indicar que a linha está no uso. Certifique-se que o CTS é alto e o DSR não é. Use o comando clear line n desligar a sessão atual no número de porta N. Se a conexão é recusada ainda, o modem pôde afirmar o

Carrier Detect (CD) todo o tempo. Desligue o modem da linha, estabeleça uma sessão de Telnet reversa, e conecte então o modem.

3. Após com sucesso ter feito a conexão Telnet, entre EM e seja certo as respostas do modem com APROVAÇÃO.

4. Se o modem não é responsivo, refira a tabela a seguir.

As causas possíveis abaixo dos esboços da tabela 16-1 de sintomas do problema de conectividade do modem-à roteador e descrevem soluções 2 aqueles problemas.

Tabela 16-1: Nenhuma Conectividade entre o modem e o roteador

Possíveis causas	Ações sugeridas
<p>O controle do modem não é permitido no servidor de acesso ou no roteador</p>	<ol style="list-style-type: none"> 1. Use o comando show line exec no servidor de acesso ou no roteador. A saída para o porto auxiliar deve mostrar InOut ou RlisCD na coluna de modem. Isto indica que o controle do modem está permitido na linha do servidor de acesso ou do roteador. Para uma explicação da linha saída da mostra, refira a “utilização de comandos Debug” no capítulo 15. 2. Configurar a linha para o controle do modem usando o comando modem inout line configuration. O controle do modem é permitido agora no servidor de acesso. <p>Exemplo: O exemplo seguinte ilustra como configurar uma linha para ambas as chamadas recebidas e enviadas: <code>line 5</code> <code>modem inout</code></p> <p>Nota: É certo que usarão o comando modem inout, e não o comando modem dialin quando a Conectividade do modem estiver na pergunta. O último comando permite que a linha aceite chamadas recebidas somente. As chamadas feitas serão recusadas e será impossível estabelecer uma sessão de Telnet com o modem a fim configurar-lo. Se você quer usar o comando modem dialin, faça assim somente depois que você está certo que o modem está funcionando corretamente.</p>
<p>O modem podia ser desconfigurado ou tido uma sessão</p>	<p>Incorpore AT&FE1Q0 para retorná-lo aos padrões de fábrica e certificar-se do modem é ajustada ecoar caracteres e retornada a saída. O modem pode ter uma sessão suspensa. Use o “^U” para cancelar a linha e o “^Q” para abrir o controle de fluxo (XON). Verifique configurações de paridade.</p>

suspensa.	
Cabeamento incorreto	<ol style="list-style-type: none"> 1. Verifique a expedição de cabogramas entre o modem e o servidor de acesso ou o roteador. Confirme que o modem está conectado ao porto auxiliar no servidor de acesso ou no roteador com um cabo RJ-45 rolado e um adaptador MMOD DB-25. Esta configuração de cabeamento é recomendada e apoiada por Cisco para as portas RJ-45. (Estes conectores são etiquetados tipicamente "Modem.") 2. Use o comando show line exec verificar que a expedição de cabogramas está correta. Veja a explicação da saída do comando show line na seção autorizada "usando comandos Debug" no capítulo 15.
Problema de hardware	<ol style="list-style-type: none"> 1. Verifique que você está usando o cabeamento correto e que todas as conexões são boas. 2. Verifique todo o hardware para ver se há dano, incluindo a expedição de cabogramas (fios quebrados), os adaptadores (pinos fracos), as portas de servidor de acesso, e o modem. 3. Veja o capítulo 3, "pesquisando defeitos o hardware e os problemas de inicialização," para obter mais informações sobre do Troubleshooting de hardware.

Usando grupos giratórios

Para alguns aplicativos, o Modems em um roteador dado precisa de ser compartilhado por um grupo de usuários. O utilitário do dialout Cisco é um exemplo deste tipo de aplicativo. Basicamente, os usuários conectam a uma porta que os conecta a um modem disponível. Para adicionar uma linha assíncrono a um grupo giratório, incorpore simplesmente n giratório onde n é o número do grupo giratório na configuração para a linha assíncrono. Refira 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 conectassem ao grupo giratório entrando no **telnet 192.169.53.52 3001** para o telnet normal. As alternativas incluem as portas 5001 para o TCP cru, 7001 para o telnet binário (que usos do utilitário do dialout Cisco), e 10001 para conexões Xremote.

Nota: Para verificar a configuração do utilitário do dialout Cisco, fazer duplo clique no ícone do utilitário de discagem no direita inferior da tela e pressione o botão de More>. Em seguida, pressione o botão de Ports> configurar. Certifique-se que a porta está na escala 7000, se usando grupos giratórios, e a escala 6000, se o utilitário de discagem está visando um modem individual. Você deve igualmente permitir o modem que entra o PC. Isto é feito selecionando a seguinte sequência: **Modems-> de Start->Control Panel->** (escolha seu modem do dialout Cisco) ->Properties->Connection->Advanced... ->Record um **arquivo de registro**.

Interpretando a linha saída da mostra

A saída do **comando show line line-number exec** é útil ao pesquisar defeitos um servidor de modem a acesso ou conexão de roteador. Está abaixo 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 dsxl(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 1 at pad telnet rlogin udptn v120 lapb-ta. No
output characters are padded No special data dispatching characters as5200-1#
```

Quando os problemas de conectividade ocorrem, a saída importante aparece no estado do modem e nos campos de estado de hardware do modem.

Nota: O campo de estado de hardware do modem não aparece na **linha da mostra** output para cada plataforma. Em certos casos, as indicações para estados de sinal serão mostradas no campo do estado do modem pelo contrário.

Mostras cordas típicas do estado do modem da tabela 16-2 e do estado de hardware do modem da saída do **comando show line**. Igualmente explica o significado de cada estado.

Tabela 16-2: Modem e estados de hardware do modem na linha saída da mostra

Estado do modem	Estado de hardware do modem	Significado
Ociosos	CTS DT R noD SR RTS	Estes são os estados do modem apropriados para conexões entre um servidor de acesso ou um roteador e um modem (quando não há nenhuma chamada recebida). A saída de qualquer outro tipo indica geralmente um problema.
Pronto	-	Se o estado do modem está pronto, em vez da quietude, considere o seguinte:

		<ol style="list-style-type: none"> 1. O controle do modem não é configurado no servidor de acesso ou no roteador. Configurar o servidor de acesso ou o roteador com o comando modem inout line configuration. 2. Uma sessão existe na linha. Use o comando show users exec e use o comando clear line privileged exec parar a sessão se desejado. 3. O DSR é alto. Há duas razões possíveis para esta: Problemas de cabeamento. Se seu conector usa DB-25 o pino 6 e não tem nenhum pino 8, você deve mover o pino de 6 para 8 ou obter o conector apropriado. O modem configurado para o DCD é sempre alto. O modem deve ser reconfigurado para ter o DCD alto somente um CD(1). Isto é feito geralmente com o comando modem &C1, mas verifica sua documentação de modem para ver se há a sintaxe exata para seu modem. Se seu software não apoia o controle do modem, você deve configurar a linha de servidor de acesso a que o modem é conectado com o comando no exec line configuration. Cancele a linha com o comando clear line privileged exec, inicie uma sessão de Telnet reversa com o modem, e reconfigure o modem de modo que o DCD seja alto somente no CD. Termine a sessão de Telnet incorporando a disconexão e reconfigure a linha de servidor de acesso com o comando exec line configuration.
Pro nto	noC TS DT R noD SR RTS (2)	<p>A corda do noCTS aparece no campo de estado de hardware do modem para uma das seguintes quatro razões:</p> <ol style="list-style-type: none"> 1. O modem é desligado. 2. O modem não é conectado corretamente ao servidor de acesso. Verifique as conexões de expedição de cabogramas do modem ao servidor de acesso. 3. Cabeamento incorreto (mdce enrolado, ou MDTE reto, mas sem os pinos movidos). A configuração de cabeamento recomendada é dada mais cedo nesta

		<p>tabela.</p> <p>4. O modem não é configurado para o controle de fluxo de hardware. Use o comando no flowcontrol hardware line configuration desabilitar o controle de fluxo de hardware no servidor de acesso. Permita então o controle de fluxo de hardware no modem através de uma sessão de Telnet reversa. (Consulte sua documentação de modem e veja a seção “estabelecer uma sessão de Telnet reversa a um modem” mais cedo neste capítulo.) Re-permita o controle de fluxo de hardware no servidor de acesso com o comando flowcontrol hardware line configuration.</p>
Pro nto	CTS DS R DT R RTS (2)	<p>A corda DSR (em vez da corda noDSR) aparece no campo de estado de hardware do modem para uma das seguintes razões:</p> <ol style="list-style-type: none"> 1. Cabeamento incorreto (mdce enrolado, ou MDTE reto, mas sem os pinos movidos). A configuração de cabeamento recomendada é dada mais cedo nesta tabela. 2. O modem é configurado para o DCD sempre altamente. Reconfigure o modem de modo que o DCD seja somente alto no CD. Isto é feito geralmente com o comando modem &C1, mas verifique sua documentação de modem para ver se há a sintaxe exata para seu modem. Configure a linha de servidor de acesso a que o modem é conectado com o comando no exec line configuration. Cancele a linha com o comando clear line privileged exec, inicie uma sessão de Telnet reversa com o modem, e reconfigure o modem de modo que o DCD seja alto somente no CD. Termine a sessão de Telnet incorporando a disconexão. Reconfigure a linha de servidor de acesso com o comando exec line configuration.
Pro nto	CTS * DS R* DT	<p>Se esta corda aparece no campo de estado de hardware do modem, o controle do modem não está permitido provavelmente no servidor de acesso. Use o comando modem inout line configuration permitir o controle do modem na</p>

	R RTS (2)	linha. A informação adicional em configurar o controle do modem em um servidor de acesso ou em uma linha de roteador é fornecida mais cedo nesta tabela.
--	-----------------	--

(1) CD = revelação do sinal de comunicação

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

Reunindo informações de desempenho do modem

Esta seção explica métodos para recolher dados de desempenho nos modems digitais MICA encontrados na família do Cisco AS5x00 dos servidores de acesso. Os dados de desempenho podem ser usados para a análise de tendências e são úteis nos problemas de desempenho do Troubleshooting que puderam ser encontrados. Quando olhar os números apresentou abaixo, tenha que a perfeição não é possível no mundo real. A taxa de sucesso possível da chamada de modem (CSR) é uma função da qualidade dos circuitos, do userbase do modem do cliente, e do grupo de modulações que estão sendo usadas. Um porcentagem típica de CSR para os atendimentos V.34 é 95%. Os atendimentos V.90 podem ser esperados conectar com sucesso 92% do tempo. As gotas prematuras são prováveis acontecer 10% do tempo.

Use os comandos seguintes ganhar uma ideia total do comportamento do modem no servidor de acesso:

- **mostre o modem**
- **mostre o resumo de modem**
- **mostre modem connect-speeds**
- **mostre modem call-stats**

A informação seguinte é útil ao pesquisar defeitos uma conexão de modem individual ou ao recolher dados para a análise de tendências:

- debug modem csm
- modem call-record terse
- mostram modem op) (MICA/AT@E1 (Microcom) quando conectado
- mostre o log de modem para a sessão do interesse após a desconexão
- ANI (o número do chamador)
- Time Of Day
- Hardware/revisão de firmware do modem do cliente
- Informação interessante do cliente (após disconnect)-ATI6, ATI11, AT&V, AT&V1, e assim por diante
- Um registro audio (arquivo do .WAV) da tentativa do trainup do modem do cliente

Nas seguintes seções, os comandos serão explicados mais e algumas tendências comuns serão discutidas.

Mostre o modem/resumo de modem da mostra

O comando **show modem** dá uma vista dos modems individuais. Destes números a saúde dos 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 para todo o 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: mostre campos do modem

Campos	Descrições
Chamadas recebidas e enviadas	Atendimentos que discam e fora do modem. <ul style="list-style-type: none"> • Uso - Porcentagem do uptime do sistema total que todo o Modems está no uso. • Succ - Chamadas total conectadas com sucesso. • Falha - Chamadas total que não conectaram com sucesso. • Proveito - Modems total disponível para o uso no sistema.
Busied para fora	O número total de épocas o Modems foi tomado fora de serviço com o comando modem busy ou o comando modem shutdown .
Seletor falhado	Número total de tentativas que o Modems não pendurou acima ou havia sem tom de discagem.
No Ans	O número total de toque de chamada das épocas foi detectado, mas os atendimentos não foram respondidos por um modem.
Pct de Succ.	Porcentagem da conexão bem sucedida do Modems disponível total.

[Mostre modem call-stats a saída](#)

