DFÜ-Technologie: Übersichten und Erklärungen

Inhalt

Einführung

In diesem Kapitel werden einige der in DFÜ-Netzwerken verwendeten Technologien vorgestellt und erläutert. Sie finden Konfigurationstipps und Interpretationen einiger **show**-Befehle, die zur Überprüfung des ordnungsgemäßen Netzwerkbetriebs nützlich sind. Die Fehlerbehebungsverfahren werden in diesem Dokument nicht behandelt. Sie finden sie im Dokument *Troubleshooting Dialup (Fehlerbehebung bei DFÜ)*.

Bevor Sie beginnen

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips

Conventions.

Voraussetzungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Modembetrieb

In diesem Abschnitt werden Probleme im Zusammenhang mit der Einrichtung, Verifizierung und Verwendung von Modems für Cisco Router beschrieben.

Verwenden des Befehls Modem Autoconfigure

Wenn Sie das Cisco Internetwork Operating System (Cisco IOS) Version 11.1 oder höher verwenden, können Sie Ihren Cisco Router so konfigurieren, dass er automatisch mit dem Modem kommuniziert und konfiguriert.

Führen Sie die folgenden Schritte aus, um einen Cisco Router so zu konfigurieren, dass automatisch versucht wird, zu erkennen, welche Modemart an die Leitung angeschlossen ist, und dann das Modem zu konfigurieren:

1. Um nach dem Modemtyp zu suchen, der an den Router angeschlossen ist, verwenden Sie den Befehl **zur automatischen** Konfiguration der **Discovery-**Leitung.
2. Wenn das Modem erfolgreich erkannt wurde, konfigurieren Sie das Modem automatisch mithilfe des **Konfigurationsbefehls Modemname-**Modemname.

Wenn Sie die Liste der Modems anzeigen möchten, für die der Router Einträge hat, verwenden Sie den Befehl **modemcap *Modemname*.** Wenn Sie einen Modemwert ändern möchten, der über den Befehl **show modemcap** zurückgegeben wurde, verwenden Sie den Befehl **modemcap Edit *modem name attribute value* line configuration (Modemcap bearbeiten-*Attributwert*)**.

Vollständige Informationen zur Verwendung dieser Befehle finden Sie im Konfigurationshandbuch zu *Cisco IOS-Dokumentationen für Wählösungen und in der Befehlsreferenz für Wählösungen*.

Hinweis: Geben Sie *nicht* **&W** im modemcap-Eintrag ein, der für die automatische Konfiguration verwendet wird. Dies bewirkt, dass der NVRAM jedes Mal neu geschrieben wird, wenn ein Modem automatisch konfiguriert wird, und zerstört das Modem.

Einrichten einer umgekehrten Telnet-Sitzung zu einem Modem

Für Diagnosezwecke oder zur Erstkonfiguration des Modems, wenn Sie Cisco IOS Release 11.0

oder früher verwenden, müssen Sie eine umgekehrte Telnet-Sitzung einrichten, um ein Modem für die Kommunikation mit einem Cisco Gerät zu konfigurieren. Solange Sie die Modemgeschwindigkeit auf der Seite des Datenendgeräts (DTE) sperren, kommuniziert das Modem immer mit dem Zugangsserver oder -router mit der gewünschten Geschwindigkeit. In Tabelle 16-5 finden Sie Informationen zum Sperren der Modemgeschwindigkeit. Stellen Sie sicher, dass die Geschwindigkeit des Cisco Geräts konfiguriert ist, bevor Sie Befehle an das Modem über eine umgekehrte Telnet-Sitzung senden. In Tabelle 16-5 finden Sie weitere Informationen zum Konfigurieren der Geschwindigkeit des Zugangs-Servers oder -Routers.

Um das Modem für eine umgekehrte Telnet-Sitzung zu konfigurieren, verwenden Sie den Befehl line configuration **transport input telnet**. Zum Einrichten einer Rotationsgruppe (in diesem Fall auf Port 1) geben Sie den Befehl **rotal 1** für die Leitungskonfiguration ein. Wenn diese Befehle unter die Leitungskonfiguration gestellt werden, weist IOS IP-Listener für eingehende Verbindungen in Port-Bereichen zu, beginnend mit den folgenden Basisnummern:

2000	Telnet-Protokoll
3000	Telnet-Protokoll mit Rating
4000	Raw-TCP-Protokoll
5000	Rohes TCP-Protokoll mit rotierendem
6000	Telnet-Protokoll, binärer Modus
7000	Telnet-Protokoll, binärer Modus mit rotierendem
9000	Xremote-Protokoll
10.000	XRemote-Protokoll mit rotierendem

So starten Sie eine umgekehrte Telnet-Sitzung mit Ihrem Modem:

1. Verwenden Sie von Ihrem Terminal aus den Befehl **telnet ip-address 20yy**, wobei *ip address die IP-Adresse einer beliebigen aktiven, verbundenen Schnittstelle auf dem Cisco Gerät ist und yy die Leitungsnummer, mit der das Modem verbunden ist.*Der folgende Befehl würde Sie beispielsweise mit dem AUX-Port eines Cisco 2501-Routers mit der IP-Adresse 192.169.53.52 verbinden: **192.169.53.52 2001**. Im Allgemeinen kann ein derartiger Telnet-Befehl von jedem beliebigen Ort im Netzwerk aus ausgegeben werden, wenn er **einen Ping an** die betreffende IP-Adresse senden kann.**Hinweis:** Auf den meisten Cisco Routern ist Port 01 der AUX-Port. Auf einem Cisco Access-Server ist der AUX-Port der letzte TTY +1. Beispielsweise ist der AUX-Port eines 2511 Port 17 (16 TTY-Ports + 1). Verwenden Sie immer den Befehl **show line** exec, um nach der Anschlussnummer zu suchen. Dies gilt insbesondere für die Serien 2600 und 3600, die nicht zusammenhängende Portnummern für unterschiedliche async Modulgrößen verwenden.
2. Wenn die Verbindung verweigert wird, kann dies darauf hinweisen, dass entweder kein Listener an der angegebenen Adresse und dem angegebenen Port vorhanden ist oder dass jemand bereits mit diesem Port verbunden ist. Überprüfen Sie die Anschlussadresse und die Portnummer. Stellen Sie außerdem sicher, dass das **Modem** oder **Modem DTR-active** sowie **die Transport-Eingabe alle** unter der Leitungskonfiguration für die erreichbaren Leitungen angezeigt werden.Wenn Sie die Drehfunktion verwenden, stellen Sie sicher, dass der Befehl *rotal n* ***auch in der Leitungskonfiguration angezeigt wird, wobei n die Nummer der Drehgruppe ist.*** Um zu überprüfen, ob jemand bereits verbunden ist, führen Sie Telnet zum Router aus, und verwenden Sie den Befehl **show line *n*.** Achten Sie auf ein Sternchen, das

angibt, dass die Leitung verwendet wird. Stellen Sie sicher, dass der CTS hoch ist und der DSR nicht. Verwenden Sie den Befehl **clear line *n*, um die Verbindung zur aktuellen Sitzung an Port-Nummer n zu trennen.** Wenn die Verbindung immer noch verweigert wird, bestätigt das Modem möglicherweise die Carrier Detect (CD)-ROM (Carrier Detect) ständig. Trennen Sie das Modem von der Leitung, richten Sie eine umgekehrte Telnet-Sitzung ein, und schließen Sie dann das Modem an.

3. Geben Sie nach erfolgreicher Herstellung der Telnet-Verbindung AT ein, und vergewissern Sie sich, dass das Modem mit OK antwortet.
4. Wenn das Modem nicht reagiert, lesen Sie die folgende Tabelle.

In Tabelle 16-1 werden mögliche Ursachen für Modem-to-Router-Verbindungsprobleme aufgeführt und Lösungen für diese Probleme beschrieben.

Tabelle 16-1: Keine Verbindung zwischen Modem und Router

Mögliche Ursachen	Empfohlene Aktionen

Die Modemsteuerung ist auf dem Zugriffsserver oder Router nicht aktiviert.	1. Verwenden Sie den Befehl **show line** exec auf dem Zugriffsserver oder Router. Die Ausgabe für den AUX-Port sollte **InOut** oder **RlisCD** in der Spalte Modem anzeigen. Dies zeigt an, dass die Modemsteuerung auf der Leitung des Zugangs-Servers oder -Routers aktiviert ist. Eine Erklärung zur **Ausgabe** der **Befehlszeile** finden Sie in Kapitel 15 unter "Verwenden von Debug-Befehlen".
	2. Konfigurieren Sie die Leitung für die Modemsteuerung mithilfe des Konfigurationsbefehls **Modem** für die **Inout-**Leitung. Die Modemsteuerung ist jetzt auf dem Zugriffsserver aktiviert.
	Beispiel: Im folgenden Beispiel wird veranschaulicht, wie eine Leitung für eingehende und ausgehende Anrufe konfiguriert wird:
	`line 5`
	`modem inout`
	Hinweis: Stellen Sie sicher, dass Sie den Befehl **Modem** Inout und nicht den Befehl **Modem Dialin** verwenden, während die Verbindung des Modems in Frage steht. Mit diesem Befehl kann die Leitung nur eingehende Anrufe annehmen. Ausgehende Anrufe werden abgelehnt, und es ist nicht möglich, eine Telnet-Sitzung mit dem Modem einzurichten, um sie zu konfigurieren. Wenn Sie den Befehl **Modem Dialin** verwenden möchten, müssen Sie dies erst tun, wenn Sie sicher sind, dass das Modem richtig funktioniert.

Das Modem kann falsch konfiguriert sein oder eine Sitzung ohne Unterbrechung aufgeben.	Geben Sie **AT&FE1Q0 ein**, um die Werkseinstellungen wiederherzustellen und sicherzustellen, dass das Modem auf Echo-Zeichen festgelegt ist und die Ausgabe zurückgibt. Möglicherweise ist die Sitzung des Modems hängen geblieben. Verwenden Sie "**^U**", um die Zeile zu löschen, und "**^Q**", um die Flusssteuerung (XON) zu öffnen. Überprüfen der Paritätseinstellungen
Falsche Verkabelung	1. Überprüfen Sie die Verkabelung zwischen dem Modem und dem Zugriffsserver oder -Router. Bestätigen Sie, dass das Modem über ein gerolltes RJ-45-Kabel und einen MMOD DB-25-Adapter mit dem AUX-Port des Zugangs-Servers oder -Routers verbunden ist. Diese Verkabelungskonfiguration wird von Cisco für RJ-45-Ports empfohlen und unterstützt. (Diese Anschlüsse sind in der Regel mit "Modem" beschriftet.) 2. Überprüfen Sie mit dem Befehl **show line exec**, ob die Kabel korrekt sind. In Kapitel 15 finden Sie eine Erläuterung der Befehlsausgabe der **show line** im Abschnitt "Verwenden von Debug-Befehlen".
Hardware problem	1. Stellen Sie sicher, dass Sie die richtige Verkabelung verwenden und dass alle Verbindungen funktionieren. 2. Überprüfen Sie die gesamte Hardware auf Beschädigungen, z. B. Kabel (unterbrochene Drähte), Adapter (lose Stifte), Zugangs-Server-Ports und Modem. 3. Siehe Kapitel 3, "Fehlerbehebung bei Hardware- und Startproblemen" für weitere Informationen zur Hardware-Fehlerbehebung.

Verwendung von Rotary-Gruppen

Bei einigen Anwendungen müssen die Modems auf einem bestimmten Router von einer Benutzergruppe gemeinsam genutzt werden. Das Cisco Dialout-Dienstprogramm ist ein Beispiel für diese Art von Anwendung. Grundsätzlich stellen Benutzer eine Verbindung zu einem Port her, der sie mit einem verfügbaren Modem verbindet. Um eine async-Linie zu einer Rotationsgruppe

hinzuzufügen, geben Sie einfach **rotierend *n ein*,** wobei **n die Nummer der** Rotationsgruppe in der Konfiguration der asynchronen Leitung ist. Siehe nachstehendes Beispiel.

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

Die obige Leitungskonfiguration würde es Benutzern ermöglichen, eine Verbindung zur Rotationsgruppe herzustellen, indem sie **Telnet 192.169.53.52 3001** für ein normales Telnet eingeben. Alternativ sind die Ports 5001 für Raw TCP, 7001 für binäres Telnet (das vom Cisco Dialout-Dienstprogramm verwendet wird) und 10001 für Xremote-Verbindungen verfügbar.