```

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

```

Tabela 16-4: mostre modem call-stats campos

rmt Link	Esta mostra que a correção de erros era de fato, e o atendimento foram pendurados acima pelo sistema de cliente anexado ao modem remoto.
hos tDr	Isto mostra que o atendimento esteve pendurado acima pelo sistema host IO. Alguns motivos

op	comuns incluem: idle timeout, um circuito claro da companhia telefônica, ou um termreq PPP LCP do cliente. A melhor maneira de determinar a razão para o cair está acima usando o registro de chamada do modem sóbrio ou contabilidade AAA.
----	---

Os outros motivos de desconexão devem adicionar acima a menos de 10% do total.

[Mostre a saída dos modem connect-speeds](#)

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

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

Espreze ver uma distribuição das velocidades V.34. Deve haver um pico em 26.4, se a sinalização associada a canal (CAS) do uso do T1s. Para o T1s ISDN (PRI), o pico deve estar em 31.2.

Também, procure algum o K56Flex, velocidades v.90. Se não há nenhuma conexão V.90 pode haver um problema da topologia de rede.

[Compreendendo o comando sóbrio do registro de chamada do modem \(11.3AA/12.0T\)](#)

Um pouco do que um comando exec, este é um comando configuration colocado no nível de sistema do servidor de acesso na pergunta. Quando desconexões de um usuário, uma mensagem similar aos seguintes indicadores:

```
*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 **modem operational-status** do exec command show mostra os parâmetros atuais (ou a maioria de recente) que referem-se a conexão de modem.

A entrada de documentação para este comando é encontrada no *Dial Solutions Command Reference do Cisco IOS Release 12.0*. o **modem operational-status** da mostra é somente para modems MICA. O comando equivalente para modems Microcom é **modem em-MODE/AT@E1**. Use o **comando modem at-mode <slot>/<port>** conectar ao modem, a seguir emita o comando de **AT@E1**. A documentação completa para o **comando modem at-mode** pode ser encontrada no *manual de configuração do software do Cisco AS5300*, e a documentação para o comando de **AT@E1** está no *no comando set e no sumário de registro para a referência de comandos dos módulos do modem Microcom*.

Use as seguintes etapas para determinar que Modems um usuário está vindo dentro:

1. Emita o comando show user e procure o TTY a que são conectados.
2. Use o comando show line e procure os números da /porta do entalhe do modem.

Recolhendo dados de desempenho do lado do cliente

Para a análise de tendências, é muito importante recolher dados de desempenho do lado do cliente. Tente sempre obter a informação seguinte:

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

As outras informações disponíveis na extremidade de cliente inclui modemlog.txt e ppplog.txt do PC. Você deve especificamente configurar seu PC para gerar estes arquivos.

Análise os dados de desempenho

Uma vez que você recolheu e compreendeu os dados de desempenho para seu sistema de modem, você precisa de olhar todos os testes padrões e componentes restantes que puderem precisar a melhoria.

Problemas com Modems do servidor particular

Use o **modem da mostra** ou **mostre-o modem call-stats** para identificar anormalmente todo o Modems com taxas altas da falha de trainup ou das taxas ruins da desconexão (MICA). Se os pares adjacentes de modems estão tendo problemas, o problema é provável pendurado/absolutamente DSP. Use o **modem de flash de cópia ao HMM** afetado a fim recuperar. Certifique-se que o Modems está executando a versão a mais atrasada do portware. Para verificar que todo o Modems está configurado corretamente, use o configuration command modem **autoconfigure o tipo mica/microcom_server** na configuração de linha. Para certificar-se o Modems autoconfigured sempre que um atendimento é pendurado acima, usa o comando **exec debuga o confmodem**. A fim fixar o Modems que é desconfigurado ruim, você pode precisar de estabelecer uma sessão de Telnet reversa.

Problemas com DS0 particulares

Os problemas DS0 são raros, mas possíveis. Para encontrar DS0 funcionando mal, use o comando show controller t1 call-counters e procure todos os DS0 com anormalmente as Chamadas Total altas e o TotalDuration anormalmente baixo. Para visar suspeito DS0, você pode precisar ocupado para fora outros DS0 com o **serviço dsl** do configuration command ISDN, o **busyout ds0** sob a interface serial para o T1. A saída do **show controller t1 call-counters** olha como esta:

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

Obviamente, o intervalo de tempo 3 é o canal suspeito neste caso.

Tendências adicionais da terra comum

Estão abaixo algumas das tendências mais comuns vistas pelo tac Cisco.

1. Trajetos do circuito ruins Você pôde obter trajetos do circuito ruins através da rede telefônica pública comutada (PSTN) se você tem os seguintes problemas: as chamadas interurbanas têm problemas, mas o local não faz (ou vice versa) os atendimentos por vezes do dia têm problemas os atendimentos das trocas remotas específicas têm problemas
2. Problemas com chamadas interurbanas Se seu serviço interurbano não está funcionando corretamente ou de todo (mas o serviço local é muito bem): Seja certo que a linha digital conecta em um switch digital, não um banco de memória de canal. Instrua as companhias telefônica examinar os trajetos do circuito usados para a longa distância.
3. Problemas com atendimentos das áreas de chamada específicas. Se os atendimentos das regiões geográficas/trocas específicas tendem a ter problemas, você deve obter a topologia de rede da companhia telefônica. Se as conversões de analógico para digital múltiplas são exigidas, o modem V.90/K56flex conecta não será possível e o V.34 pode um tanto ser degradado. As conversões de analógico para digital são exigidas nas áreas que são servidas por switch digitais NON-integrados ou pelo Switches análogo.

Operações de ISDN

O ISDN refere um grupo de serviços digitais que estão disponíveis aos utilizadores finais. Envolvimentos de ISDN a numeração da rede telefônica de modo que a Voz, os dados, o texto, os gráficos, a música, o vídeo, e o outro material de origem possam ser fornecidos aos utilizadores finais de um único, terminal do utilizador final sobre a fiação do telefone existente. Os proponentes do ISDN imaginam uma rede mundial bem como a rede telefônica atual, mas com transmissão digital e uma variedade de serviços novos.

O ISDN é um esforço para standardizar serviços de assinante, usuário/interfaces de rede, e rede e capacidades inter-redess. Standardizar serviços de assinante tenta assegurar um nível da compatibilidade internacional. Standardizar o usuário/interface de rede estimula o desenvolvimento e o mercado destas relações por fabricantes da terceira. Standardizando ajudas da rede e das capacidades inter-redess consiga o objetivo da conectividade mundial assegurando-se de que as redes de ISDN se comuniquem facilmente um com o outro.

Os aplicativos ISDN incluem aplicativos de imagem de alta velocidade (tais como o fac-símile do grupo IV), linhas de telefone adicionais nas HOME servir a indústria do telecommuting, transferência de arquivo de alta velocidade, e a vídeo conferência. Voz, naturalmente, isl igualmente um aplicativo popular para o ISDN.

O mercado de acesso de home está sendo dividido acima entre Tecnologias diferentes. Nas áreas onde novo menos tecnologias caras tais como o DSL e o cabo tornam-se disponíveis o mercado de home estão movendo-se longe do ISDN. Os negócios, contudo, continuam a usar o ISDN sob a forma de PRI T1/E1 para levar grandes quantidades de dados ou para fornecer o acesso da discagem v.90.

Componentes ISDN

Os componentes ISDN incluem terminais, adaptadores terminal (TA), dispositivos de terminação de rede, equipamento de terminação de linha, e equipamento da terminação de intercâmbio. Os terminais ISDN vêm em dois tipos. Os terminais ISDN especializados são referidos como o tipo-1 do equipamento de terminal (TE1). Os terminais não ISDN, tais como o DTE que pre-datar os

padrões de ISDN, são referidos como o tipo-2 do equipamento de terminal (TE2). Os TE1 conectam à rede de ISDN com um de quatro fios, link digital do twisted pair. Os TE2 conectam à rede de ISDN através de um adaptador terminal. O ISDN TA pode ser um dispositivo autônomo ou uma placa dentro do TE2. Se o TE2 é executado como um dispositivo autônomo, 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 ponto de conexão seguinte na rede de ISDN é o tipo-1 da terminação de rede (NT1) ou o tipo-2 da terminação de rede (NT2) dispositivo. Estes são os dispositivos de terminação de rede que conectam o subscritor de quatro fios que prende ao loop local convencional do dois-fio. Em America do Norte, o NT1 é um dispositivo do Customer Premises Equipment (CPE). Na maioria outras de partes do mundo, o NT1 é parte da rede fornecida pelo portador. O NT2 é um dispositivo mais complicado, encontrado tipicamente nos centrais telefônica privada digitais (PBX), que execute serviços da concentração da camada 2 e 3 funções do protocolo e. Um dispositivo NT1/2 igualmente existe; é um dispositivo único que combine as funções de um NT1 e de um NT2.

Um número de pontos de referência são especificados no ISDN. Estes pontos de referência definem interfaces lógica entre disposições funcionais tais como TA e NT1. Os pontos de referência ISDN incluem o seguinte:

- Ponto de referência de R-The entre o equipamento não-ISDN e um TA
- Ponto de referência de S-The entre terminais de usuário e o NT2
- Ponto de referência de T-The entre os dispositivos NT1 e NT2
- Ponto de referência de U-The entre os dispositivos NT1 e o equipamento de terminação de linha na rede do portador. O ponto de referência U é relevante somente em America do Norte, onde a função NT1 não é fornecida pela rede do portador

O seguinte é um exemplo de configuração de ISDN. Esta amostra mostra três dispositivos anexados a um switch ISDN no escritório central. Dois destes dispositivos são ISDN-compatíveis, assim que podem ser anexados através de um ponto de referência S aos dispositivos NT2. Os terceiros diplomatas telefone do dispositivo (um padrão, não ISDN) através do ponto de referência R a um TA. Qualquens um dispositivos poderiam igualmente anexar a um dispositivo NT1/2, que substituísse o NT1 e o NT2. E, embora não sejam mostradas, as estações de usuário similares são anexadas ao switch ISDN do extrema direita.

[Um exemplo de configuração de 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 de ISDN](#)

O serviço do Basic Rate Interface (BRI) ISDN oferece dois canais B e um canal D (2B+D). O serviço do canal B BRI opera-se em 64 kbps e é significado levar dados do usuário; O serviço do canal D BRI opera-se em 16 kbps e é significado levar o controle e a informação de sinalização, embora possa apoiar a transmissão dos dados do usuário em certas circunstâncias. O protocolo de sinalização de canal D compreende as camadas 1 a 3 do OSI Reference Model. O BRI

igualmente prevê o controle de estruturação e o outro aéreo, trazendo sua taxa total de bits a 192 kbps. A especificação de camada física BRI é Setor de Padronização de Telecomunicação de União de Telecomunicação Internacional (ITU-T; anteriormente o [CCITT]) do comitê consultivo para telégrafo e telefone internacional I.430.

O serviço da interface de taxa primária de ISDN (PRI) oferece 23 canais B e um canal D em America do Norte e em Japão, rendendo uma taxa total de bits do 1.544 Mbps (o canal D PRI é executado em 64 kbps). O ISDN PRI em Europa, em Austrália, e em outras partes do mundo fornece 30 B mais um canal D 64-kbps e uma taxa da interface total de 2.048 Mbps. A especificação de camada física PRI é o ITU-T I.431.

Layer 1

Os formatos de frame da camada física ISDN (Layer 1) diferem segundo se o quadro é de partida (do terminal à rede) ou de entrada (da rede ao terminal). Ambas as interfaces de camada física são mostradas em figura 16-1.

Figura 16-1: Formatos do frame de camada física ISDN

Os quadros são 48 bit por muito tempo, de que 36 bit representam dados. Os bit de um frame de camada física ISDN são usados como segue:

- F - Permite sincronização.
- L - Ajusta o valor do bit médio.
- E - Usado para a resolução de contenção quando diversos terminais em um barramento passivo afirmarem para um canal.
- A - Ativa dispositivos.
- S - Unassigned.
- B1, B2, e D - Para dados do usuário.

Os dispositivos de usuário do ISDN múltiplo podem fisicamente ser anexados a um circuito. Nesta configuração, as colisões podem resultar se dois terminais transmitem simultaneamente. Consequentemente, o ISDN fornece características para determinar a disputa do link. Quando NT recebe um D mordido do TE, ecoa para trás o bit na posição seguinte do E-bit. O TE espera o bit seguinte E ser o mesmo que seu último bit transmitido D.

Os terminais não podem transmitir no canal D a menos que detectarem primeiramente um número específico de uns (indicando o “sem sinal”) que correspondem a uma prioridade PRE-estabelecida. Se o TE detecta um bit no canal do eco (e) que é diferente de seus bit D, deve parar de transmitir imediatamente. Esta técnica simples assegura-se de que somente um terminal possa transmitir seu mensagem D ao mesmo tempo. Após a transmissão bem sucedida do mensagem D, o terminal tem sua prioridade reduzida sendo exigido para detectar o mais contínuos antes de transmitir. Os terminais não podem levantar sua prioridade até que todos os outros dispositivos na mesma linha tenham uma oportunidade de enviar um mensagem D. As conexões de telefone têm a prioridade mais alta do que todos os outros serviços, e a informação de sinalização tem uma prioridade mais alta do que a informações sem sinalização.

Camada 2

A camada 2 do protocolo de sinalização ISDN é procedimento de acesso de enlace no canal D, igualmente conhecido como o LAPD. O LAPD é similar ao High-Level Data Link Control (HDLC) e ao procedimento de acesso de enlace, equilibrado (LAPB). Enquanto a expansão da abreviação

LAPD indica, está usada através do canal D para assegurar-se de que fluxos de controle e de informação de sinalização e recebida corretamente. O formato de frame de lapd (veja figura 16-2) é muito similar àquele do HDLC e, como o HDLC, do LAPD usa supervisorio, a informação, e os frames não numerados. O protocolo LAPD é especificado formalmente no ITU-T Q.920 e no ITU-T Q.921.

Figura 16-2: Formato de frame de lapd

A bandeira e os campos de controle LAPD são idênticos àquelas do HDLC. O campo de endereço LAPD pode ser 1 ou 2 bytes por muito tempo. Se o bit do endereço prolongado do primeiro byte é ajustado, o endereço é 1 byte; se não é ajustado, o endereço é 2 bytes. O primeiro byte do campo de endereço contém o identificador de ponto de acesso de servidor (SAPI), que identifica o portal em que os serviços LAPD são proporcionados para mergulhar 3. O bit C/R indica se o quadro contém um comando ou uma resposta. O campo do identificador de ponto final terminal (TEI) identifica um único terminal ou vários terminais. Um TEI de todos os indica uma transmissão.

Camada 3

Duas especificações da camada 3 são usadas para a sinalização ISDN: ITU-T (anteriormente CCITT) I.450 (igualmente conhecido como o ITU-T Q.930) e ITU-T I.451 (igualmente conhecido como o ITU-T Q.931). Junto, conexões usuários para usuário, circuito-comutadas, e comutáveis por blocos do apoio destes protocolos. Uma variedade de estabelecimento de chamada, terminação de chamada, informação, e mensagens variada são especificados, incluindo a INSTALAÇÃO, CONECTAM, LIBERAM-SE, INFORMAÇÃO SOBRE O USUÁRIO, CANCELAMENTO, ESTADO, e DISCONEXÃO.

Estas mensagens são funcionalmente similares àquelas fornecidas pelo protocolo x.25 (veja o capítulo 19, “pesquisando defeitos as conexões X.25,” para mais informação). Figura 16-3, do ITU-T I.451, mostra as fases típicas de uma chamada de circuito comutado ISDN.

Figura 16-3 fases da chamada de circuito comutado ISDN

Saída da interpretando exibição de status de ISDN

Para encontrar o que a condição atual da conexão ISDN está entre o roteador e o switch de companhia telefônica, use o comando show isdn status. Os dois tipos das relações que são apoiadas por este comando são o BRI e o 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
```

Status de ISDN da mostra da tabela 16-5:- para o BRI

Campo	Significado
Status da camada	Isto indica que a interface BRI não está considerando um sinal na linha. Há cinco razões possíveis para esta circunstância.

<p>1: DESATI VADO</p>	<ul style="list-style-type: none"> • A interface BRI é parada programada. Verifique a configuração para ver se há o comando shutdown sob a interface BRI, ou procure administrativamente para baixo uma indicação do comando show interface. Use o utilitário de configuração e não incorpore nenhuma parada programada sob a interface BRI. Inscreva o comando clear interface bri no prompt de exec certificar-se que a interface BRI está reiniciada. • Um problema existe com a expedição de cabogramas. Você precisará de substituir o cabo. Certifique-se que você usa a reto-atraves do cabo RJ-45. Para verificar o cabo, guarde as extremidades de cabo RJ-45 de lado a lado. Se os pinos estão na mesma ordem, o cabo está reto-atraves de. Se o ordem do pino é invertido, o cabo está rolado. Substitua o cabo. • A porta do ISDN BRI de um roteador pôde exigir um dispositivo NT1. No ISDN, o NT1 é um dispositivo que forneça a relação entre o Customer Premises Equipment e o equipamento de switching do escritório central. Se o roteador não tem um NT1 interno, obtenha e conecte um NT1 à porta BRI. Certifique-se de que o BRI ou o adaptador terminal estão anexados à porta S/T do NT1. Refira a documentação do fabricante para verificar a operação correta do NT1 externo. • A linha não pôde funcionar. Contacte o portador para confirmar a operação da conexão e para verificar o tipo de switch ajustes. • Certifique-se que o roteador está funcionando corretamente. Se há defeituoso ou hardware de MAU funcionamento, substitua como necessário.
<p>Status da camada 2: Estado = TEI_AS SIGNE</p>	<p>Verifique a configuração de tipo de switch e os SPID. A configuração de switch ISDN interface-especifico cancelará a configuração de switch global. O status de SPID indicará se o interruptor aceitou os SPID (válido ou inválido). Contacte seu provedor de serviços para verificar o ajuste configurado no roteador. Para mudar os ajustes SPID, use o comando</p>

D	<p>interface configuration do spidn isdn. Onde <i>n</i> é 1 ou 2, segundo o canal na pergunta. Não use nenhum formulário deste comando remover o spid especificado. <code>isdn spidn spid-number [ldn]</code> no <code>isdn spidn spid-number [ldn]</code></p> <p>Descrição da sintaxe: <code>spid-number</code> O número que identifica o serviço a que você subscreveu. Este valor é atribuído pelo fornecedor de serviço de ISDN e é geralmente um número de telefone 10-dígito com dígitos adicionais. <code>ldn</code> O número de diretório local (LDN) (opcional), que é um número do 7-dígito atribuído pelo provedor de serviços. O interruptor no mensagem de configuração recebida entrega esta informação. Se você não inclui o acesso do diretório local ao interruptor está permitido, mas o outro canal B não pode poder receber chamadas recebidas. Para ver as negociações da camada 2 entre o interruptor e o roteador, use o comando <code>privileged exec debugam isdn q921</code>. O <code>q921</code> debuga é documentado na <i>referência do comando Debug</i>. Debugs confia pesadamente em recursos do CPU, assim que use o cuidado ao empregá-los.</p>
---	---

```
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 trabalha nem não mostra o PRI, tente usar o comando **show isdn service**. Certifique-se que o comando **pri-group** aparece na configuração sob o controlador T1/E1 na configuração. Se o comando não está atual, configurar o controlador com o comando **pri-group**.

O seguinte é um exemplo de uma 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: mostre o status de ISDN para o PRI

Campo	Significado
Status da camada 1: DESATIVA DO	<p>Isto indica que a relação PRI não está considerando o T1/E1 moldar na linha. Considere as seguintes causas possíveis para esta circunstância:</p> <ul style="list-style-type: none"> A relação PRI é parada programada. Verifique a configuração para ver se há o comando <code>shutdown</code> sob a relação <code>serial0:23</code> ou procure administrativamente para baixo uma

	<p>indicação do comando show interface. Use o utilitário de configuração e não incorpore nenhuma parada programada sob a relação na pergunta. Inscreva o comando clear controller T1/E1 n no prompt de exec certificar-se que a relação PRI está reiniciada.</p> <ul style="list-style-type: none"> • Um problema existe com a expedição de cabogramas. Você precisará de substituir o cabo. Certifique-se que você usa a reto-atraves do cabo RJ-45. Para verificar o cabo, guarde as extremidades de cabo RJ-45 de lado a lado. Se os pinos estão na mesma ordem, o cabo está reto-atraves de. Se o ordem do pino é invertido, o cabo está rolado. Substitua o cabo. • A linha não pôde funcionar. Contacte o portador para confirmar a operação da conexão, e para verificar o tipo de switch ajustes. • Certifique-se que o roteador está funcionando corretamente. Se há defeituoso ou hardware de MAU funcionamento, substitua como necessário.
<p>Status da camada 2: Estado = TEI_ASSIG NED</p>	<p>Verifique a configuração de tipo de switch. A configuração de switch ISDN interface-específico cancelará a configuração de switch global. Verifique que o T1/E1 está configurado para combinar o interruptor do fornecedor (os problemas T1/E1 são discutidos no capítulo 15). Para ver as negociações da camada 2 entre o interruptor e o roteador, use o comando privileged exec debugam isdn q921. O q921 debuga é documentado na <i>referência do comando Debug</i>. Debugs confia pesadamente em recursos do CPU, assim que use o cuidado ao empregá-los.</p>
<p>O número de atendimentos/blocos de controle de chamadas no uso/total atribuiu</p>	<p>Estes números indicam quantos atendimentos são em andamento, e o número de recursos que são atribuídos para apoiar aqueles atendimentos. Se o número de CCB atribuídos é mais alto do que o número de CCB que estão sendo usados, considere que pôde haver um problema em liberar CCB. Certifique-se que há CCB disponíveis para chamadas</p>

blocos de controle da chamada ISDN	recebidas.
------------------------------------	------------

[Discar o roteamento por encomenda: Operações de interface do discador](#)

O roteamento por encomenda do seletor (DDR) é um método de fornecimento de conectividade de WAN em uma base econômica, conforme necessário, como um link principal ou como o backup para um link do serial sem discagem.