Hinweis: Um die Konfiguration des Cisco Dialout-Dienstprogramms zu überprüfen, doppelklicken Sie auf das Symbol des Wählprogramms unten rechts im Bildschirm, und drücken Sie die Taste More (Mehr). Drücken Sie anschließend die Schaltfläche Configure Ports (Ports konfigurieren). Stellen Sie sicher, dass sich der Port im 7000-Bereich befindet, wenn Sie rotierende Gruppen verwenden, und im 6000-Bereich, wenn das Dialout-Dienstprogramm ein einzelnes Modem anvisiert. Sie sollten auch die Modemprotokollierung auf dem PC aktivieren. Wählen Sie dazu die folgende Sequenz aus: **Start ->Systemsteuerung-> Modems->**(wählen Sie Ihr Cisco Dialout-Modem aus)**->Eigenschaften->Verbindung->**Erweitert...**->Protokolldatei aufzeichnen**.

Anzeigen der Zeilenausgabe

Die Ausgabe des **Befehls show line *line-number* exec** ist bei der Fehlerbehebung einer Modem-to-Access-Server- oder -Router-Verbindung nützlich. Unten sehen Sie die Ausgabe des Befehls **show line**.

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

Line 1, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits
Status: No Exit Banner
Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
Modem state: Hanging up
  modem(slot/port)=1/0, state=IDLE
  dsx1(slot/unit/channel)=NONE, status=VDEV_STATUS_UNLOCKED
Group codes:    0
Modem hardware state: CTS noDSR  noDTR RTS
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
                ^^x    none   -     -       none
Timeouts:      Idle EXEC    Idle Session   Modem Answer  Session   Dispatch
               00:10:00        never                      none     not set
                            Idle Session Disconnect Warning
                              never
                            Login-sequence User Response
                             00:00:30
                            Autoselect Initial Wait
                              not set
Modem type is unknown.
Session limit is not set.
```

```
Time since activation: never
Editing is enabled.
History is enabled, history size is 10.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed transports are lat pad telnet rlogin udptn v120 lapb-ta.
Preferred is l
at pad telnet rlogin udptn v120 lapb-ta.
No output characters are padded
No special data dispatching characters
as5200-1#
```

Wenn Verbindungsprobleme auftreten, wird eine wichtige Ausgabe im Modemstatus und in den Feldern für den Hardwarestatus des Modems angezeigt.

Hinweis: Das Feld "Modem Hardware state" (Modem-Hardwarestatus) wird nicht in der Ausgabe der **angezeigten Zeile** für jede Plattform angezeigt. In einigen Fällen werden stattdessen die Anzeichen für Signalzustände im Feld Modem State (Modemstatus) angezeigt.

In Tabelle 16-2 sind die typischen Modem-Status- und Modem-Hardwarestatuszeichenfolgen aus der Ausgabe des Befehls **show line** aufgeführt. Es erklärt auch die Bedeutung der einzelnen Staaten.

Tabelle 16-2: Modem- und Modem-Hardware-Status in der Zeilenausgabe

Modemstatus	Status der Modemhardware	Bedeutung
Inaktivität	CTS noDSR DTR RTS	Dies sind die richtigen Modemzustände für Verbindungen zwischen einem Zugriffsserver oder -router und einem Modem (wenn kein eingehender Anruf eingeht). Eine andere Ausgabe weist im Allgemeinen auf ein Problem hin.
Bereit	-	Wenn der Modemstatus Ready (Bereit) statt Idle (Inaktiv) lautet, sollten Sie Folgendes berücksichtigen: 1. Die Modemsteuerung ist auf dem Zugriffsserver oder Router nicht konfiguriert. Konfigurieren Sie den Access-Server oder den Access-Router mit dem Konfigurationsbefehl **Modem** für die **Inout**-Leitung. 2. In der Zeile ist eine Sitzung vorhanden. Verwenden Sie den Befehl **show users** exec, und verwenden Sie den Befehl **clear line** privilegierten exec, um die Sitzung bei Bedarf zu beenden.

		3. Der DSR ist hoch. Dafür gibt es zwei mögliche Gründe: Kabelprobleme. Wenn Ihr Steckverbinder den DB-25-Pin 6 verwendet und keinen Pin 8 hat, müssen Sie den Pin von 6 auf 8 verschieben, oder Sie müssen den entsprechenden Anschluss erhalten.Das für DCD konfigurierte Modem ist immer hoch. Das Modem sollte so umkonfiguriert werden, dass DCDs nur auf einer CD(1) hoch sind. Dies erfolgt in der Regel über den Befehl **&C1**-Modem. Überprüfen Sie jedoch in der Modemdokumentation die genaue Syntax für Ihr Modem. Wenn Ihre Software die Modemsteuerung nicht unterstützt, müssen Sie die Zugriffsserver-Leitung konfigurieren, mit der das Modem verbunden ist, indem Sie den Befehl **no exec** line configuration eingeben. Löschen Sie die Leitung mit dem Befehl **clear line** privileged exec, starten Sie eine umgekehrte Telnet-Sitzung mit dem Modem, und konfigurieren Sie das Modem so neu, dass DCD nur auf CD hoch ist. Beenden Sie die Telnet-Sitzung, indem Sie **disconnect** eingeben und die Zugriffsserver-Leitung mit dem exec-Leitungskonfigurationsbefehl neu konfigurieren.
Bereit	noCTS noDSR DTR RTS(2)	Die Zeichenfolge noCTS wird aus einem der folgenden vier Gründe im Feld "Modem Hardware state" angezeigt: 1. Das Modem ist ausgeschaltet. 2. Das Modem ist nicht ordnungsgemäß mit dem Zugriffsserver verbunden. Überprüfen Sie die Kabelverbindungen vom Modem zum Zugriffsserver.

		3. Falsche Verkabelung (entweder gerollter MDCE oder gerader MDTE, aber ohne die Stifte verschoben). Die empfohlene Verkabelungskonfiguration ist weiter oben in dieser Tabelle aufgeführt. 4. Das Modem ist nicht für die Hardware-Flusssteuerung konfiguriert. Deaktivieren Sie mit dem Befehl **no flow control hardware** line configuration die Hardware Flow Control (Hardware-Flusssteuerung) auf dem Zugriffsserver. Aktivieren Sie dann die Hardware-Flusssteuerung am Modem über eine umgekehrte Telnet-Sitzung. (Lesen Sie die Modemdokumentation, und lesen Sie den Abschnitt "Einrichten einer Telnet-Reverse-Sitzung mit einem Modem" weiter oben in diesem Kapitel.) Aktivieren Sie die Hardware-Flusssteuerung auf dem Zugriffsserver mithilfe des Befehls für die Leitungskonfiguration der **Flusssteuerung erneut**.
Bereit	CTS DSR DTR RTS(2)	Die DSR-Zeichenfolge (anstelle der noDSR-Zeichenfolge) wird im Feld Modem Hardware state (Modem-Hardwarestatus) aus einem der folgenden Gründe angezeigt: 1. Falsche Verkabelung (entweder gerollter MDCE oder gerader MDTE, aber ohne die Stifte verschoben). Die empfohlene Verkabelungskonfiguration ist weiter oben in dieser Tabelle aufgeführt. 2. Das Modem ist für DCD immer hoch konfiguriert. Konfigurieren Sie das Modem so neu, dass die DCD nur hoch auf der CD ist. Dies erfolgt in der Regel über den Befehl **&C1**-Modem. Überprüfen

		Sie jedoch in der Modemdokumentation die genaue Syntax für Ihr Modem. Konfigurieren Sie die Zugriffsserver-Leitung, mit der das Modem verbunden ist, mithilfe des Konfigurationsbefehls **no exec** line. Löschen Sie die Leitung mit dem Befehl **clear line** privileged exec, starten Sie eine umgekehrte Telnet-Sitzung mit dem Modem, und konfigurieren Sie das Modem so neu, dass DCD nur auf CD hoch ist. Beenden Sie die Telnet-Sitzung, indem Sie **disconnect** eingeben. Konfigurieren Sie die Zugriffsserver-Leitung mit dem Konfigurationsbefehl exec line neu.
Bereit	CTS* DSR* DTR RTS(2)	Wenn diese Zeichenfolge im Feld "Modem Hardware state" (Modem-Hardwarestatus) angezeigt wird, ist die Modemsteuerung wahrscheinlich nicht auf dem Zugriffsserver aktiviert. Verwenden Sie den Befehl **Modem Inout** Line Configuration (Modemkonfiguration in der Leitung), um die Modemsteuerung in der Leitung zu aktivieren. Weitere Informationen zum Konfigurieren der Modemsteuerung auf einem Zugriffsserver oder einer Router-Leitung finden Sie weiter oben in dieser Tabelle.

(1) CD = Carrier Detection

(2) Ein * neben einem Signal gibt eines von zwei Dingen an: Das Signal hat sich in den letzten Sekunden geändert, oder das Signal wird von der ausgewählten Modemsteuermethode nicht verwendet.

Sammeln von Informationen zur Modemleistung

In diesem Abschnitt werden die Methoden zum Sammeln von Leistungsdaten für die digitalen MICA-Modems der Cisco AS5x00-Familie von Zugriffsservern beschrieben. Die Leistungsdaten können für Trendanalysen verwendet werden und sind nützlich bei der Behebung von Leistungsproblemen, die auftreten können. Wenn Sie sich die unten aufgeführten Zahlen anschauen, denken Sie daran, dass Perfektion in der realen Welt nicht möglich ist. Die mögliche Erfolgsrate von Modemanrufen (CSR) hängt von der Qualität der Leitungen, der Benutzerbasis des Client-Modems und den verwendeten Modulationen ab. Ein typischer CSR-Prozentsatz für

V.34-Anrufe liegt bei 95 %. Es ist zu erwarten, dass V.90-Anrufe 92 % der Zeit erfolgreich verbunden werden. In 10 % der Fälle treten vorzeitige Tropfen auf.

Verwenden Sie die folgenden Befehle, um eine Gesamtübersicht über das Modemverhalten auf dem Zugriffsserver zu erhalten:

- **Show-Modem**
- **Modemübersicht anzeigen**
- **Anzeigen der Modem-Verbindungsgeschwindigkeiten**
- **Anrufstatus des Modems anzeigen**

Die folgenden Informationen sind bei der Fehlerbehebung einer einzelnen Modemverbindung oder beim Erfassen von Daten für Trendanalysen hilfreich:

- Debug-Modem csm
- Modem Call Record Terse
- show modem op (MICA) / AT@E1 (Microcom) bei Verbindung
- Anzeige des Modemprotokolls für die Sitzung nach dem Trennen der Verbindung
- ANI (Anrufernummer)
- Tageszeit
- Client-Modem-Hardware/Firmware-Version
- Interessante Informationen vom Client (nach Trennung)-ATI6, ATI11, AT&V, AT&V1 usw.
- Ein Audiodatensatz (WAV-Datei) für den Ausbilder des Client-Modems

In den folgenden Abschnitten werden die Befehle weiter erläutert. Außerdem werden einige allgemeine Trends besprochen.

Modem anzeigen/Modemzusammenfassung anzeigen

Der Befehl **show modem** gibt einen Überblick über die einzelnen Modems. Anhand dieser Zahlen kann der Zustand der einzelnen Modems angezeigt werden.

```
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%
```

Verwenden Sie den Befehl **show modem summary** (**Modemübersicht anzeigen**), um die

aggregierten Nummern aller Modems auf dem Router anzuzeigen.