Uma **interface do discador** é definida como toda a interface do roteador capaz de colocar ou de receber um atendimento. Este termo genérico deve ser distinto da **interface do discador do termo** (com um D) principal, que refiram uma interface lógica configurada para controlar umas ou várias interfaces física de um roteador e que seja visto em uma configuração de roteador como o discador X. da relação. Deste ponto para a frente, salvo indicação em contrário, nós estaremos usando o discador do termo em seu sentido genérico.

A configuração da interface do discador vem em dois sabores: discador com base no mapa (referido às vezes como o DDR anterior), e Perfis de discagem. Que método você usa depende das circunstâncias sob que você precisa a Conectividade do seletor. O discador DDR com base no mapa foi introduzido primeiramente na Versão do IOS 9.0, Perfis de discagem na Versão do IOS 11.2.

[Provocando um seletor](#)

Em seu coração, o DDR é *pacotes interessantes da* extensão de roteamento em que é distribuído apenas a uma interface do discador, provocando uma tentativa de discagem. As seguintes seções explicam os conceitos envolvidos em definir o tráfego interessante e explicam o roteamento usado para conexões DDR.

[Pacotes interessantes](#)

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

- o pacote deve encontrar os critérios da “licença” definidos por uma lista de acesso
- a lista de acesso deve ser provida pela discador-lista ou o pacote deve ser de um protocolo que seja permitido universalmente pela discador-lista
- a lista de discadores deve ser associada com uma interface do discador por meio de um discador-grupo

Os pacotes nunca são considerados automaticamente ser interessantes (à revelia). As definições interessantes de pacote devem explicitamente ser declaradas em um roteador ou em uma configuração do servidor de acesso.

[Grupo de discadores](#)

Na configuração de cada interface do discador no roteador ou no servidor de acesso, deve haver um **comando dialer-group**. Se o **comando dialer-group** não está atual, não há nenhum enlace lógico entre as definições interessantes de pacote e a relação. A sintaxe de comando:

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

O número do grupo é o número do grupo de acesso de discadores a que a relação específica pertence. Este grupo de acesso é definido com o **comando dialer-list**. Os valores aceitáveis são diferente de zero, inteiros positivos entre 1 e 10.

Uma relação pode ser associada com um único grupo de acesso de discadores somente; a atribuição múltipla do discador-grupo não é permitida. Uma segunda atribuição do grupo de acesso de discadores cancelará a primeira. Um grupo de acesso de discadores é definido com o **comando dialer-group**. O **comando dialer-list** associa uma lista de acessos com um grupo de acesso de discadores.

Pacotes que combinam o disparador do grupo do discador especificado um pedido de conexão.

O endereço de destino do pacote é avaliado contra a lista de acessos especificada no comando `associated dialer-list`. Se passa, ou um atendimento está iniciado (se nenhuma conexão tem sido estabelecida já) ou o temporizador de ociosidade é restaurado (se um atendimento é conectado atualmente).

[Lista de discadores](#)

O **comando dialer-list global configuration** é usado definir uma lista do discador DDR para controlar discar pelo protocolo, ou por uma combinação do protocolo e da lista de acessos. Os pacotes interessantes são aqueles que combinam a licença do nível de protocolo ou que são permitidas pela lista no **comando dialer-list: dialer-list dialer-group protocol protocol-name {permit | negue | list access-list-number | acesso-grupo}**

o discador-grupo é o número de um grupo de acesso de discadores identificado em todo o comando `dialer-group interface configuration`.

o protocolo-nome é uma das seguintes palavras-chave de protocolo: APPLETALK, ponte, clns, clns_es, clns_is, DECNet, decnet_router-L1, decnet_router-L2, decnet_node, IP, IPX, videiras, ou XNS.

a licença permite o acesso a um protocolo completo.

negue nega o acesso a um protocolo completo.

a lista especifica que uma lista de acessos estará usada definindo uma granularidade mais fina do que um protocolo completo.

access-list-number - Accesss list number especificados em algumas DECNet, Banyan VINES, IP, Novell IPX, ou XNS padrão ou listas de acesso estendida, incluindo Listas de acesso e dispositivos de Bridging do ponto de acesso ao serviço estendido de Novell IPX (SAP). Veja a tabela 16-7 para os tipos e os números apoiados da lista de acessos.

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

Tabela 16-7: Numeração da lista de acesso pelo protocolo

Tipo da lista de acessos	Escala do access list number (decimal)
Apple Talk	600-699
Banyan VINES (padrão)	1-100
Banyan VINES (estendido)	101-200
DECNet	300-399
IP (padrão)	1-99
IP (estendido)	100-199
Novell IPX (padrão)	800-899
Novell IPX (estendido)	900-999
Bridging Transparente	200-299
XNS	500-599

[Lista de acessos](#)

Para cada protocolo de rede que deve ser enviada através da conexão de discagem, uma lista de acessos pode ser configurada. Para fins do controle de custo, é geralmente desejável configurar uma lista de acessos a fim impedir que determinado tráfego, tal como atualizações de roteamento, traga acima ou prossiga uma conexão. Note que quando nós criamos Listas de acesso com a finalidade de definição interessante e de tráfego desinteressante, nós não estão declarando que os pacotes desinteressante não podem cruzar o link de discagem. Nós apenas estamos indicando que não restaurarão o temporizador de ociosidade, nem trarão acima uma conexão no seus próprios. Enquanto a conexão de discagem está acima, os pacotes desinteressante estarão permitidos ainda fluir através do link.

Por exemplo, um roteador que executa o EIGRP como seu protocolo de roteamento pode ter uma lista de acessos configurada para declarar os pacotes EIGRP sem interesse e o todo tráfego IP restante interessante:

```
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 puderam cruzar o link de discagem. Recorde que para todo o protocolo, o comportamento padrão na ausência de uma indicação do **access-list permit** é negar todo o tráfego. Se não há nenhuma lista de acessos e nenhum **comando dialer-list** permitindo o protocolo, a seguir que o protocolo será sem interesse. Na prática real, se não há nenhuma lista de discadores para um protocolo, aqueles pacotes não fluirão através do link de todo.

[Exemplo - Unindo o todo](#)

Com todos os elementos no lugar, você pode examinar o processo completo por que o estado “interessante” de um pacote é determinado. Neste exemplo, o IP e o IPX são os protocolos que podem cruzar o link de discagem. O usuário quer impedir que as transmissões e as atualizações de roteamento iniciem um atendimento ou mantenham o link acima.

```
!
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 indicações do **access-list 121**, antes de cruzar o **interface async 1**, a fim ser considerado *interessante*. Neste caso, os pacotes EIGRP são negados, como são todos os outros pacotes de transmissão, quando todo tráfego IP restante for permitido. Recorde que isto não impede que os pacotes EIGRP transitem pelo link. Significa somente que estes pacotes não restaurarão o temporizador de ociosidade nem iniciarão uma tentativa de discagem.

Similarmente, o **access-list 903** declara o RASGO IPX, as seivas e os pedidos GNS ser sem interesse, quando todo tráfego IPX restante for interessante. Sem estas instruções de negação, a conexão de discagem provavelmente nunca viria para baixo e uma conta telefônica muito grande resultaria desde que os pacotes destes tipos fluem constantemente através de uma Rede IPX.

Com o **dialer-group 7** configurado na interface assíncrona, nós sabemos que a **discador-lista 7** está precisada de amarrar os filtros de tráfego interessante (isto é, Listas de acesso) à relação. Uma indicação da **discador-lista** é exigida (e *somente* uma pode ser configurado) para cada protocolo, certificando-se de que o número da lista de discadores é o mesmo que o número de grupo de discadores na relação.

Mais uma vez, é importante recordar que as *instruções de negação nas* Listas de acesso configuradas definindo o tráfego interessante não impedirão que os pacotes negados cruzem o link.

Usando o comando debug dialer, você pode ver a atividade que provoca uma tentativa de discagem:

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

Aqui nós vemos que o tráfego IP com um endereço de origem de 172.16.1.111 e um endereço de destino de 172.16.2.22 provocou uma tentativa de discagem na relação Async1.

[Roteamento](#)

Uma vez que definido, os pacotes interessantes devem ser distribuídos corretamente para que um atendimento seja iniciado. O processo de roteamento depende de duas coisas: entradas de tabela de roteamento e “acima” da relação sobre que aos pacotes de rota.

[Relações - up/up \(spoofing\)](#)

Para que os pacotes sejam distribuídos e através de uma relação, essa relação deve ser Up/Up como visto nas **relações de uma mostra** output:

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

Que acontece a uma interface do discador que não seja conectada? Se o protocolo não é em serviço na relação, a implicação é que a relação própria não estará acima. Distribui que confiam nessa relação serão niveladas da tabela de roteamento, e o tráfego não será distribuído a essa relação. O resultado é que nenhum atendimento estaria iniciado pela relação.

A solução para opor esta possibilidade é permitir o estado up/up (falsificação) para interfaces do discador. Toda a relação pode ser configurada como uma interface do discador. Por exemplo, uma série ou uma interface assíncrona podiam ser feitas em um discador adicionando o comando dialer in-band ou dialer dtr à configuração da relação. Estas linhas são desnecessárias para as relações que são por natureza uma interface do discador (BRI e PRI). A saída para uma relação da mostra olhará como esta:

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

Ou seja a relação “finge” ser **Up/Up** de modo que as rotas associadas permaneçam na força e de modo que os pacotes possam ser distribuídos à relação.

Há as circunstâncias sob que uma interface do discador não será **up/up (spoofing)**. **As saídas de interface da mostra** podem mostrar a relação como sendo administrativamente para baixo:

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

Administrativamente abaixo de meramente significa que a relação esteve configurada com o comando shutdown. Este é o estado padrão de toda a interface do roteador quando o roteador é carreg pela primeira vez mesma. Para remediar isto, use o comando interface configuration **nenhuma parada programada**.

A relação pode igualmente ser considerada para reagir do modo standby:

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

Este estado indica que a relação esteve configurada porque o backup para uma outra relação. Quando uma conexão exige a Redundância em caso da falha, uma interface do discador pode ser estabelecida o backup. Isto é realizado adicionando os comandos seguintes à relação da conexão principal:

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

Uma vez que o **comando backup interface** foi configurado, a relação usada como o backup estará posta no modo standby até que hora como a interface principal vá a um estado de **para baixo/para baixo**. Naquele tempo, a interface do discador configurada como um backup, irá a um estado de up/up (**FALSIFICAÇÃO**) durante um evento do seletor.

[Rotas estáticas e Rotas estáticas flutuantes](#)

A maneira mais certa aos pacotes de rota a uma interface do discador é com roteamento estático. Estas rotas são entradas manualmente na configuração do roteador ou do servidor de acesso com o comando:

máscara do prefixo da rota IP {endereço | [distance] da relação}

prefixo: Prefixo da rota IP para o destino.

máscara: Máscara do prefixo para o destino.

endereço: Endereço IP de Um ou Mais Servidores Cisco ICM NT do salto seguinte que pode ser usado para alcançar a rede de destino.

interface: Interface de rede a usar-se para o tráfego de saída.

distância: (Opcional) uma distância administrativa. Este argumento é usado nas Rotas estáticas flutuantes.

As rotas estáticas são usadas nas situações onde o link de discagem é a única conexão ao local remoto. Uma rota estática tem um valor de distância administrativa de um (1), que o faz preferido sobre rotas dinâmica ao mesmo destino.

Por outro lado, as Rotas estáticas flutuantes - isto é, rotas estáticas com uma distância administrativa predefinida - são usadas tipicamente nos cenários DDR de backup. Nestas encenações um protocolo de roteamento dinâmico, tal como o RASGO ou o EIGRP, distribui pacotes através do link principal.

Uma rota estática normal (distância administrativa = 1) é preferível ao EIGRP (distância administrativa = 90) ou ao RASGO (distância administrativa = 120). A rota estática faz com que os pacotes sejam distribuídos através da linha de discagem, mesmo se o preliminar é ascendente e capaz de passar o tráfego. Se, contudo, a rota estática é configurada com uma distância administrativa mais alta do que aquela de alguns dos protocolos de roteamento dinâmico no uso no roteador, a Rota estática flutuante estará usada somente na ausência de uma rota "melhor" - uma com uma distância administrativa mais baixa.

Se o backup DDR está sendo invocado por meio do **comando backup interface**, a situação é um tanto diferente. Porque a interface do discador permanece no modo standby quando o preliminar estiver **acima**, uma rota estática ou uma Rota estática flutuante podem ser configuradas. A interface do discador não tentará conectar até depois a interface principal vai **abaixo de/para baixo**.

Para uma conexão dada, o número (ou a estática flutuante) de rotas estáticas necessárias são uma função do endereçamento nas interfaces do discador. Nos casos onde as duas interfaces do discador (uma em cada um dos dois Roteadores) compartilham de uma rede comum ou de uma sub-rede, tipicamente somente uma rota estática é exigida. Aponta ao LAN remota usando o endereço da interface do discador do roteador remoto como o endereço de próximo salto.

Exemplos

Exemplo 1: O seletor é a única conexão usando interfaces numeradas. Uma rota é suficiente.

Figura 16-4: Seletor 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: O seletor é a única conexão usando interfaces não numeradas. Isto pode ser configurado com a apenas uma rota, mas é comum configurar duas rotas: uma host-rota à interface de LAN no roteador remoto e uma rota ao LAN remota através do LAN remota conectam. Isto é feito para impedir os problemas de mapeamento Layer3-to-Layer2, que podem

conduzir às falhas de encapsulamento.

Este método é usado igualmente se as interfaces do discador nos dois dispositivos são numeradas, mas não na mesma rede ou sub-rede.

Figura 16-5: Seletor 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: O seletor é uma conexão de backup usando interfaces numeradas. Uma Rota estática flutuante é exigida.

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: O seletor é uma conexão de backup usando interfaces não numeradas. Como no exemplo 2 acima, este método é usado igualmente se as interfaces do discador nos dois dispositivos são numeradas, mas não na mesma rede ou sub-rede.

Figura 16-7: Backup usando relações de Unnumbered

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

Mapas de discagem

O discador (legado) DDR com base no mapa é extensibilidade poderosas e suas das limitações da influência escamação detalhadas, mas e. O discador DDR com base no mapa é baseado em uma associação estática entre a especificação do atendimento do destino per. e a configuração de interface física.

Contudo, o discador DDR com base no mapa igualmente tem muitas forças. Apoia Frame Relay, ISO CLNS, LAPB, Roteamento Snapshot, e todos os protocolos roteado que são apoiados em roteadores Cisco. À revelia, o discador DDR com base no mapa apoia o interruptor rápido.

Ao configurar uma relação para a chamada de saída, um mapa de discadores deve ser configurado para cada destino remoto, e para cada número chamado diferente no destino remoto. Por exemplo, se você quer uma conexão de PPP multilink ao discar de um ISDN BRI em uma outra relação do ISDN BRI que tenha um número de diretório local diferente para cada um de seus canais B, você precisa um mapa de discadores 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 em que os Mapas de discagem são configurados pode ser importante. Se dois ou mais comandos dialer map referem o mesmo endereço remoto, o roteador ou o servidor de acesso tentá-los-ão um após o outro, em ordem, até que estabeleça com sucesso uma conexão

Nota: Os IO podem dinamicamente construir Mapas de discagem em um roteador que recebe um atendimento. O mapa de discadores é construído com base no nome de usuário autenticado e no endereço IP de Um ou Mais Servidores Cisco ICM NT negociado do chamador. Os mapas de discadores dinâmicos podem somente ser vistos na saída do comando show dialer map. Você não pode vê-los na configuração running do roteador ou do servidor de acesso.

Sintaxe do comando

Use o seguinte formulário do **comando dialer map interface configuration** a:

- configurar uma interface serial ou uma interface para chamar um ou sites múltiplo, ou
- receba atendimentos das sites múltiplo.

Todas as opções são mostradas neste primeiro formulário do comando. Para suprimir de uma entrada de mapa de discador particular, não use **nenhum** formulário deste 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 o seguinte formulário do **comando dialer map** a:

- configurar uma interface serial ou uma interface para colocar um atendimento às sites múltiplo, e
 - para autenticar atendimentos das sites múltiplo.
- ```
dialer map protocol next-hop-address [name
hostname] [spc] [speed 56 | 64]
[broadcast] [dial-string[:isdn-subaddress]]
```

Use o seguinte formulário do **comando dialer map** configurar uma interface serial ou uma interface para apoiar a construção de uma ponte sobre.

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

Use o seguinte formulário do **comando dialer map** configurar um interface assíncrono para colocar um atendimento a:

- um único local que exijam um script de sistema ou que não tenha nenhum script de modem atribuído, ou
  - sites múltiplo em uma linha única, em múltiplas linhas, ou em um grupo giratório de discador.
- ```
dialer map protocol next-hop-address [name hostname] [broadcast]
[modem-script modem-regexp] [system-script system-regexp] [dial-string]
```

Descrição da sintaxe

- palavras-chaves do *protocolo de protocolo*. Use um do seguinte: **APPLETALK**, **ponte**, **clns**, **DECNet**, **IP**, **IPX**, **novell**, **instantâneo**, **videiras**, ou **XNS**.
- *endereço de próximo salto* - O endereço de protocolo usado para combinar contra os endereços a que os pacotes são destinados. Este argumento não é usado com a palavra-chave do **Bridge Protocol**.
- **nome** - (opcional) indica o sistema remoto com que o roteador local ou o servidor de acesso se comunicam. Usado para autenticar o sistema remoto em chamadas recebidas.

- *hostname* - nome que diferencia maiúsculas de minúsculas (opcional) ou ID do dispositivo remoto (geralmente o nome de host). Para os roteadores com interfaces, o campo do *hostname* pode conter o número que a linha de chamada ID fornece (nos casos onde Calling Line Identification, igualmente referido como o *CLI*, *ID de chamada*, e *identificação de número automática* (ANI), está disponível).
- **spc** - (opcional) especifica uma conexão semipermanente entre o equipamento do cliente e a troca. É usada somente em Alemanha para circuitos entre um ISDN BRI e um switch ISDN 1TR6 e em Austrália para circuitos entre um ISDN PRI e um interruptor TS-014.
- **velocidade 56 | 64** - palavra-chave (opcional) e avaliam indicar a velocidade de linha nos kilobits por segundo para usar-se. Usado para o ISDN somente. A velocidade padrão é 64 kbps.
- **transmissão** - (opcional) indica que as transmissões devem ser enviadas a este endereço de protocolo.
- **script de modem** - (opcional) indica o script de modem a ser usado para a conexão (para interface assíncrono).
- *modem-regexp* - expressão regular (opcional) a que um script de modem será combinado (para interface assíncrono).
- **script de sistema** - (opcional) indica o script de sistema a ser usado para a conexão (para interface assíncrono).
- *sistema-regexp* - expressão regular (opcional) a que um script de sistema será combinado (para interface assíncrono).
- *série de discagem* [: número de telefone (opcional) do *sub-endereço ISDN*] enviado ao dispositivo de discagem após reconhecimento dos pacotes com um endereço de próximo salto especificado que combine a lista de acessos definida (e o número opcional do subaddress usado para conexões multiponto ISDN). A série de discagem e o sub-endereço ISDN, se usados, devem ser o último artigo na linha de comando.

[Perfis de discador](#)

Nota: Nesta seção o termo “interface do discador” refere a interface configurada; não a uma interface física no roteador ou no servidor de acesso.

A aplicação dos Perfis de discagem do DDR, introduzida na Versão do IOS 11.2, é baseada em uma separação entre lógico e a configuração de interface física. Os Perfis de discagem igualmente permitem que as configurações lógica e física sejam limitadas junto dinamicamente na por chamada.

A metodologia dos Perfis de discagem é vantajosa quando você quer fazer o seguinte:

- compartilhe de uma relação (ISDN, assíncrono, ou do serial síncrona) para colocar ou receber atendimentos
- mude toda a configuração em uma base do usuário per. (exceto o encapsulamento na primeira fase de Perfis de discagem)
- ponte a muitos destinos
- evite problemas rachados do horizonte

Os Perfis de discagem permitem a configuração das interfaces física seja separada da configuração lógica exigida para um atendimento, e igualmente permitem que as configurações lógica e física sejam limitadas junto dinamicamente na por chamada.

Um perfil do Dialer consiste nos seguintes elementos:

- Uma configuração da *interface do discador* (uma entidade lógica), incluindo umas ou várias séries de discagem (cada qual é usada para alcançar uma sub-rede de destino)
- *Uma classe de mapa de discadores* que defina todas as características para todo o atendimento à série de discagem especificada
- *Um pool de discadores* pedido das interfaces física a ser usadas pela interface do discador

Tudo chama indo a ou do mesmo uso da sub-rede de destino o mesmo perfil do discador.

Uma configuração da interface do discador inclui todos os ajustes necessários alcançar uma sub-rede de destino específica (e algumas redes alcançadas através dela). As séries de discagem múltiplas podem ser especificadas para a mesma interface do discador; cada série de discagem pode ser associada com uma classe de mapa de discadores diferente. A classe de mapa de discadores define todas as características para todo o atendimento à série de discagem especificada. Por exemplo, a classe de mapas para um destino pôde especificar uma velocidade 56-kbps ISDN. A classe de mapas para um destino diferente pôde especificar uma velocidade 64-kbps ISDN.