```
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%
```

Tabelle 16-3: Modemfelder anzeigen

Felder	Beschreibungen
Eingehende und ausgehende Anrufe	Anrufe, die in das Modem eingehen oder es verlassen. • Nutzung - Prozentsatz der Gesamtbetriebszeit des Systems, die alle Modems in Betrieb sind. • Succ - Gesamtanzahl erfolgreich verbundener Anrufe. • Fail (Fehlgeschlagen): Gesamtzahl der Anrufe, die nicht erfolgreich verbunden wurden. • Avail - Gesamtanzahl an Modems, die im System verwendet werden können.
Ausgebügelt	Gesamtzahl der Male, die die Modems mit dem Befehl **Modem Besetzt** oder dem Befehl **Modem Shutdown** außer Betrieb genommen wurden.
Fehlgeschlagenes Wählen	Gesamtanzahl der Versuche, die Modems nicht aufgelegt haben oder kein Wählton ausgegeben wurde.
Keine Ans	Die Gesamtzahl der klingelnden Anrufe wurde erkannt, aber die Anrufe wurden von einem Modem nicht beantwortet.
Ein solcher PC.	Prozentsatz erfolgreicher Verbindungen der insgesamt verfügbaren Modems

[Ausgabe von Modem-Anrufstationen anzeigen]

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

Tabelle 16-4: Anzeigen von Modem-Anrufstatusfeldern

Rmt Link	Dies zeigt, dass eine Fehlerkorrektur wirksam war und der Anruf vom Client-System aufgelegt wurde, das an das Remote-Modem angeschlossen war.

HostDrop	Dies zeigt, dass der Anruf vom IOS-Hostsystem aufgelegt wurde. Einige häufige Gründe sind: Timeout bei Inaktivität, freie Leitung beim Telefonunternehmen oder PPP-LCP-Terminologie beim Client. Der Grund für das Auflegen lässt sich am besten durch die Verwendung von Terminen mit Modem-Anrufaufzeichnungen oder AAA-Abrechnung ermitteln.

Die anderen Trennungsgründe sollten weniger als 10 % der Gesamtsumme ausmachen.

Ausgabe der Modem Connect-Geschwindigkeiten anzeigen

```
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
```

Es wird eine Verteilung der V.34-Geschwindigkeiten erwartet. Wenn die T1 Channel Associated Signaling (CAS) verwenden, sollte ein Peak von 26,4 vorliegen. Bei ISDN (PRI) T1 muss der Peak bei 31,2 liegen. Achten Sie auch auf einige K56Flex-, V.90-Geschwindigkeiten. Wenn keine V.90-Verbindungen vorhanden sind, kann es zu einem Netzwerktopologieproblem kommen.

Befehl "Understanding the Modem Call-Record Terse (11.3AA/12.0T)"

Statt eines exec-Befehls handelt es sich um einen Konfigurationsbefehl, der auf der Systemebene des betreffenden Zugriffsservers platziert wird. Wenn ein Benutzer die Verbindung trennt, wird eine Meldung wie die folgende angezeigt:

```
*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
```

Befehl "Modem Operational Status" anzeigen

Der Befehl exec **show modem Operational Status** (**Modembetrieb anzeigen)** zeigt die aktuellen (oder aktuellsten) Parameter für die Modemverbindung an.

Der Dokumentationseintrag für diesen Befehl finden Sie in der Befehlsreferenz zu *Cisco IOS Release 12.0 Dial Solutions*. **show modem operations status** is only for MICA modems. Der entsprechende Befehl für Microcom-Modems lautet **Modem at-Mode / AT@E1**. Verwenden Sie den Befehl **Modem at-Mode <slot>/<port>**, um eine Verbindung zum Modem herzustellen, und

geben Sie dann den Befehl **AT@E1** aus. Die vollständige Dokumentation des Befehls **Modem at-Mode** finden Sie im *Cisco AS5300 Software Configuration Guide*, und die Dokumentation zum Befehl **AT@E1** finden Sie im *AT-Befehlssatz und in der Registerübersicht für Microsoft Modem Modules-Befehlsreferenz*.

Bestimmen Sie anhand der folgenden Schritte, welches Modem ein Benutzer einsetzt:

1. Geben Sie den Befehl **show user (Benutzer anzeigen)** ein, und suchen Sie nach dem TTY, mit dem sie verbunden sind.
2. Verwenden Sie den Befehl **show line** und suchen Sie nach den Steckplatz-/Portnummern des Modems.

Erfassen von clientseitigen Leistungsdaten

Für Trendanalysen ist es sehr wichtig, clientseitige Leistungsdaten zu erfassen. Versuchen Sie immer, die folgenden Informationen zu erhalten:

- Client-Hardwaremodell/Firmware-Version (erreichbar mit dem Befehl **ATI3I7** auf dem Client-Modem)
- vom Client gemeldete Trennungsgründe (**ATI6** oder **AT&V1**)

Weitere Informationen, die auf dem Client-Ende verfügbar sind, sind die PCs modemlog.txt und ppplog.txt. Sie müssen Ihren PC speziell konfigurieren, um diese Dateien zu generieren.

Analysieren der Leistungsdaten

Nachdem Sie die Leistungsdaten für das Modemsystem erfasst und verstanden haben, müssen Sie sich die verbleibenden Muster und Komponenten ansehen, die möglicherweise verbessert werden müssen.

Probleme mit bestimmten Servermodems

Verwenden Sie **show modem** oder **show modem call stats**, um Modems mit einer ungewöhnlich hohen Rate an Ausübungsfehlern oder schlechten Verbindungsraten (MICA) zu identifizieren. Wenn benachbarte Modempaare Probleme haben, liegt das Problem wahrscheinlich in einem nicht mehr reagierenden/ausgefallenen DSP. Verwenden Sie **Flash-Modem** zum betroffenen HMM, um die Wiederherstellung durchzuführen. Stellen Sie sicher, dass auf den Modems die aktuellste Version von Portware ausgeführt wird. Um zu überprüfen, ob alle Modems korrekt konfiguriert sind, verwenden Sie den Konfigurationsbefehl **Modem auto configure type mica/microcom_server** in der Leitungskonfiguration. Um sicherzustellen, dass die Modems automatisch konfiguriert werden, wenn ein Anruf aufgelegt wird, verwenden Sie den Befehl **debug config**. Um Modems zu beheben, die stark falsch konfiguriert sind, müssen Sie möglicherweise eine umgekehrte Telnet-Sitzung einrichten.

Probleme mit bestimmten DS0s

DS0-Probleme sind selten, aber möglich. Um defekte DS0s zu finden, verwenden Sie den Befehl **show controller t1 call counter** und suchen Sie nach DS0s mit ungewöhnlich hohen TotalCalls und ungewöhnlich niedriger TotalDuration. Um DS0s zu finden, die im Verdacht stehen, müssen Sie möglicherweise andere DS0s mit dem Konfigurationsbefehl **isdn service dsl, ds0 busyout** unter der seriellen Schnittstelle für die T1 ausfüllen. Die Ausgabe der **Anrufzähler show controller t1** sieht

wie folgt aus:

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

Natürlich ist Timeslot 3 in diesem Fall der verdächtige Kanal.

Weitere häufige Trends

Im Folgenden finden Sie einige der häufigsten Trends, die das Cisco TAC verzeichnet.

1. Falsche LeitungspfadeWenn folgende Probleme auftreten, erhalten Sie möglicherweise schlechte Pfade über das öffentliche Telefonnetz (PSTN):Ferngespräche haben Probleme, aber lokal nicht (oder umgekehrt)Anrufe zu bestimmten Tageszeiten haben ProblemeAnrufe von bestimmten Remote-Austauschen sind problematisch
2. Probleme mit FerngesprächenWenn Ihr Ferngespräch nicht ordnungsgemäß oder überhaupt nicht funktioniert (aber der lokale Service ist in Ordnung):Stellen Sie sicher, dass die digitale Leitung mit einem digitalen Switch und nicht mit einer Kanalbank verbunden ist.Weisen Sie die Telefongesellschaften an, die für Ferngespräche verwendeten Leitungen zu prüfen.
3. Probleme mit Anrufen aus bestimmten Anrufsbereichen.Wenn Anrufe aus bestimmten geografischen Regionen/Börsen Probleme haben, sollten Sie die Netzwerktopologie von der Telefongesellschaft beziehen.Wenn mehrere analoge/digitale Konvertierungen erforderlich sind, sind V.90/K56flex-Modemverbindungen nicht möglich, und V.34 ist möglicherweise etwas abgebaut. In Bereichen, die von nicht integrierten Digitalschaltern oder von analogen Switches bedient werden, sind Analog-Digital-Konvertierungen erforderlich.

ISDN-Betrieb

ISDN bezieht sich auf eine Reihe digitaler Dienste, die Endbenutzern zur Verfügung stehen. ISDN umfasst die Digitalisierung des Telefonnetzes, sodass Endbenutzer von einem einzigen Endbenutzer-Terminal aus über ein vorhandenes Telefonkabel Sprach-, Daten-, Text-, Grafik-, Musik-, Video- und andere Ausgangsmaterialien erhalten können. Die Befürworter von ISDN stellen sich ein weltweites Netz vor, das dem heutigen Telefonnetz ähnelt, aber mit digitaler Übertragung und einer Vielzahl neuer Dienste.

ISDN ist ein Ansatz zur Standardisierung von Teilnehmerdiensten, Benutzer-/Netzwerkschnittstellen sowie Netzwerk- und Internetfunktionen. Durch die Standardisierung von Teilnehmerdiensten wird versucht, ein bestimmtes Maß an internationaler Kompatibilität sicherzustellen. Die Standardisierung der Benutzer-/Netzwerkschnittstelle fördert die Entwicklung und Vermarktung dieser Schnittstellen durch Dritthersteller. Die Standardisierung von Netzwerk- und Internetfunktionen trägt dazu bei, das Ziel einer weltweiten Anbindung zu erreichen, indem die einfache Kommunikation zwischen ISDN-Netzwerken sichergestellt wird.

ISDN-Anwendungen umfassen Hochgeschwindigkeits-Bildanwendungen (z. B. Telefonnetze der Gruppe IV), zusätzliche Telefonleitungen für Heimnetzwerke, Hochgeschwindigkeits-Dateiübertragung und Videokonferenzen. Die Sprachkommunikation ist natürlich auch eine beliebte Anwendung für ISDN.

Der Markt für den Heimzugang ist auf verschiedene Technologien aufgeteilt. In Bereichen, in denen neuere, kostengünstigere Technologien wie DSL und Kabel verfügbar werden, verlagert sich der heimische Markt weg von ISDN. Unternehmen verwenden jedoch weiterhin ISDN in Form von PRI T1/E1, um große Datenmengen zu übertragen oder v.90-Einwahlzugriff bereitzustellen.

ISDN-Komponenten

Zu den ISDN-Komponenten gehören Terminals, Terminaladapter (TAs), Netzwerkterminierungsgeräte, Line Termination Equipment (Line Termination Equipment, Terminierungsgeräte für den Austausch). ISDN-Terminals sind in zwei Typen erhältlich. Spezialisierte ISDN-Terminals werden als Endgeräte Typ 1 (TE1) bezeichnet. Nicht-ISDN-Terminals wie DTE, die den ISDN-Standards vorgreifen, werden als Endgeräte vom Typ 2 (TE2) bezeichnet. TE1-Verbindungen werden über eine digitale Verbindung mit vier Kabeln und Twisted Pair mit dem ISDN-Netzwerk verbunden. TE2s verbinden sich über einen Terminaladapter mit dem ISDN-Netzwerk. Das ISDN TA kann entweder ein eigenständiges Gerät oder ein Mainboard innerhalb des TE2 sein. Wenn der TE2 als eigenständiges Gerät implementiert wird, wird die Verbindung mit dem TA über eine physische Standardschnittstelle hergestellt. Beispiele hierfür sind EIA/TIA-232-C (ehemals RS-232-C), V.24 und V.35.

Über die TE1- und TE2-Geräte hinaus ist der nächste Verbindungspunkt im ISDN-Netzwerk das Gerät für die Netzwerkterminierung vom Typ 1 (NT1) oder den Netzwerkterminierungstyp 2 (NT2). Hierbei handelt es sich um Netzwerkterminierungsgeräte, die die vieradrigen Subscriber-Kabel mit der konventionellen Zweidrahtleitung verbinden. In Nordamerika ist das NT1 ein Gerät für Kundenstandorte (Customer Premises Equipment, CPE). In den meisten anderen Teilen der Welt ist das NT1 Teil des Netzwerks, das vom Betreiber bereitgestellt wird. Das NT2 ist ein komplizierteres Gerät, das normalerweise in PBX-Systemen (Digital Private Branch Exchange) eingesetzt wird und Protokollfunktionen und Konzentrationsdienste für Layer 2 und 3 ausführt. Ein NT1/2-Gerät ist ebenfalls vorhanden. Es ist ein einzelnes Gerät, das die Funktionen eines NT1 und eines NT2 kombiniert.

Eine Reihe von Referenzpunkten ist in ISDN angegeben. Diese Referenzpunkte definieren logische Schnittstellen zwischen funktionalen Gruppierungen wie TAs und NT1s. ISDN-Referenzpunkte umfassen Folgendes:

- R - Der Referenzpunkt zwischen Nicht-ISDN-Geräten und einem TA
- S-Der Bezugspunkt zwischen Benutzerterminals und NT2
- T-Der Bezugspunkt zwischen NT1- und NT2-Geräten
- U - Der Bezugspunkt zwischen NT1-Geräten und Line Termination Equipment im Carrier-Netzwerk. Der U-Referenzpunkt ist nur in Nordamerika relevant, wo die NT1-Funktion nicht vom Betreibernetzwerk bereitgestellt wird

Im Folgenden sehen Sie eine ISDN-Beispielkonfiguration. Dieses Beispiel zeigt drei Geräte, die an einen ISDN-Switch in der Zentrale angeschlossen sind. Zwei dieser Geräte sind ISDN-kompatibel, sodass sie über einen S-Referenzpunkt an NT2-Geräte angeschlossen werden können. Das dritte Gerät (ein Standard-Nicht-ISDN-Telefon) wird über den R-Referenzpunkt an einen TA angeschlossen. Jedes dieser Geräte kann auch an ein NT1/2-Gerät angeschlossen werden, das sowohl das NT1 als auch das NT2 ersetzen würde. Auch wenn diese nicht angezeigt werden, sind ähnliche Benutzerkonsolen mit dem ISDN-Switch ganz rechts verbunden.

Eine ISDN-Beispielkonfiguration

```
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#
```

ISDN-Services

Der ISDN Basic Rate Interface (BRI)-Dienst bietet zwei B-Kanäle und einen D-Kanal (2B+D). Der BRI-B-Channel-Service arbeitet mit 64 Kbit/s und ist für die Übertragung von Benutzerdaten vorgesehen. Der BRI D-Channel-Service arbeitet mit 16 Kbit/s und dient zur Übertragung von Steuerungs- und Signalisierungsinformationen, kann jedoch unter bestimmten Umständen die Übertragung von Benutzerdaten unterstützen. Das D-Channel-Signalisierungsprotokoll umfasst die Layer 1 bis 3 des OSI-Referenzmodells. BRI bietet außerdem eine Steuerung des Framings und andere Overhead und erhöht damit die Bitrate auf insgesamt 192 Kbit/s. Die Spezifikation der physischen BRI-Schicht lautet International Telecommunication Union Telecommunication Standardization Sector (ITU-T). ehemals Beratender Ausschuss für internationale Telegraf- und Telefondienste (CCITT) I.430.

Der ISDN Primary Rate Interface (PRI)-Service bietet 23 B-Kanäle und einen D-Kanal in Nordamerika und Japan mit einer Bitrate von insgesamt 1,544 Mbit/s (der PRI D-Kanal läuft mit 64 Kbit/s). ISDN PRI in Europa, Australien und anderen Teilen der Welt bietet 30 B plus einen 64-Kbit/s-D-Kanal und eine Gesamtschnittstellenrate von 2,048 Mbit/s. Die Spezifikation der physischen PRI-Schicht lautet ITU-T I.431.

Layer 1

Die Frame-Formate der ISDN-Ebene (Layer 1) unterscheiden sich je nachdem, ob der Frame ausgeht (von Terminal zu Netzwerk) oder ein eingehender (von Netzwerk zu Terminal). Beide physischen Layer-Schnittstellen sind in Abbildung 16-1 dargestellt.

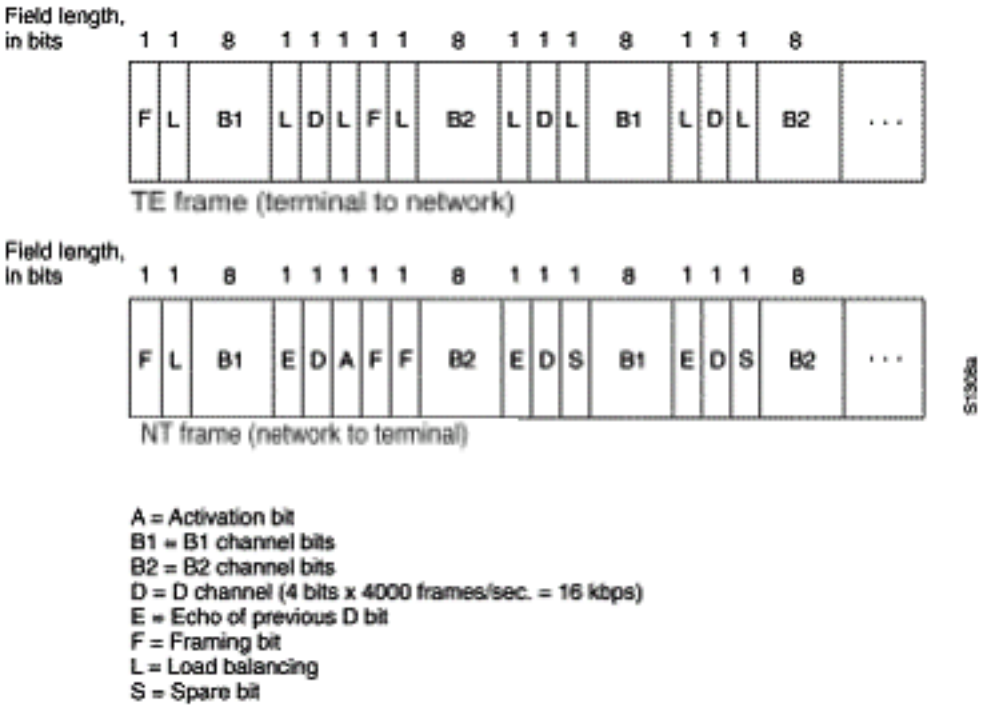

Abbildung 16-1: ISDN Physical-Layer Frame-Formate

Die Frames sind 48 Bit lang, wovon 36 Bit Daten darstellen. Die Bits eines physischen ISDN-Layer-Frames werden wie folgt verwendet:

- F - Stellt die Synchronisierung bereit.
- L - Passt den durchschnittlichen Bitwert an.
- E - Wird für die Beilegung von Streitigkeiten verwendet, wenn mehrere Terminals auf einem passiven Bus um einen Kanal konkurrieren.
- A - Aktiviert Geräte.
- S - Nicht zugewiesen.
- B1, B2 und D - Für Benutzerdaten.

Mehrere ISDN-Benutzergeräte können physisch an einen Stromkreis angeschlossen werden. Bei dieser Konfiguration können Kollisionen auftreten, wenn zwei Terminals gleichzeitig übertragen werden. Aus diesem Grund stellt ISDN Funktionen bereit, um den Konflikt zwischen den Verbindungen zu bestimmen. Wenn ein NT ein D-Bit von der TE empfängt, wird das Bit in der nächsten E-Bit-Position zurückgegeben. Der TE erwartet, dass das nächste E-Bit mit dem zuletzt übertragenen D-Bit identisch ist.

Terminals können nur dann in den D-Kanal übertragen werden, wenn sie eine bestimmte Anzahl von Terminals erkennen (wobei "kein Signal" angibt), die einer zuvor festgelegten Priorität entspricht. Wenn die TE ein Bit im Echokanal (E) erkennt, das sich von den D-Bits unterscheidet, muss sie die Übertragung sofort beenden. Diese einfache Technik stellt sicher, dass nur ein Terminal seine D-Nachricht gleichzeitig übertragen kann. Nach erfolgreicher D-Nachrichtenübertragung wird die Priorität des Terminals verringert, da vor der Übertragung weitere Nachrichten erkannt werden müssen. Terminals können ihre Priorität erst dann erhöhen, wenn alle anderen Geräte auf derselben Leitung die Möglichkeit hatten, eine D-Nachricht zu senden. Telefonverbindungen haben eine höhere Priorität als alle anderen Dienste, und Signalisierungsinformationen haben eine höhere Priorität als Informationen ohne Signalisierung.

Layer 2

Layer 2 des ISDN-Signalisierungsprotokolls ist Link Access Procedure auf dem D-Kanal, auch als LAPD bezeichnet. LAPD ähnelt High-Level Data Link Control (HDLC) und Link Access Procedure, Balanced (LAPB). Wie die Erweiterung der LAPD-Abkürzung zeigt, wird sie im gesamten D-Kanal verwendet, um sicherzustellen, dass Steuerungs- und Signalisierungsinformationen ordnungsgemäß übertragen und empfangen werden. Das LAPD-Frame-Format (siehe Abbildung 16-2) ähnelt dem von HDLC, und wie bei HDLC verwendet LAPD Überwachungs-, Informations- und nicht nummerierte Frames. Das LAPD-Protokoll ist in ITU-T Q.920 und ITU-T Q.921 formell spezifiziert.

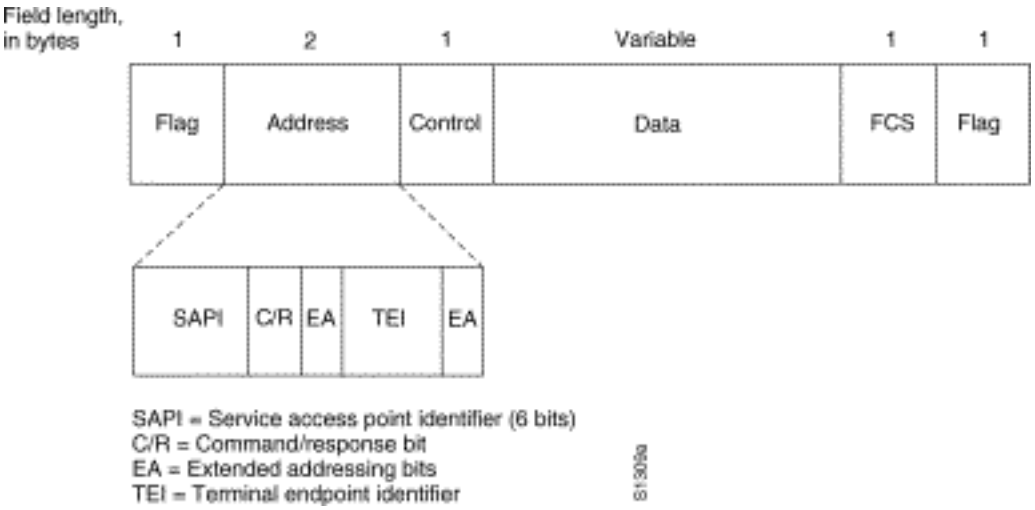

Abbildung 16-2: LAPD Frame-Format

Die Felder LAPD Flag und Control sind identisch mit denen von HDLC. Das Feld "LAPD Address" kann 1 oder 2 Byte lang sein. Wenn das erweiterte Adressbit des ersten Bytes festgelegt ist, beträgt die Adresse 1 Byte. Wenn sie nicht festgelegt ist, beträgt die Adresse 2 Byte. Das erste Adressfeldbyte enthält die Service Access Point Identifier (SAPI), die das Portal kennzeichnet, in dem LAPD-Services für Layer 3 bereitgestellt werden. Das C/R-Bit gibt an, ob der Frame einen Befehl oder eine Antwort enthält. Das TEI-Feld (Terminal Endpoint Identifier) identifiziert entweder ein einzelnes Terminal oder mehrere Terminals. Ein TEI aller deutet auf eine Sendung hin.

Layer 3

Für die ISDN-Signalisierung werden zwei Layer-3-Spezifikationen verwendet: ITU-T (ehemals CCITT) I.450 (auch bekannt als ITU-T Q.930) und ITU-T I.451 (auch bekannt als ITU-T Q.931). Zusammen unterstützen diese Protokolle Benutzer-zu-Benutzer-, leitungsvermittelte und paketvermittelte Verbindungen. Es werden eine Reihe von Anruferfassungen, Anrufbeendigungen,

Informationen und verschiedene Nachrichten angegeben, darunter SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS und DISCONNECT.

Diese Meldungen ähneln funktional denen des X.25-Protokolls (weitere Informationen finden Sie in Kapitel 19, "Fehlerbehebung bei X.25-Verbindungen"). In Abbildung 16-3, ITU-T I.451, sind die typischen Phasen eines ISDN-Leitungs-Switch dargestellt.

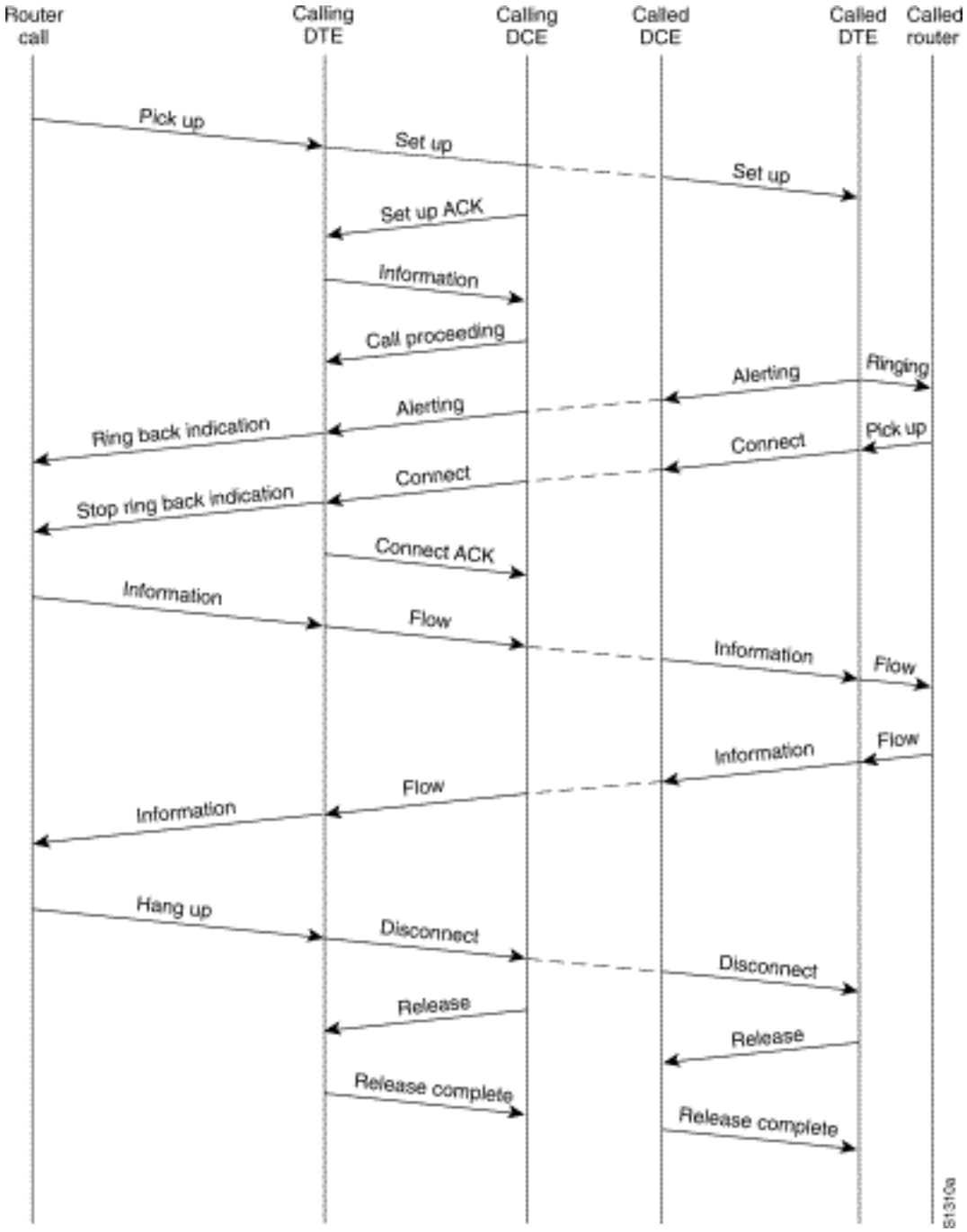

Abbildung 16-3: ISDN-Anrufphasen (Circuit-Switched Call Stages)

Interpretieren der ISDN-Statusausgabe anzeigen

Um herauszufinden, wie sich die aktuelle Situation der ISDN-Verbindung zwischen dem Router und dem Switch der Telefongesellschaft befindet, verwenden Sie den Befehl **show isdn status**. Die beiden Schnittstellentypen, die von diesem Befehl unterstützt werden, sind BRI und 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
```