Cada interface do discador usa um pool de discadores, que seja um pool de interface física pedido com base na prioridade atribuída a cada interface física. Uma interface física pode pertencer aos pool de discadores múltiplos, com a disputa que está sendo resolvida pela prioridade. As relações do ISDN BRI e PRI podem ajustar um limite no mínimo e no número máximo de canais B reservados por todos os pool de discadores. Um canal reservado por um pool de discadores permanece inativo até que o tráfego esteja dirigido ao pool.

Quando os Perfis de discagem são usados para configurar o DDR, uma interface física não tem nenhum ajuste de configuração exceto o encapsulamento e os pool de discadores a que a relação pertence.

Nota: O parágrafo precedente tem uma exceção. Os comandos que se aplicam antes que a autenticação esteja completa devem ser configurados na relação física (ou BRI ou PRI) e não no perfil do discador. Os Perfis de discagem não fazem comandos ppp authentication de cópia (ou comandos LCP) à interface física.

Figura 16-8 mostra um aplicativo comum dos Perfis de discagem. O roteador A tem a interface do discador 1 para o Dial-on-Demand Routing (DDR) com a sub-rede 1.1.1.0, e a interface do discador 2 para o Dial-on-Demand Routing (DDR) com a sub-rede 2.2.2.0. O endereço IP de Um ou Mais Servidores Cisco ICM NT para a interface do discador 1 é seu endereço como um nó na rede 1.1.1.0. Ao mesmo tempo, esse endereço IP de Um ou Mais Servidores Cisco ICM NT serve como o endereço IP de Um ou Mais Servidores Cisco ICM NT das interfaces física usadas pela interface do discador 1. Similarmente, o endereço IP de Um ou Mais Servidores Cisco ICM NT para a interface do discador 2 é seu endereço como um nó na rede 2.2.2.0.

Figura 16-8: Aplicativo típico dos Perfis de discagem

Uma interface do discador usa somente um pool de discadores. Uma interface física, contudo, pode ser um membro de um ou muito pool de discadores, e um pool de discadores pode ter diversas interfaces física como membros.

Figura 16-9 ilustra as relações entre os conceitos da interface do discador, do pool de discadores, e das interfaces física. O BRI 1 da interface física do pool de discadores 2. dos usos da interface do discador 0 pertence ao pool de discadores 2 e tem uma prioridade específica no pool. A

interface física BRI2 igualmente pertence ao pool de discadores 2. Porque a disputa é resolvida com base em níveis da prioridade das interfaces físicas no pool, BRI 1 e o BRI2 têm que ser atribuídos as prioridades diferentes no pool. Talvez o BRI 1 é a prioridade designada 100 e o BRI2 é 50 pés da prioridade designada no pool de discadores 2 (uma prioridade dos 50 pés é mais alta do que uma prioridade de 100). O BRI2 tem uma prioridade mais alta no pool, e seus atendimentos serão colocados primeiramente.

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

[Etapas da configuração do perfil de discador](#)

Comando	Propósito
<code>interface dialer number</code>	Crie uma interface do Dialer.
<code>máscara de endereço do endereço IP de Um ou Mais Servidores Cisco ICM NT</code>	Especifique o endereço IP e a máscara da interface do discador como um nó na rede de destino a ser chamada.
<code>encapsulamento ppp</code>	Especifique o encapsulamento PPP.
<code>dialer remote-name username</code>	Especifique o nome da autenticação chap do roteador remoto.
<code>dialer string dial-string class class-name</code>	Especifique o destino remoto a ser chamado e a classe de mapa que define as características das chamadas a este destino.
<code>poolnumber do discador</code>	Especifique o pool de discagem a ser usado para chamadas para esse destino.
<code>dialer-group group-number</code>	Atribua a interface do Dialer a um grupo de discadores.
<code>dialer-list dialer-group protocol protocol-name {permit negue list access-list-number}</code>	Especifique uma lista de acessos pelo número de listas ou pelo protocolo e pelo número de listas para definir os pacotes "interessantes" que podem provocar um atendimento.

[Operações PPP](#)

O Point-to-Point Protocol (PPP) é de longe o protocolo de transporte o mais comum da camada de link, usurpando completamente o SLIP como o protocolo da escolha para o seletor (e em muitos casos, NON-seletor) síncrono e as conexões de série síncrona. O PPP foi definido originalmente em 1989 pelo RFC 1134, que tem sido feito desde Obsoleto por uma série de RFC que culminam (até à data desta escrita) no RFC1661. Há igualmente os RFC numerosos que definem elementos do protocolo, tais como o RFC1990 (o protocolo do multilink de PPP), o RFC2125 (o protocolo bandwidth allocation PPP), e o muito outro. Um repositório on-line dos RFC

pode ser encontrado em:

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

Talvez a melhor definição do PPP pode ser encontrada no RFC1661, que indica:

O Point-to-Point Protocol (PPP) fornece um método padrão transportando datagramas de multiprotocolo sobre os link de ponto a ponto. O PPP é compreendido de três componentes principais:

1. Um método para encapsular datagramas de multiprotocolo.
2. Um protocolo de controle de link (LCP) para estabelecer, configurar, e testar a conexão de link de dados.
3. Uma família dos protocolos network control (NCP) para estabelecer e configurar protocolos de camada de rede diferentes.

Fases da negociação de PPP

A negociação de PPP consiste em três fases: Protocolo de controle de link (LCP), autenticação, e protocolo network control (NCP). Cada um continua em ordem, seguindo o estabelecimento do async ou da conexão ISDN.

LCP

O PPP não segue um modelo cliente/servidor. Todas as conexões são peer-to-peer. Consequentemente, quando há um chamador e um receptor, o ambas as extremidades da conexão Point-to-Point deve concordar com os protocolos e os parâmetros negociados.

Quando a negociação começa, cada um dos pares que querem estabelecer uma conexão PPP deve enviar um pedido configurar (visto dentro **debugar a negociação ppp** e referido daqui por diante como o CONFREQ). São incluídas no CONFREQ todas as opções que não forem o padrão do link. Estes incluem frequentemente o Maximum Receive Unit (MRU), o Async Control Character Map (ACCM), o protocolo de autenticação (AuthProto), e o número mágico. Igualmente são considerados o Maximum Receive Reconstructed Unit (MRRU) e o discriminador de ponto final (EndpointDisc), usado para o Multilink PPP.

Há três possíveis respostas a todo o CONFREQ:

- Um Configurar-reconhecimento (CONFACK) deve ser emitido se o par reconhece as opções e concorda aos valores vistos no CONFREQ.
- Uma Configurar-rejeição (CONFREJ) deve ser enviada se algumas das opções no CONFREQ não estão reconhecidas (por exemplo, algumas opções específicas do fornecedor) ou se os valores para algumas das opções foram recusados explicitamente na configuração do par.
- Um Configurar-Negativo-reconhecimento (CONFNAK) deve ser enviado se todas as opções no CONFREQ são reconhecidas, mas os valores não é aceitável ao par.

Os dois pares continuam a trocar CONFREQ, CONFREJ e CONFNAK até que cada um envie um CONFACK, até que a conexão de discagem esteja quebrada, ou até um ou ambos os pares indica que a negociação não pode ser terminada.

Autenticação

Após a conclusão bem sucedida da negociação de LCP e de alcançar um acordo no AuthProto, a próxima etapa é autenticação. A autenticação, quando não imperativa pelo RFC1661, é altamente recomendado em todas as conexões de discagem. Em alguns casos, é uma exigência para a operação apropriada; Perfis de discagem que são uma capitalização em ponto.

Os dois tipos principais de autenticação no PPP são o protocolo password authentication (PAP) e o protocolo de autenticação de cumprimento do desafio (RACHADURA), definido pelo RFC1334 e atualizado pelo RFC1994.

O PAP é o mais simples dos dois, mas é menos seguro porque a senha de texto é enviada através da conexão de discagem. A RACHADURA é mais segura porque a senha de texto não é enviada nunca através da 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 “solicitador” e “autenticador” para distinguir os papéis jogados pelos dispositivos em uma ou outra extremidade da conexão, embora um ou outro par pode atuar em um ou outro papel. O “solicitador” descreve o dispositivo que pede o acesso de rede e fornece a informação da autenticação; o “autenticador” verifica que a validade da informação da autenticação e permite ou recusa a conexão. É comum para que ambos os pares atuem em ambos os papéis quando uma conexão DDR está sendo feita entre o Roteadores.

PAP

O PAP é razoavelmente simples. Após a conclusão bem sucedida da negociação de LCP, o solicitador envia repetidamente sua combinação de nome de usuário/senha através do link até que o autenticador responda com um reconhecimento ou até que o link esteja quebrado. O autenticador pode desligar o link se determina que a combinação de nome de usuário/senha é inválida.

RACHADURA

A RACHADURA é um tanto mais complicada. O autenticador envia um desafio ao solicitador, que responde então com um valor. Este valor é calculado usando uma função da “mistura de sentido único” para picar junto o desafio e a senha da RACHADURA. O valor resultante é enviado ao autenticador junto com o chap hostname do solicitador (que pode ser diferente de seu nome de host real) em um *mensagem de resposta*.

O autenticador lê o hostname no mensagem de resposta, olha acima a senha prevista para esse hostname, e calcula então o valor que espera o solicitador enviado em sua resposta executando a mesma função de mistura o solicitador executada. Se os valores resultantes combinam, a autenticação é bem sucedida. A falha deve conduzir a uma desconexão.

AAA

Um serviço da autenticação, da autorização e da contabilidade (AAA), tal como o TACACS+ ou o RADIUS, pode ser usado em realizar o PAP ou a RACHADURA.

NCP

Após a autenticação bem sucedida, a fase NCP começa. Como no LCP, os pares trocam CONFREQ, CONFREJ, CONFNAK e CONFACK. Contudo, nesta fase de negociação, os elementos que estão sendo negociados têm que fazer com protocolos de camada mais elevada - IP, IPX, construindo uma ponte sobre, CDP, e assim por diante. Uns ou vários destes protocolos podem ser negociados. Porque é o mais de uso geral, e porque outros protocolos operam no muito a mesma forma, o protocolo de controle do protocolo de internet (IPCP), definido no RFC1332, é o foco desta discussão. Outros RFC pertinentes incluem, mas não são limitados a:

- RFC1552 (protocolo de controle de IPX)
- RFC1378 (protocolo de controle apple talk)
- RFC1638 (protocolo bridging control)
- RFC1762 (protocolo de controle do DECNet)
- RFC1763 (protocolo de controle das videiras)

Além, o protocolo de controle do protocolo cisco discovery (CDPCP) pode ser negociado durante o NCP, embora este não é comum. Os engenheiros de TAC da Cisco recomendarão geralmente que o comando no cdp enable esteja configurado em alguns e todas as interfaces do discador para impedir os pacotes de CDP que mantêm um atendimento acima 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 par já tem um endereço, enviará esse endereço em um CONFREQ ao outro par. Se o endereço é aceitável ao outro par, um CONFACK estará retornado. Se o endereço não é aceitável, a resposta será um CONFNAK que contém um endereço para que o par use-se.