Tabelle 16-5: - Zeigt den ISDN-Status für BRI an

Feld	Bedeutung
Layer-1-Status: DEAKTIVIERT	Dies bedeutet, dass die BRI-Schnittstelle kein Signal auf der Leitung erkennt. Dafür gibt es fünf mögliche Gründe. • Die BRI-Schnittstelle wird heruntergefahren. Überprüfen Sie entweder die Konfiguration für das **Herunterfahren** des Befehls unter der BRI-Schnittstelle, oder suchen Sie im Befehl **show interface** nach einer administrativ ausgeschalteten Anzeige. Verwenden Sie das Konfigurationsprogramm, und geben Sie **no shutdown** unter der BRI-Schnittstelle ein. Geben Sie den Befehl **clear interface bri** an der Eingabeaufforderung ein, um sicherzustellen, dass die BRI-Schnittstelle neu gestartet wird. • Bei der Verkabelung liegt ein Problem vor. Sie müssen das Kabel austauschen. Verwenden Sie ein Durchgangskabel RJ-45. Halten Sie die RJ-45-Kabelenden nebeneinander, um das Kabel zu prüfen. Wenn die Pins in der gleichen Reihenfolge angeordnet sind, ist das Kabel gerade durchgehend. Wenn die Reihenfolge der Pins umgekehrt ist, wird das Kabel gerollt. Ersetzen Sie das Kabel. • Der ISDN-BRI-Port eines Routers kann ein NT1-Gerät erfordern. In ISDN ist NT1 ein Gerät, das die Schnittstelle zwischen den

	Geräten des Kunden und den Switching-Geräten der Zentrale bereitstellt. Wenn der Router kein internes NT1 hat, rufen Sie einen NT1-Anschluss ab, und verbinden Sie ihn mit dem BRI-Port. Stellen Sie sicher, dass der BRI- oder Terminal-Adapter an den S/T-Port des NT1 angeschlossen ist. Lesen Sie die Dokumentation des Herstellers, um die ordnungsgemäße Funktion des externen NT1 zu überprüfen. • Die Leitung funktioniert möglicherweise nicht. Kontaktieren Sie den Netzbetreiber, um den Betrieb der Verbindung zu bestätigen und die Switch-Typeinstellungen zu überprüfen. • Stellen Sie sicher, dass der Router ordnungsgemäß funktioniert. Wenn fehlerhafte oder defekte Hardware vorhanden ist, ersetzen Sie diese bei Bedarf.

Layer-2-Status: State = TEI_ASSIGNED	Überprüfen Sie die Switchtypeinstellungen und SPIDS. Die Einstellung für den schnittstellenspezifischen ISDN-Switch überschreibt die globale Switch-Einstellung. Der SPID-Status gibt an, ob der Switch den SPIDS akzeptiert hat (gültig oder ungültig). Wenden Sie sich an Ihren Dienstanbieter, um die auf dem Router konfigurierte Einstellung zu überprüfen. Um die SPID-Einstellungen zu ändern, verwenden Sie den **Befehl isdn *spidn* interface configuration.** Wenn *n* ***je nach Kanal entweder 1 oder 2 ist.*** Verwenden Sie die **no**-Form dieses Befehls, um die angegebene SPID zu entfernen.
	`isdn spidn spid-number [ldn]`
	`no isdn spidn spid-number [ldn]`
	Syntaxbeschreibung:
	`spid-number`
	Die Nummer des Dienstes, für den Sie sich angemeldet haben. Dieser Wert wird vom ISDN-Dienstanbieter zugewiesen und ist in der Regel eine zehnstellige Telefonnummer mit zusätzlichen Ziffern.
	`ldn`
	(Optional) Local directory number (LDN), eine 7-stellige Nummer, die vom Service Provider zugewiesen wird. Der Switch in der eingehenden Setup-Meldung liefert diese Informationen. Wenn Sie das lokale Verzeichnis nicht angeben, ist der Zugriff auf den Switch

	zulässig, der andere B-Kanal kann jedoch möglicherweise keine eingehenden Anrufe empfangen. Um die Layer-2-Verhandlungen zwischen Switch und Router anzuzeigen, verwenden Sie den privilegierten exec-Befehl **debug isdn q921**. Die q921-Debuggen werden in der *Debug-Befehlsreferenz* dokumentiert. Debugger sind in hohem Maße von CPU-Ressourcen abhängig. Daher ist bei der Verwendung dieser Ressourcen Vorsicht geboten.

```
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#
```

Wenn der Befehl **show isdn status** nicht funktioniert oder den PRI nicht anzeigt, versuchen Sie, den Befehl **show isdn service** zu verwenden. Stellen Sie sicher, dass der Befehl **pri-group** in der Konfiguration unter dem T1/E1-Controller in der Konfiguration angezeigt wird. Wenn der Befehl nicht vorhanden ist, konfigurieren Sie den Controller mit dem Befehl **pri-group**.

Das folgende Beispiel zeigt eine Konfiguration für einen Cisco Router mit einem Channelized T1/PRI-Controller:

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

Tabelle 16-6: show isdn status für PRI

Feld	Bedeutung
Layer-1-Status: DEAKTIVIERT	Dies bedeutet, dass die PRI-Schnittstelle kein T1/E1-Framing auf der Leitung sieht. Berücksichtigen Sie die folgenden möglichen Ursachen für diese Situation: • Die PRI-Schnittstelle wird heruntergefahren. Überprüfen Sie entweder die Konfiguration für den Befehl **shutdown** unter

	der Schnittstelle serial0:23, oder suchen Sie im Befehl **show interface** nach einer administrativ deaktivierten Anzeige. Verwenden Sie das Konfigurationsprogramm, und geben Sie **no shutdown** unter der betreffenden Schnittstelle ein. Geben Sie den Befehl **clear controller T1/E1 *n* an der Eingabeaufforderung ein, um sicherzustellen, dass die PRI-Schnittstelle neu gestartet wird.** • Bei der Verkabelung liegt ein Problem vor. Sie müssen das Kabel austauschen. Verwenden Sie ein Durchgangskabel RJ-45. Halten Sie die RJ-45-Kabelenden nebeneinander, um das Kabel zu prüfen. Wenn die Pins in der gleichen Reihenfolge angeordnet sind, ist das Kabel gerade durchgehend. Wenn die Reihenfolge der Pins umgekehrt ist, wird das Kabel gerollt. Ersetzen Sie das Kabel. • Die Leitung funktioniert möglicherweise nicht. Kontaktieren Sie den Netzbetreiber, um den Betrieb der Verbindung zu bestätigen und die Switch-Typeinstellungen zu überprüfen. • Stellen Sie sicher, dass der Router ordnungsgemäß funktioniert. Wenn fehlerhafte oder defekte Hardware vorhanden ist, ersetzen Sie diese bei Bedarf.
Layer-2-Status: State = TEI_ASSIGNED	Überprüfen Sie die SwitchType-Einstellung. Die Einstellung für den schnittstellenspezifischen ISDN-Switch überschreibt die globale Switch-Einstellung. Überprüfen Sie, ob T1/E1 so konfiguriert ist, dass

	es mit dem Switch des Anbieters übereinstimmt (T1/E1-Probleme werden in Kapitel 15 behandelt). Um die Layer-2-Verhandlungen zwischen Switch und Router anzuzeigen, verwenden Sie den privilegierten exec-Befehl **debug isdn q921**. Die q921-Debuggen werden in der *Debug-Befehlsreferenz* dokumentiert. Debugger sind in hohem Maße von CPU-Ressourcen abhängig. Daher ist bei der Verwendung dieser Ressourcen Vorsicht geboten.
Anzahl der Anrufe/verwendete Anrufsteuerungsblöcke/Gesamtzahl der zugewiesenen ISDN-Anrufsteuerungsblöcke	Diese Zahlen geben an, wie viele Anrufe ausgeführt werden und wie viele Ressourcen für diese Anrufe zugewiesen sind. Wenn die Anzahl der zugewiesenen CCBs größer ist als die Anzahl der verwendeten CCBs, können Sie bedenken, dass bei der Freigabe von CCBs Probleme auftreten können. Stellen Sie sicher, dass CCBs für eingehende Anrufe verfügbar sind.

DFÜ-Routing nach Bedarf: Dialer-Schnittstellenoperationen

DFÜ-Routing (Dial on Demand Routing, DDR) ist eine Methode zur kostengünstigen und bedarfsgerechten Bereitstellung von WAN-Verbindungen, entweder als primäre Verbindung oder als Backup für eine serielle Verbindung ohne Wählen.

Eine **Dialer-Schnittstelle** ist eine beliebige Router-Schnittstelle, die einen Anruf tätigen oder empfangen kann. Dieser generische Begriff sollte von dem Begriff **Dialer-Schnittstelle** unterschieden werden (mit einem Großbuchstaben D), der sich auf eine logische Schnittstelle bezieht, die zur Steuerung einer oder mehrerer physischer Schnittstellen eines Routers konfiguriert ist und in einer Router-Konfiguration als Schnittstelle Dialer X angesehen wird. Ab diesem Punkt, sofern nicht anders angegeben, verwenden wir den Begriff Dialer im generischen Sinne.

Die Dialer-Schnittstellenkonfiguration ist in zwei Varianten erhältlich: Dialer Map-basiert (manchmal auch als Legacy DDR bezeichnet) und Dialer-Profile. Welche Methode Sie verwenden, hängt von den Umständen ab, unter denen Sie eine DFÜ-Verbindung benötigen. DDR wurde erstmals in IOS Version 9.0, Dialer-Profile in IOS Version 11.2, auf der Dialer-Zuordnung basiert, eingeführt.

Anrufen einer Nummer

Im Kern ist DDR nur eine Erweiterung des Routings, bei der *interessante Pakete* an eine Dialer-Schnittstelle weitergeleitet werden, was einen Wählversuch auslöst. In den folgenden Abschnitten werden die Konzepte für die Definition von interessantem Datenverkehr und das Routing für DDR-

Verbindungen erläutert.

Interessante Pakete

Interessant ist der Begriff zur Beschreibung von Paketen oder Datenverkehr, der entweder einen Wählversuch auslöst oder, wenn eine Wählverbindung bereits aktiv ist, den Leerlauf-Timer auf der Wählschnittstelle zurücksetzt. Damit ein Paket als interessant gilt:

- Das Paket muss die in einer Zugriffsliste definierten "permit"-Kriterien erfüllen.
- Die Zugriffsliste muss von der Wählliste referenziert werden, oder das Paket muss ein Protokoll sein, das allgemein von der Wählliste erlaubt ist.
- Die Dialer-Liste muss einer Dialer-Schnittstelle über eine Dialer-Gruppe zugeordnet sein.

Pakete werden nie automatisch als interessant angesehen (standardmäßig). Interessante Paketdefinitionen müssen explizit in einer Router- oder Zugriffsserver-Konfiguration deklariert werden.

Dialer-Gruppe

In der Konfiguration jeder Dialer-Schnittstelle auf dem Router oder dem Zugriffsserver muss ein **Dialer-Group-**Befehl vorhanden sein. Wenn der Befehl **dialer-group** nicht vorhanden ist, gibt es keine logische Verbindung zwischen den interessanten Paketdefinitionen und der Schnittstelle. Die Befehlssyntax:

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

Die Gruppennummer ist die Nummer der DFÜ-Zugriffsgruppe, zu der die jeweilige Schnittstelle gehört. Diese Zugriffsgruppe wird mit dem Befehl **dialer-list** definiert. Akzeptable Werte sind nicht null, positive ganze Zahlen zwischen 1 und 10.

Eine Schnittstelle kann nur einer einzelnen DFÜ-Zugriffsgruppe zugeordnet werden. Mehrfachzuweisungen von Wählgruppen sind nicht zulässig. Eine zweite DFÜ-Zugriffsgruppenzuweisung überschreibt die erste. Eine Dialer-Zugriffsgruppe wird mit dem Befehl **dialer-group** definiert. Der Befehl **dialer-list** ordnet eine Zugriffsliste einer Dialer-Zugriffsgruppe zu.

Pakete, die der angegebenen Dialer-Gruppe entsprechen, lösen eine Verbindungsanforderung aus.

Die Zieladresse des Pakets wird anhand der Zugriffsliste ausgewertet, die im zugehörigen Befehl **dialer-list** angegeben ist. Wenn der Anruf erfolgreich verläuft, wird entweder ein Anruf initiiert (wenn noch keine Verbindung hergestellt wurde) oder der Timer für Leerlaufzeiten zurückgesetzt (wenn ein Anruf gerade verbunden ist).

Wählliste

Mit dem globalen Konfigurationsbefehl **dialer-list** wird eine DDR-Wählliste definiert, um das Wählen nach Protokoll oder einer Kombination aus Protokoll und Zugriffsliste zu steuern. Interessante Pakete sind solche Pakete, die der Berechtigung auf Protokollebene entsprechen oder die in der Liste im Befehl **dialer-list** zugelassen sind: **dialer-list** *dialer-group* **protocol** *protocol-name* **{permit | Ablehnen | Liste** *access-list-nummer* **| access-group}**

Dialer-Gruppe ist die Nummer einer Dialer-Zugriffsgruppe, die in einem beliebigen Schnittstellenkonfigurationsbefehl für Dialer-Gruppen identifiziert wird.

Der Protokollname ist eines der folgenden Protokollschlüsselwörter: appletalk, bridge, clns, clns_es, clns_is, decnet, decnet_router-L1, decnet_router-L2, decnet_node, ip, ipx, vines oder xns.

Zulassen des Zugriffs auf ein ganzes Protokoll.

Verweigert den Zugriff auf ein ganzes Protokoll.

list gibt an, dass eine Zugriffsliste zum Definieren einer feineren Granularität als ein ganzes Protokoll verwendet wird.

access-list-number ***- Zugriffslistennummern, die in den Standard- oder erweiterten Zugriffslisten DECnet, Banyan VINES, IP, Novell IPX oder XNS, einschließlich Zugriffslisten für Novell IPX Extended Service Access Points (SAP) und Bridging-Typen, angegeben sind.*** Die unterstützten Zugriffslistentypen und -nummern finden Sie in Tabelle 16-7.

Name *der* Filterliste für die *Zugriffsgruppe*, der in den Befehlen **für den** Filtersatz **der CLN** und **für die Zugriffsgruppe** verwendet wird.

Tabelle 16-7: Nummerierung der Zugriffslisten nach Protokoll

Zugriffslistentyp	Nummernbereich der Zugriffsliste (dezimal)
AppleTalk	600-699
Banyan VINES (Standard)	1 bis 100
Banyan VINES (erweitert)	101-200
DECnet	300-399
IP (Standard)	1-99
IP (erweitert)	100-199
Novell IPX (Standard)	800-899
Novell IPX (erweitert)	900-999
Transparentes Bridging	200-299
XNS	500-599

Zugriffsliste

Für jedes Netzwerkprotokoll, das über die Wählverbindung gesendet werden soll, kann eine Zugriffsliste konfiguriert werden. Zur Kostenkontrolle ist es in der Regel wünschenswert, eine Zugriffsliste zu konfigurieren, um zu verhindern, dass bestimmte Zugriffe, z. B. Routing-Updates, eine Verbindung aufrufen oder aufrechterhalten. Beachten Sie, dass wir beim Erstellen von Zugriffslisten zum Definieren von interessantem und uninteressantem Datenverkehr nicht erklären, dass uninteressante Pakete die Wählverbindung nicht überschreiten können. Wir geben nur an, dass sie weder den Timer für die Inaktivität zurücksetzen noch eine Verbindung selbst herstellen. Solange die Wählverbindung aktiv ist, können uninteressante Pakete weiterhin über die Verbindung übertragen werden.

Beispielsweise kann auf einem Router, auf dem EIGRP als Routing-Protokoll ausgeführt wird, eine

Zugriffsliste konfiguriert werden, um EIGRP-Pakete für uninteressant und den gesamten anderen IP-Verkehr interessant zu erklären:

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

Zugriffslisten können für alle Protokolle konfiguriert werden, die die Wählverbindung passieren können. Denken Sie daran, dass das Standardverhalten bei fehlender **Zugriffslisten-Zulassen-**Anweisung für jedes Protokoll darin besteht, den gesamten Datenverkehr abzulehnen. Wenn es keine Zugriffsliste und keinen Befehl **dialer-list** gibt, der das Protokoll zulässt, dann ist dieses Protokoll uninteressant. In der Praxis fließen diese Pakete überhaupt nicht über die Verbindung, wenn keine Wählliste für ein Protokoll vorhanden ist.

Beispiel: Alles miteinander verbinden

Wenn alle Elemente vorhanden sind, können Sie den vollständigen Prozess überprüfen, durch den der "interessante" Status eines Pakets bestimmt wird. In diesem Beispiel sind IP und IPX die Protokolle, die die Wählverbindung passieren können. Der Benutzer möchte verhindern, dass Broadcasts und Routing-Updates einen Anruf initiieren oder die Verbindung aufrechterhalten.

```
!
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
!
```

Ein Paket muss von der **Zugriffsliste 121**-Anweisungen zugelassen werden, bevor die **Schnittstelle async 1** überschritten wird, um als *interessant* angesehen zu werden. In diesem Fall werden EIGRP-Pakete wie alle anderen Broadcast-Pakete abgelehnt, während der gesamte andere IP-Datenverkehr zugelassen ist. Beachten Sie, dass dies nicht verhindert, dass EIGRP-Pakete die Verbindung übertragen. Dies bedeutet nur, dass diese Pakete den Inaktivitäts-Timer nicht zurücksetzen oder einen Wählversuch auslösen.

Ebenso erklärt **die Zugriffsliste 903** IPX RIP-, SAP- und GNS-Anfragen für uninteressant, während der gesamte andere IPX-Datenverkehr interessant ist. Ohne diese Ablehnungsanweisungen würde die Wählverbindung wahrscheinlich nie ausfallen, und es würde eine sehr große Telefonrechnung entstehen, da Pakete dieser Art ständig über ein IPX-Netzwerk übertragen werden.

Wenn **Dialer-Gruppe 7** auf der asynchronen Schnittstelle konfiguriert ist, wissen wir, dass **Dialer-Liste 7** erforderlich ist, um die interessanten Datenverkehrsfilter (also Zugriffslisten) mit der Schnittstelle zu verknüpfen. Für jedes Protokoll ist eine **Dialer-Liste-**Anweisung erforderlich (und *nur* eine kann konfiguriert werden), wobei sicherzustellen ist, dass die Nummer der Dialer-Liste mit

der Nummer der Dialer-Gruppe auf der Schnittstelle übereinstimmt.

Auch hier ist zu bedenken, dass die **zur Definition von interessantem Datenverkehr konfigurierten *Ablehnungsanweisungen*** in den Zugriffslisten **die** Verbindung der **blockierten Pakete *nicht*** verhindern.

Mit dem Befehl **debug dialer** können Sie die Aktivität anzeigen, die einen Wählversuch auslöst:

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

Hier sehen wir, dass IP-Datenverkehr mit der Quelladresse 172.16.1.111 und der Zieladresse 172.16.2.22 einen Wählversuch an der Schnittstelle Async1 ausgelöst hat.

Routing

Nach der Definition müssen interessante Pakete ordnungsgemäß weitergeleitet werden, damit ein Anruf initiiert werden kann. Der Routing-Prozess ist von zwei Faktoren abhängig: Routingtabelleneinträge und eine "Up"-Schnittstelle, über die Pakete weitergeleitet werden.

Schnittstellen - Up/Up (Spoofing)

Damit Pakete an eine Schnittstelle und über diese weitergeleitet werden können, muss diese Schnittstelle aktiv/aktiv sein, wie in der Ausgabe von **Anzeigeschnittstellen** zu sehen ist:

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

Was passiert mit einer Dialer-Schnittstelle, die nicht verbunden ist? Wenn das Protokoll auf der Schnittstelle nicht aktiv ist und nicht ausgeführt wird, impliziert dies, dass die Schnittstelle selbst nicht aktiv ist. Routen, die auf dieser Schnittstelle basieren, werden von der Routing-Tabelle gelöscht, und der Datenverkehr wird nicht an diese Schnittstelle weitergeleitet. Das Ergebnis ist, dass keine Anrufe von der Schnittstelle initiiert werden.

Um dieser Möglichkeit entgegenzuwirken, ist es möglich, den Status **up/up (Spoofing)** für Dialer-Schnittstellen zuzulassen. Jede Schnittstelle kann als Dialer-Schnittstelle konfiguriert werden. Beispielsweise kann eine serielle oder async-Schnittstelle in einen Dialer umgewandelt werden, indem der Befehl **In-Band-Dialer** oder **Dialer dtr** zur Konfiguration der Schnittstelle hinzugefügt wird. Diese Leitungen sind für Schnittstellen, die naturgemäß eine Dialer-Schnittstelle (BRIs und PRIs) sind, nicht erforderlich. Die Ausgabe für eine Show-Schnittstelle sieht wie folgt aus:

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

Anders ausgedrückt: Die Schnittstelle "gibt vor, **aktiv** zu sein**/aktiv** zu sein, damit die zugehörigen Routen in Kraft bleiben und Pakete an die Schnittstelle weitergeleitet werden können.

Unter bestimmten Umständen ist eine Dialer-Schnittstelle nicht **aktiv/aktiv (Spoofing)**. Die Ausgabe

der **show interface** kann anzeigen, dass die Schnittstelle vom Administrator deaktiviert wurde:

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

Administrativ down bedeutet lediglich, dass die Schnittstelle mit dem Befehl **shutdown** konfiguriert wurde. Dies ist der Standardstatus einer beliebigen Router-Schnittstelle, wenn der Router zum ersten Mal gestartet wird. Um dies zu beheben, verwenden Sie den Schnittstellenkonfigurationsbefehl **no shutdown**.

Die Schnittstelle kann auch im Standby-Modus angezeigt werden:

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

Dieser Status gibt an, dass die Schnittstelle als Sicherung für eine andere Schnittstelle konfiguriert wurde. Wenn eine Verbindung bei einem Ausfall Redundanz erfordert, kann eine Dialer-Schnittstelle als Backup eingerichtet werden. Hierzu werden der Schnittstelle der Primärverbindung folgende Befehle hinzugefügt:

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

Sobald der Befehl **Backup Interface** konfiguriert wurde, wird die als Sicherung verwendete Schnittstelle in den Standby-Modus versetzt, bis die primäre Schnittstelle **ausfällt/ausfällt**. Zu diesem Zeitpunkt wechselt die als Sicherung konfigurierte Dialer-Schnittstelle in den Zustand **"up/up" (spoofing)** bis zu einem Wählereignis.