Se o par não tem nenhum endereço, enviará um CONFREQ com o endereço 0.0.0.0. Isto diz o outro par para atribuir um endereço, que seja realizado pela emissão de um CONFNAK com o endereço adequado.

As outras opções podem ser negociadas no IPCP. Geralmente - vistos são o preliminares e os endereços secundários para o Domain Name Server e o servidor de nome de netbios, como descrito no RFC1877 informativo. O protocolo de compactação IP (RFC1332) é igualmente comum.

Metodologias de PPP alternado

As metodologias de PPP alternado incluem o Multilink PPP, o multichassis PPP, e os Perfis virtuais.

Multilink PPP

A característica do protocolo multilink point-to-point (MLP) fornece a funcionalidade de balanceamento de carga sobre link de WAN múltiplo. Ao mesmo tempo fornece a Interoperabilidade do multi-vendedor, a fragmentação de pacote de informação e arranjar em seqüência apropriado, e cálculo de carga em ambos tráfego de entrada e de saída. A implementação Cisco do Multilink PPP apoia as especificações da fragmentação e do seqüenciamento de pacote no RFC1717.

O Multilink PPP permite que os pacotes sejam fragmentados. Estes fragmentos podem ser enviados ao mesmo tempo sobre link múltiplo Point-to-Point ao mesmo endereço remoto. Os links

múltiplos vêm acima em resposta a um limiar de carga de discador que você defina. A carga pode ser calculada no tráfego de entrada, tráfego de saída, ou em qualquer um, como necessária para o tráfego entre os locais específicos. O MLP fornece a largura de banda por encomenda e reduz a latência da transmissão através dos links MACILENTOS.

O Multilink PPP trabalha sobre os seguintes tipos de interface (únicos ou) que múltiplos são configurados para apoiar grupos giratórios e encapsulamento PPP da Discagem sob demanda:

- interfaces serial assíncronas
- BRI
- PRI

Configuração

Para configurar o Multilink PPP em interface assíncrono, você configura os interface assíncrono para apoiar o DDR e o encapsulamento PPP. Você configura então uma interface do discador para apoiar o encapsulamento PPP, a largura de banda por encomenda, e o Multilink PPP. Em algum momento, contudo, adicionar mais interface assíncrono não melhora o desempenho. Com o tamanho de MTU default, o Multilink PPP deve apoiar três interface assíncrono usando o Modems V.34. Contudo, os pacotes puderam ser deixados cair ocasionalmente se o MTU é pequeno ou se as grandes explosões dos frames curtos ocorrem.

Para permitir o Multilink PPP em uma única relação do ISDN BRI ou PRI, você não é exigido definir separadamente um grupo giratório de discador porque as interfaces são grupos giratórios de discador à revelia. Se você não usa procedimentos da autenticação de PPP, seu serviço de telefonia deve passar a informação de identificador de chamada.

Um número do limiar de carga é exigido. Para um exemplo de configurar o Multilink PPP em uma única relação do ISDN BRI, veja o *exemplo de multilink PPP em uma interface* abaixo.

Quando o Multilink PPP é configurado e você quer um conjunto multilink ser conectado indefinidamente, use o **comando dialer idle-timeout** ajustar um temporizador de ociosidade muito alto. O **comando dialer-load threshold 1** não mantém um conjunto multilink de links *n* conectados indefinidamente, e o **comando dialer-load threshold 2** não mantém um conjunto multilink de dois links conectados indefinidamente.

Para permitir o Multilink PPP no ISDN múltiplo BRI ou nas relações PRI, você estabelece uma relação giratória do discador e configurar-la para o Multilink PPP. Você configura então os BRI separadamente e adicionar-los cada um ao mesmo grupo giratório. Veja o *exemplo de multilink PPP em interfaces ISDN múltiplas* abaixo.

Exemplo de multilink PPP em uma interface

O exemplo seguinte permite o Multilink PPP na interface BRI 0. Quando um BRI é configurado, nenhuma configuração de grupo giratório de discador está exigida (a interface é um grupo giratório à revelia).

```
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 multilink PPP em interfaces ISDN múltiplas

O exemplo seguinte configura o ISDN múltiplo BRI para pertencer ao mesmo grupo giratório de discador para o Multilink PPP. Use o **comando dialer rotary-group** atribuir cada um do ISDN BRI a esse grupo giratório de discador que deve combinar o número da interface do discador (número 0 neste caso).

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

Multilink de Multichassi PPP

O Multilink PPP fornece a capacidade de rachadura e de pacotes de recombinação a um único sistema final através de uma tubulação lógica (igualmente chamada um *pacote*) formada por links múltiplos. O Multilink PPP fornece a largura de banda por encomenda e reduz a latência da transmissão através dos links MACILENTOS.

O Multilink de Multichassi PPP (MMP), por outro lado, fornece a capacidade adicional para que os links terminem em roteadores múltiplos com endereços remotos diferentes. O MMP pode igualmente segurar ambo o tráfego analógico e digital.

Esta funcionalidade é pretendida para as situações em que há grandes associações dos usuários de discagem de entrada, em que um único servidor de acesso não pode fornecer bastante portas de discagem. O MMP permite que as empresas forneçam um único número dialup a seus usuários e apliquem a mesma solução às chamadas analógicas e digital. Esta característica permite que os provedores de serviços de Internet, por exemplo, atribuam um único número giratório ISDN aos diversos ISDN PRI através de diversos Roteadores.

Para uma descrição completa dos comandos mmp providos nisto, refira a *referência do comando solutions do discagem da Cisco*. Para encontrar a documentação de outros comandos que aparecem neste capítulo, usam o índice principal de referência de comando ou o procuram em linha.

O MMP é apoiado no Cisco 7500, 4500, e em Plataformas do 2500 Series e no serial síncrona, na série assíncrona, no ISDN BRI, no ISDN PRI, e nas interfaces do discador.

O MMP não exige a reconfiguração dos switch de companhia telefônica.

Configuração

O Roteadores ou os servidores de acesso são configurados para pertencer aos grupos de pares, chamados *grupos de pilhas*. Todos os membros do grupo de pilhas são pares; os grupos de pilhas não precisam um roteador líder permanente. Todo o membro de grupo de pilhas pode responder aos atendimentos que vêm de um único número de acesso, que seja geralmente um grupo de buscas ISDN PRI. Os atendimentos podem vir dentro dos dispositivos do usuário remoto, tais como o Roteadores, o Modems, os adaptadores terminal de ISDN, ou as placas de PC.

Uma vez que uma conexão é estabelecida com o um membro de um *grupo de pilhas*, esse membro possui o atendimento. Se uma segunda chamada vem dentro do mesmo cliente e um roteador diferente responde ao atendimento, o roteador estabelece túnel e para a frente todos os pacotes que pertencem ao atendimento ao roteador que possui o atendimento. O processo de estabelecer um túnel e de transmissão chama com ele ao roteador que possui o atendimento é chamado às vezes *projetar o link de PPP ao mestre do atendimento*.

Se mais roteador potente está disponível, pode ser configurado como um membro do grupo de pilhas e os outros membros de grupo de pilhas podem estabelecer túneis e dianteiro todos os atendimentos a ele. Em tal caso, os outros membros de grupo de pilhas apenas estão respondendo que os atendimentos e o tráfego de encaminhamento ao mais poderoso *offload* o roteador.

Nota: As linhas MACILENTOS da Alta latência entre membros de grupo de pilhas podem fazer a operação do grupo de pilhas incapaz.

O tratamento de chamada MMP, oferecendo, e mergulha 2 operações de encaminhamento no grupo de pilhas continua como segue. Igualmente mostra-se em figura 16-10.

1. Quando a primeira chamada entrar ao grupo de pilhas, respostas do roteador A.
2. No oferecimento, o roteador A ganha porque já tem o atendimento. O roteador A transforma-se o atendimento-*mestre* para essa sessão com o dispositivo remoto. O roteador A pôde igualmente ser chamado o *host ao feixe de interface mestre*.
3. Quando o dispositivo remoto que iniciou o atendimento precisa mais largura de banda, faz um segundo atendimento do Multilink PPP ao grupo.
4. Quando a segunda chamada entra, o roteador D responde-lhe e informa-o o grupo de pilhas. O roteador A ganha o oferecimento porque já está segurando a sessão com esse dispositivo remoto.
5. O roteador D estabelece um túnel ao roteador A e para a frente os dados crus PPP ao roteador A.
6. O roteador A remonta e novas sequências os pacotes.
7. Se mais atendimentos entram ao roteador D e pertencem demasiado ao roteador A, o túnel entre A e D amplia para segurar o tráfego adicionado. O roteador D não estabelece um túnel adicional ao A.
8. Se mais atendimentos entram e são respondidos por qualquer outro roteador, esse roteador igualmente estabelece um túnel a A e para a frente aos dados crus PPP.
9. Os dados remontados são passados na rede corporativa como se mandaram todos vir através de um enlace físico.

Figura 16-10: Cenário PPP típico do Multilink de Multichassi

Em contraste com a figura precedente, figura 16-11 caracteriza um roteador do offload. Os servidores de acesso que pertencem aos atendimentos de uma resposta do grupo de pilhas, estabelecem túneis, e para a frente chamam-nos a um Cisco 4700 Router que ganhe o oferecimento e são-nos o atendimento-mestre para todos os atendimentos. O Cisco 4700 remonta e novas sequências todos os pacotes que entram através do grupo de pilhas.

Figura 16-11: Multilink de Multichassi PPP com um roteador do Offload como um membro de grupo de pilhas

Nota: Você pode construir os grupos de pilhas que usam o servidor de acesso diferente, o interruptor, e as plataformas de roteador. Contudo, os servidores de acesso universal tais como o Cisco AS5200 não devem ser combinados com o ISDN. Isto deve somente ser feito com os servidores de acesso tais como a plataforma 4x00. Porque os atendimentos do escritório central são atribuídos em uma maneira arbitrária, esta combinação poderia conduzir a uma chamada analógica que está sendo entregue a um servidor de acesso digital-somente, que não pudesse segurar o atendimento.

O apoio MMP em um grupo de Roteadores exige que cada roteador esteja configurado para apoiar o seguinte:

- Multilink PPP
- Protocolo stack group bidding (SGBP)
- Molde virtual usado clonando a configuração da interface para apoiar o MMP

Perfis virtuais

Os Perfis virtuais são um aplicativo original do Point-to-Point Protocol (PPP) que possa criar e configure uma interface de acesso virtual dinamicamente quando uma chamada de discagem de entrada é recebida, e rasgar para baixo a relação dinamicamente quando o atendimento termina. Os Perfis virtuais trabalham com PPP direto e com Multilink PPP (MLP).

A informação de configuração para uma interface de acesso virtual dos Perfis virtuais pode vir de uma relação virtual do molde, ou da configuração usuário-específica armazenada em um server do Authentication, Authorization, and Accounting (AAA), ou em ambos.

A configuração do user-specific aaa usada por Perfis virtuais é *configuração da interface* e é transferida durante negociações de LCP. Uma outra característica, chamada Configuração para usuários, igualmente usa a informação de configuração ganhada de um servidor AAA. Contudo, a Configuração para usuários usa a *configuração de rede* (tal como Listas de acesso e filtros da rota) transferida durante negociações de NCP.

Duas regras governam a configuração de interface de acesso virtual por relações virtuais do molde e por configurações de AAA dos Perfis virtuais:

- Cada aplicativo de acesso virtual pode ter, no máximo, um molde de que a clonar. Contudo, pode ter as configurações de AAA múltiplo de que para clonar (Perfis virtuais a informação de AAA e a configuração AAA per-user, que por sua vez puderam incluir protocolos da configuração de várias).
- Quando os Perfis virtuais são configurados pelo molde virtual, seu molde tem a prioridade

mais alta do que todo o outro molde virtual.

Veja “Interoperabilidade com a seção de outras falhas de discagem Cisco” abaixo para uma descrição das sequências da possível configuração que dependem da presença ou da ausência pelo MLP ou por uns outros recursos de acesso virtual que clonem uma relação virtual do molde.

Esta característica é executado em todas as plataformas do IOS da Cisco que apoiam o MLP.

Para uma descrição completa dos comandos mencionados nesta seção, refira os “Perfis virtuais comanda” o capítulo no *Dial Solutions Command Reference* no grupo da documentação IOS Cisco. Para encontrar a documentação de outros comandos que aparecem neste capítulo, você pode usar o índice principal de referência de comando ou procurá-lo em linha.

Informações de Apoio

Esta seção apresenta a informações de fundo sobre Perfis virtuais para ajudá-lo a compreender este aplicativo antes que você comece o configurar.

Restrições

Nós recomendamos que os endereços unnumbered estejam usados nas relações virtuais do molde para se assegurar de que os endereços de rede duplicados não estejam criados em interfaces de acesso virtual.

Pré-requisitos

O uso da informação de configuração de interface de AAA usuário-específico com Perfis virtuais exige o roteador ser configurado para o AAA e exige o servidor AAA ter pares AV da configuração de interface usuário-específica. Os pares AV relevantes (em um servidor Radius) começam como segue:

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

A informação que segue o sinal de igual (=) poderia ser todo o comando configuration da interface Cisco IOS. Por exemplo, a linha pôde ser a seguinte:

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

O uso de uma relação virtual do molde com os Perfis virtuais exige um molde virtual ser definido especificamente para Perfis virtuais.

Interoperabilidade com outras falhas de discagem Cisco

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

[Configuração DDR das interfaces física](#)

Os Perfis virtuais interoperam inteiramente com interfaces física nos seguintes estados da configuração DDR quando nenhum outro aplicativo da interface de acesso virtual é configurado:

- Os Perfis de discagem são configurados para a relação. O perfil do discador é usado em vez

da configuração dos Perfis virtuais.

- O DDR não é configurado na relação. Os Perfis virtuais cancelam a configuração atual.
- O DDR anterior é configurado na relação. Os Perfis virtuais cancelam a configuração atual.

Nota: Se uma interface do discador está usada (incluindo algum discador ISDN), sua configuração está usada na interface física em vez da configuração dos Perfis virtuais.

Efeito do Multilink PPP na configuração de interface de acesso virtual

Segundo as indicações da tabela 16-8, a configuração exata de uma interface de acesso virtual depende dos seguintes três fatores:

- Se os Perfis virtuais estão configurados pelo molde virtual, pelo AAA, por ambos, ou por nenhuns. Estes estados são mostrados como o “VP VT somente,” o “VP AAA somente,” o “VP VT e o VP AAA,” e o “nenhum VP de todo,” respectivamente, na tabela.
- A presença ou a ausência de uma interface do discador.
- A presença ou a ausência de MLP. A etiqueta “MLP” da coluna é uma substituição todos os recursos de acesso virtual que apoiarem o MLP e o clonarem de uma relação virtual do molde.

Na tabela 16-8, o “Multilink VT” significa que uma relação virtual do molde está clonada se se é definido para o MLP ou uns recursos de acesso virtual que usem o MLP.

Tabela 16-8: Sequência da clonagem da configuração dos Perfis virtuais

Configuração dos Perfis virtuais	MLP nenhum discador	Discador MLP	Nenhum MLP nenhum discador	Nenhum discador MLP
VP VT somente	VP VT	VP VT	VP VT	VP VT
VP AAA somente	(Multilink VT) VP AAA	(Multilink VT) VP AAA	VP AAA	VP AAA
VP VT e VP AAA	VP AAA DO VP VT	VP AAA DO VP VT	VP AAA DO VP VT	VP AAA DO VP VT
Nenhum VP de todo	(Multilink VT)	Discador	Nenhuma interface de acesso virtual é criada.	Nenhuma interface de acesso virtual é criada.

A ordem de artigos em toda a pilha da tabela é importante. Onde o VP VT é mostrado acima o VP AAA, significa que o molde virtual dos Perfis virtuais está clonado primeiramente na relação, e a configuração de interface de AAA para o usuário é-lhe aplicada então. A configuração de interface de AAA usuário-específico adiciona à configuração e cancela todos os comandos de oposição da interface física ou de configuração de molde virtual.

Interoperabilidade com outros recursos que usam moldes virtuais

Os Perfis virtuais igualmente interoperam com aplicativos de acesso virtuais que clonam uma relação virtual do molde. Cada aplicativo de acesso virtual pode ter, no máximo, um molde de que a clonar, mas pode clonar das configurações de AAA múltiplo.

A interação entre Perfis virtuais e outros aplicativos do molde virtual é como segue:

- Se os Perfis virtuais são permitidos e um molde virtual está definido para ele, o molde virtual dos Perfis virtuais está usado.
- Se os Perfis virtuais estão configurados pelo AAA apenas (nenhum molde virtual está definido para Perfis virtuais), o molde virtual para um outro aplicativo de acesso virtual (VPDN, por exemplo) pode ser clonado na interface de acesso virtual.
- Um molde virtual, eventualmente, é clonado a uma interface de acesso virtual antes dos Perfis virtuais configuração de AAA ou configuração AAA per-user. A configuração AAA per-user, se usada, é último aplicado.

Terminologia

Os seguintes termos novos ou raros 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 aos pedidos de autorização específicas de usuário. O roteador interpreta cada par AV como Cisco IOS comando router configuration e aplica os pares AV em ordem. Neste capítulo, o par AV do termo refere um parâmetro de configuração de interface em um servidor Radius.

Um par AV da configuração da interface para Perfis virtuais pode tomar um formulário tal como este:

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

clonar: Criando e configurando uma interface de acesso virtual aplicando comandos configuration de um molde virtual específico. O molde virtual é a fonte da informação sobre o usuário e da informação dependente de roteador genéricas. O resultado da clonagem é uma interface de acesso virtual configurada com todos os comandos no molde.

interface de acesso virtual: Exemplo de uma interface virtual original que seja criada dinamicamente e exista temporariamente. As interfaces de acesso virtual podem ser criadas e configurado diferentemente por aplicativos diferentes, tais como Perfis virtuais e Virtual Private Dialup Networks.

relação virtual do molde: Usuários da configuração da interface genérica com certeza ou para alguma finalidade, mais a informação dependente de roteador. Isto toma o formulário de uma lista de comandos da interface Cisco IOS ser aplicado à interface virtual como necessária.

perfil virtual: O exemplo de uma interface de acesso virtual original que esteja criada dinamicamente quando os usuários determinados chamam dentro, e está rasgado para baixo dinamicamente quando o atendimento desliga. O perfil virtual de um usuário específico pode ser configurado por uma relação virtual do molde, configuração de interface usuário-específica armazenada em um servidor AAA, ou uma relação virtual do molde e configuração de interface usuário-específica do AAA.

A configuração de uma interface de acesso virtual começa com uma relação virtual do molde (eventualmente), seguida pelo pedido da configuração usuário-específica para a sessão de discagem de entrada do usuário particular (eventualmente).

Exemplo anotado de negociação PPP

Neste exemplo, um sibilo traz acima um enlace de ISDN entre o *montecito* do Roteadores e o *Goleta*. Note que, quando não houver nenhum timestamping neste exemplo, se recomenda geralmente que você usa o **service timestamps debug datetime msec** do comando global configuration.

Figura 16-12: Roteador-ISDN-roteador

Estes debugam são tomados do *montecito*; contudo, a eliminação de erros em *Goleta* olharia muito mesmo.

Nota: Seu debuga pode aparecer em um formato diferente. Esta saída é o formato de emissor mais velho do PPP debugging, antes das alterações introduzidas na Versão do IOS 11.2(8). Veja o capítulo 17 para um exemplo do PPP debugging em umas versões mais novas dos IO.

```
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 a fim iniciar uma tentativa de discagem.

B - A conexão é estabelecida (o ISDN debuga não usado neste exemplo).

Comece o LCP:

C - O *montecito* envia pedidos de configuração LCP para o AUTHTYPE e para o MAGICNUMBER.

D - *Goleta* envia seus CONFREQ. Se o valor para o MAGICNUMBER é o mesmo que o valor enviado pelo *montecito*, há uma grande probabilidade que a linha está dada laços.

E - Isto indica que o *montecito* enviou reconhecimentos aos CONFREQ de *Goleta*.

F - O *montecito* recebe CONFACK de *Goleta*.

Comece fase de autenticação:

G, H - Desafio do *montecito* e do *Goleta* para a autenticação.

J - *Goleta* responde ao desafio.

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

M - Mensagem de *Goleta ao montecito*: autenticação bem sucedida.

A negociação de NCP começa:

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

Q, R - O *montecito* envia um CONFACK ao CONFREQ de *Goleta*.

S -? e vice-versa.

T, U - Uma rota é instalada do *montecito a Goleta* e o protocolo na relação muda a “acima de”, indicando que as negociações de NCP terminaram com sucesso.

[Antes de chamar o equipe tac do Cisco Systems](#)

Antes de chamar o centro de assistência técnica (TAC) do Cisco Systems, certifique-se de você ter lido com este capítulo e ter terminado as ações sugeridas para seu problema de sistema.

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

Para todos os problemas, recolha a saída da executar-**configuração da mostra e mostre a versão**. Assegure-se de que o comando `service timestamps debug datetime msec` esteja na configuração.

Para problemas com DDR, recolha o seguinte:

- **mostre o mapa de discadores**
- **debug dialer**
- **negociação de debug ppp**
- **debug ppp authentication**

Se o ISDN é envolvido, recolha:

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

Se o Modems é envolvido, recolha:

- **mostre linhas**
- **mostre a linha [x]**
- **mostre o modem** (se os modems integrados são envolvidos)
- **mostre a versão de modem** (se os modems integrados são envolvidos)
- **debugar o modem**

- **debug modem csm** (se os modems integrados são envolvidos)
- **debugar o bate-papo** (se um cenário DDR)

Se o T1s ou os PRI são envolvidos, recolha:

- **mostre o T1 do controlador**

Informações Relacionadas

- [Guia das soluções de discagem IOS Cisco](#)
- [Visão geral sobre interfaces, controladores e linhas usados para acesso discado](#)
- [Roteamento através das linhas do modem](#)
- [Porta serial e configuração de tronco T1/E1](#)
- [Criação de Inter-redes DDR](#)
- [Decisão e Preparação para Configurar DDR](#)
- [Configurando DDRtitle](#)
- [Visão geral da tecnologia PPP](#)
- [Projetando inter-redes ISDN](#)
- [Tipos de Switch, códigos e valores ISDN](#)
- [Abastecimento a linha de ISDN](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)