Statische Routen und statische Floating-Routen

Die sicherste Methode zum Weiterleiten von Paketen an eine Dialer-Schnittstelle ist statisches Routing. Diese Routen werden manuell mit dem folgenden Befehl in die Konfiguration des Routers oder des Zugriffservers eingegeben:

ip route ***prefix mask*** **{*Adresse* | *interface*} [*Distanz*]**

Präfix: IP-Routenpräfix für das Ziel.

Maske: Präfixmaske für das Ziel.

Adresse: IP-Adresse des nächsten Hop, die zum Erreichen des Zielnetzwerks verwendet werden kann.

Schnittstelle: Netzwerkschnittstelle für ausgehenden Datenverkehr.

Entfernung: (Optional) Eine administrative Distanz. Dieses Argument wird in schwimmenden

statischen Routen verwendet.

Statische Routen werden in Situationen verwendet, in denen die Wählverbindung die einzige Verbindung mit dem Remote-Standort ist. Eine statische Route hat einen Wert für die administrative Distanz von einem (1), was sie gegenüber dynamischen Routen zum gleichen Ziel bevorzugt.

Auf der anderen Seite werden Floating-statische Routen - d. h. statische Routen mit einer vordefinierten administrativen Distanz - in der Regel in Backup-DDR-Szenarien verwendet. In diesen Szenarien werden Pakete über ein dynamisches Routing-Protokoll wie RIP oder EIGRP über die primäre Verbindung weitergeleitet.

Eine normale statische Route (administrative Distanz = 1) ist entweder EIGRP (administrative Distanz = 90) oder RIP (administrative Distanz = 120) vorzuziehen. Die statische Route führt dazu, dass Pakete über die Wählleitung weitergeleitet werden, selbst wenn die primäre Leitung aktiv ist und Datenverkehr weiterleiten kann. Wenn die statische Route jedoch mit einer höheren administrativen Distanz konfiguriert wird als die der auf dem Router verwendeten dynamischen Routing-Protokolle, wird die Floating-statische Route nur verwendet, wenn keine "bessere" Route vorhanden ist - eine Route mit einer geringeren administrativen Distanz.

Wenn Backup DDR über den Befehl **backup interface** aufgerufen wird, ist die Situation etwas anders. Da sich die Dialer-Schnittstelle im Standby-Modus befindet, während die primäre **aktiv** ist, kann eine statische Route oder eine Floating-statische Route konfiguriert werden. Die Dialer-Schnittstelle versucht erst dann eine Verbindung herzustellen, wenn die primäre Schnittstelle **ausfällt/ausfällt**.

Für eine bestimmte Verbindung ist die Anzahl der statischen (oder schwimmenden statischen) Routen eine Funktion der Adressierung auf den Dialer-Schnittstellen. Wenn die beiden Dialer-Schnittstellen (eine auf jedem der beiden Router) ein gemeinsames Netzwerk oder ein gemeinsames Subnetz nutzen, ist in der Regel nur eine statische Route erforderlich. Er verweist auf das Remote-LAN, wobei die Adresse der Dialer-Schnittstelle des Remote-Routers als Next-Hop-Adresse verwendet wird.

Beispiele

Beispiel 1: Wählen ist die einzige Verbindung, die nummerierte Schnittstellen verwendet. Eine Route ist ausreichend.

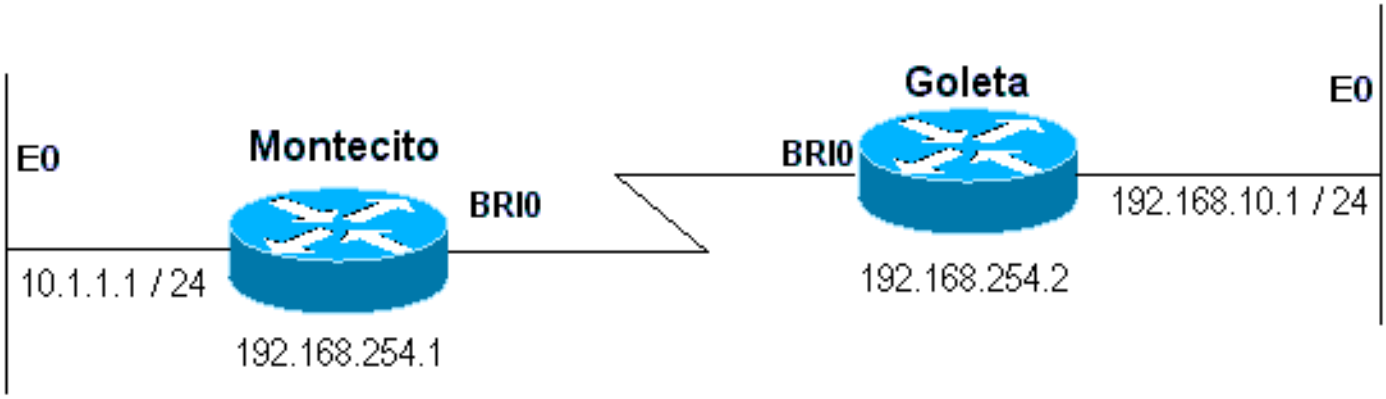

Abbildung 16-4: Wählen über nummerierte Schnittstellen

```
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
```

Beispiel 2: Wählen ist die einzige Verbindung, die unnummerierte Schnittstellen verwendet. Dies kann mit nur einer Route konfiguriert werden, es ist jedoch üblich, zwei Routen zu konfigurieren: eine Hostroute zur LAN-Schnittstelle am Remote-Router und eine Route zum Remote-LAN über die Remote-LAN-Schnittstelle. Dadurch werden Probleme bei der Zuordnung von Layer 3 zu Layer 2 vermieden, die zu Kapselungsfehlern führen können.

Diese Methode wird auch verwendet, wenn die Dialer-Schnittstellen auf den beiden Geräten nummeriert sind, jedoch nicht im gleichen Netzwerk oder Subnetz.

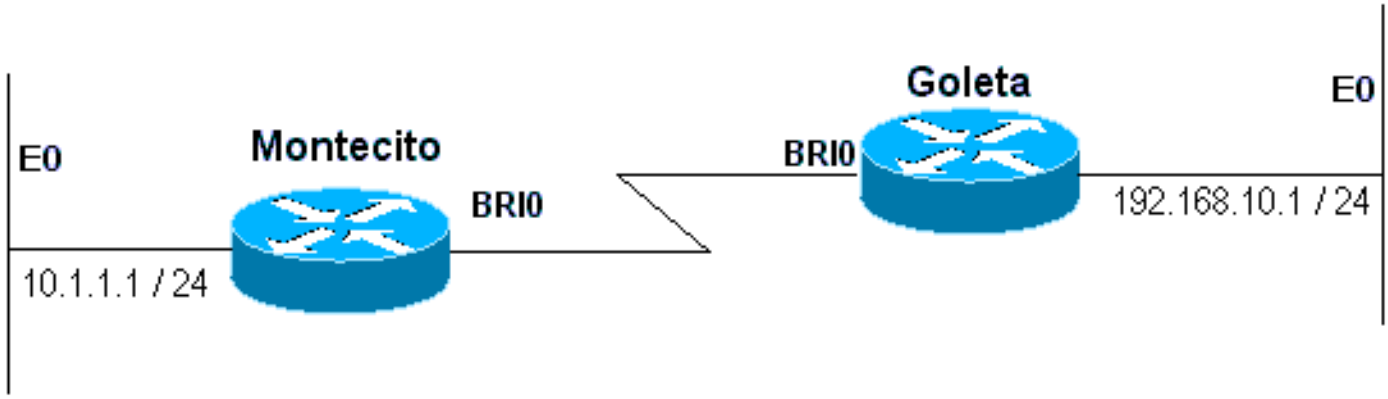

Abbildung 16-5: Wählen mit nicht nummerierten Schnittstellen

```
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
```

Beispiel 3: Dial ist eine Sicherungsverbindung über nummerierte Schnittstellen. Eine Floating-statische Route ist erforderlich.

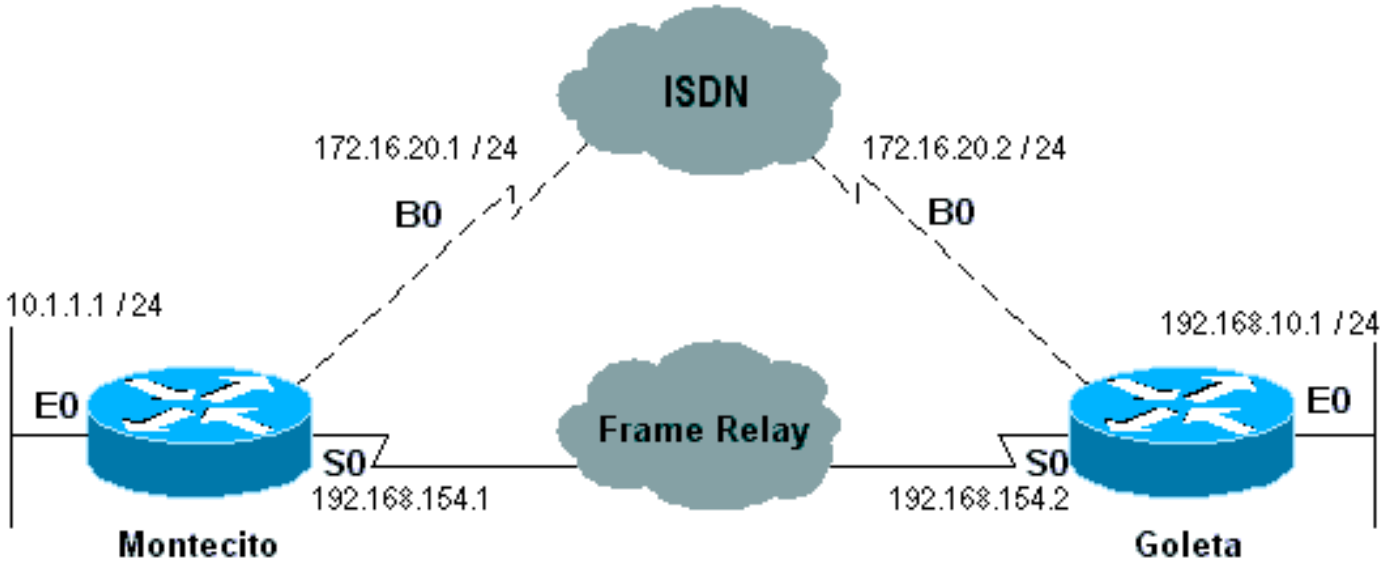

Abbildung 16-6: Sicherung über nummerierte Schnittstellen

```
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
```

Beispiel 4: Dial (Wählen) ist eine Sicherungsverbindung, die unnummerierte Schnittstellen verwendet. Wie in Beispiel 2 oben wird diese Methode auch verwendet, wenn die Dialer-Schnittstellen auf den beiden Geräten nummeriert sind, jedoch nicht im gleichen Netzwerk oder Subnetz.

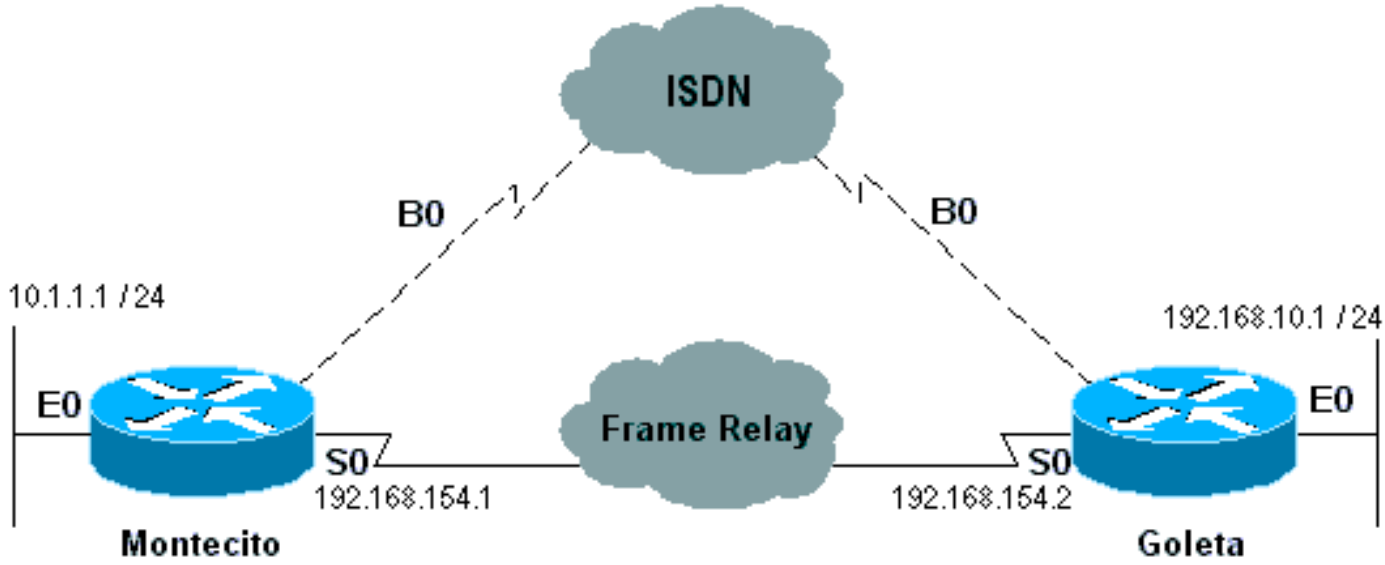

Abbildung 16-7: Sicherung mithilfe nicht nummerierter Schnittstellen

```
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
```

Dialer-Karten

Dialer Map-basierter (Legacy-)DDR ist leistungsstark und umfassend, aber seine Beschränkungen wirken sich auf Skalierung und Erweiterbarkeit aus. DDR basiert auf einer statischen Bindung zwischen der Anrufspezifikation pro Ziel und der Konfiguration der physischen Schnittstelle.

DDR basiert jedoch auch auf Dialer Map und hat viele Stärken. Sie unterstützt Frame Relay, ISO CLNS, LAPB, Snapshot-Routing und alle Routing-Protokolle, die von Cisco Routern unterstützt werden. Standardmäßig unterstützt Dialer Map-basierter DDR schnelles Switching.

Wenn eine Schnittstelle für ausgehende Anrufe konfiguriert wird, muss für jedes Remote-Ziel und für jede unterschiedliche angerufene Nummer am Remote-Ziel eine Wählzuordnung konfiguriert werden. Wenn Sie beispielsweise eine Multilink-PPP-Verbindung bei der Wahl von einem ISDN BRI auf eine andere ISDN BRI-Schnittstelle mit einer unterschiedlichen lokalen Verzeichnisnummer für jeden seiner B-Kanäle wünschen, benötigen Sie eine Wählzuordnung für jede der Remote-Nummern:

```
!
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
!
```

Die Reihenfolge, in der Dialer Maps konfiguriert werden, kann wichtig sein. Wenn zwei oder mehr Wählzuordnungsbefehle auf dieselbe Remote-Adresse verweisen, versucht der Router oder der Zugriffsserver diese nacheinander, bis eine Verbindung erfolgreich hergestellt wird.

Hinweis: IOS kann Wählzuordnungen dynamisch auf einem Router erstellen, der einen Anruf empfängt. Die Wählzuordnung basiert auf dem authentifizierten Benutzernamen und der ausgehandelten IP-Adresse des Anrufers. Dynamische Dialer-Karten können nur in der Ausgabe des Befehls **show dialer map** angezeigt werden. Sie können diese nicht in der aktuellen Konfiguration des Routers oder des Zugriffservers anzeigen.

Befehlssyntax

Verwenden Sie die folgende Form des Befehls **Dialer Map** Interface Configuration, um:

- eine serielle Schnittstelle oder eine ISDN-Schnittstelle konfigurieren, um einen oder mehrere Standorte anzurufen, oder
- Anrufe von mehreren Standorten empfangen.

Alle Optionen werden in dieser ersten Form des Befehls angezeigt. Um einen bestimmten Dialer Map-Eintrag zu löschen, verwenden Sie eine **no**-Form dieses Befehls.

```
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]]
```

Verwenden Sie die folgende Form des Befehls **Dialer Map**, um:

- eine serielle Schnittstelle oder eine ISDN-Schnittstelle konfigurieren, um einen Anruf an mehrere Standorte zu tätigen, und
- um Anrufe von mehreren Standorten zu authentifizieren.
  ```
  dialer map protocol next-hop-address [name hostname] [spc] [speed 56 | 64]
  [broadcast] [dial-string[:isdn-subaddress]]
  ```

Verwenden Sie die folgende Form des Befehls **Dialer Map**, um eine serielle Schnittstelle oder eine ISDN-Schnittstelle zur Unterstützung der Bridging-Funktion zu konfigurieren.

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

Verwenden Sie die folgende Form des Befehls **Dialer Map**, um eine asynchrone Schnittstelle zu konfigurieren, um einen Anruf zu tätigen:

- eine einzelne Site, die ein Systemskript erfordert oder über kein Modem-Skript verfügt, oder
- mehrere Standorte auf einer einzigen Leitung, auf mehreren Leitungen oder in einer Dialer-Drehgruppe.

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

Syntaxbeschreibung

- *Protocol* **-** Protokollschlüsselwörter. Wählen Sie eine der folgenden Optionen: **appletalk, bridge, clns, decnet, ip, ipx, novell, Snapshot, vines** oder xns.
- *next-hop-address* - Die Protokolladresse, die verwendet wird, um Adressen zuzuordnen, für die Pakete bestimmt sind. Dieses Argument wird nicht mit dem **bridge** Protocol-Schlüsselwort verwendet.
- **Name** - (Optional) gibt das Remote-System an, mit dem der lokale Router oder der Zugriffsserver kommuniziert. Wird für die Authentifizierung des Remote-Systems bei eingehenden Anrufen verwendet.
- *hostname* - (Optional) Groß- und Kleinschreibung beachten: Name oder ID des Remote-Geräts (in der Regel der Hostname). Bei Routern mit ISDN-Schnittstellen kann das *Hostnamensfeld* die Nummer enthalten, die die Anrufer-Leitung-ID bereitstellt (in Fällen, in denen die Rufnummernerkennung, auch *CLI* genannt*, Anrufer-ID* und *automatische Rufnummernerkennung* ***(ANI), verfügbar ist).***
- **SPC** - (Optional) Gibt eine semipermanente Verbindung zwischen Kundengerät und Austausch an. Es wird nur in Deutschland für Schaltungen zwischen einem ISDN BRI- und einem ISDN 1TR6-Switch und in Australien für Schaltungen zwischen einem ISDN PRI- und einem TS-014-Switch verwendet.
- **Geschwindigkeit 56 | 64** - (Optional) Stichwort und Wert, der die Leitungsgeschwindigkeit in Kilobit pro Sekunde angibt. Nur für ISDN. Die Standardgeschwindigkeit ist 64 Kbit/s.
- **Broadcast** - (Optional) Gibt an, dass Broadcasts an diese Protokolladresse weitergeleitet werden sollen.
- **Modem-Skript** - (Optional) gibt das Modem-Skript an, das für die Verbindung (für asynchrone Schnittstellen) verwendet werden soll.
- *modem-regexp* - (Optional) Regulärer Ausdruck, dem ein Modem-Skript zugeordnet wird (für asynchrone Schnittstellen).
- **Systemskript** - (Optional) gibt das für die Verbindung zu verwendende Systemskript an (für asynchrone Schnittstellen).
- *system-regexp* - (Optional) Regulärer Ausdruck, dem ein Systemskript zugeordnet wird (für asynchrone Schnittstellen).
- *dial-string[:isdn-subaddress]* ***(Optional):*** Die Telefonnummer wird nach Erkennung von Paketen mit einer angegebenen Next-Hop-Adresse, die der definierten Zugriffsliste (und der optionalen Subadressnummer für ISDN-Multipoint-Verbindungen) entspricht, an das Wählgerät gesendet. Bei Verwendung der Wählzeichenfolge und der ISDN-Subadresse muss es sich um das letzte Element in der Befehlszeile handeln.

Dialer-Profile

Hinweis: In diesem Abschnitt bezieht sich der Begriff "Dialer-Schnittstelle" auf die konfigurierte Schnittstelle. nicht an eine physische Schnittstelle am Router oder Zugriffsserver.

Die in IOS 11.2 eingeführte DDR-Implementierung von Dialer-Profilen basiert auf einer Trennung zwischen der Konfiguration der logischen und der physischen Schnittstelle. Dialer-Profile

ermöglichen auch die dynamische Verbindung der logischen und physischen Konfigurationen auf Anrufbasis.

Die Dialer Profiles-Methode ist von Vorteil, wenn Sie folgende Schritte ausführen möchten:

- gemeinsame Nutzung einer Schnittstelle (ISDN, asynchron oder synchron) zum Tätigen oder Empfangen von Anrufen
- Änderung der Konfiguration auf Benutzerbasis (außer Kapselung in der ersten Phase von Dialer-Profilen)
- Brücke zu vielen Zielen
- Vermeidung von Split-Horizon-Problemen

Dialer-Profile ermöglichen die Trennung der Konfiguration physischer Schnittstellen von der für einen Anruf erforderlichen logischen Konfiguration. Außerdem können die logischen und physischen Konfigurationen dynamisch pro Anruf miteinander verbunden werden.

Ein *Dialer-Profil* besteht aus den folgenden Elementen:

- Eine Dialer-Schnittstellenkonfiguration (eine logische Einheit), einschließlich einer oder mehrerer Wählzeichenfolgen (von denen jede zum Erreichen eines Zielsubnetzwerks verwendet wird)
- Eine *Dialer-Map-**Klasse, die alle Eigenschaften für einen Anruf in der angegebenen Wählzeichenfolge definiert.***
- Ein geordneter *Dialer-Pool* von physischen Schnittstellen, die von der Dialer-Schnittstelle verwendet werden

Alle Anrufe, die an oder von demselben Ziel-Subnetz gehen, verwenden dasselbe Wählprofil.

Eine Dialer-Schnittstellenkonfiguration enthält alle Einstellungen, die zum Erreichen eines bestimmten Zielsubnetzwerks erforderlich sind (und alle durch dieses erreichten Netzwerke). Für dieselbe Dialer-Schnittstelle können mehrere Wählzeichenfolgen angegeben werden. Jede Wählzeichenfolge kann einer anderen Wählzuordnungsklasse zugeordnet werden. Die Dialer-Zuordnungsklasse definiert alle Eigenschaften für jeden Anruf in der angegebenen Wählzeichenfolge. Beispielsweise kann die Map-Klasse für ein Ziel eine ISDN-Geschwindigkeit von 56 Kbit/s angeben. Die Zuordnungsklasse für ein anderes Ziel kann eine ISDN-Geschwindigkeit von 64 Kbit/s angeben.

Jede Dialer-Schnittstelle verwendet einen Dialer-Pool. Hierbei handelt es sich um einen Pool aus physischen Schnittstellen, die basierend auf der Priorität, die jeder physischen Schnittstelle zugewiesen wird, angeordnet werden. Eine physische Schnittstelle kann mehreren Dialer-Pools angehören, wobei der Konflikt durch Priorität gelöst wird. ISDN BRI- und PRI-Schnittstellen können ein Limit für die minimale und maximale Anzahl von B-Kanälen festlegen, die von allen Dialer-Pools reserviert werden. Ein Kanal, der von einem Dialer-Pool reserviert wird, bleibt inaktiv, bis der Datenverkehr zum Pool geleitet wird.

Wenn Dialer-Profile zum Konfigurieren von DDR verwendet werden, verfügt eine physische Schnittstelle über keine Konfigurationseinstellungen außer Kapselung und den Dialer-Pools, zu denen die Schnittstelle gehört.

Hinweis: Der vorstehende Absatz hat eine Ausnahme. Befehle, die vor Abschluss der Authentifizierung angewendet werden, müssen auf der physischen Schnittstelle (oder BRI oder PRI) und nicht im Dialer-Profil konfiguriert werden. Dialer-Profile kopieren keine PPP-Authentifizierungsbefehle (oder LCP-Befehle) auf die physische Schnittstelle.

Abbildung 16-8 zeigt eine typische Anwendung von Dialer-Profilen. Router A verfügt über die Dialer-Schnittstelle 1 für das Einwahl-on-Demand-Routing mit dem Subnetz 1.1.1.0 und die Dialer-Schnittstelle 2 für das Einwahl-on-Demand-Routing mit dem Subnetz 2.2.2.0. Die IP-Adresse für die Dialer-Schnittstelle 1 ist ihre Adresse als Knoten im Netzwerk 1.1.1.0. Gleichzeitig dient diese IP-Adresse als IP-Adresse der physischen Schnittstellen, die von der Dialer-Schnittstelle 1 verwendet werden. Ebenso ist die IP-Adresse für die Dialer-Schnittstelle 2 ihre Adresse als Knoten im Netzwerk 2.2.2.0.

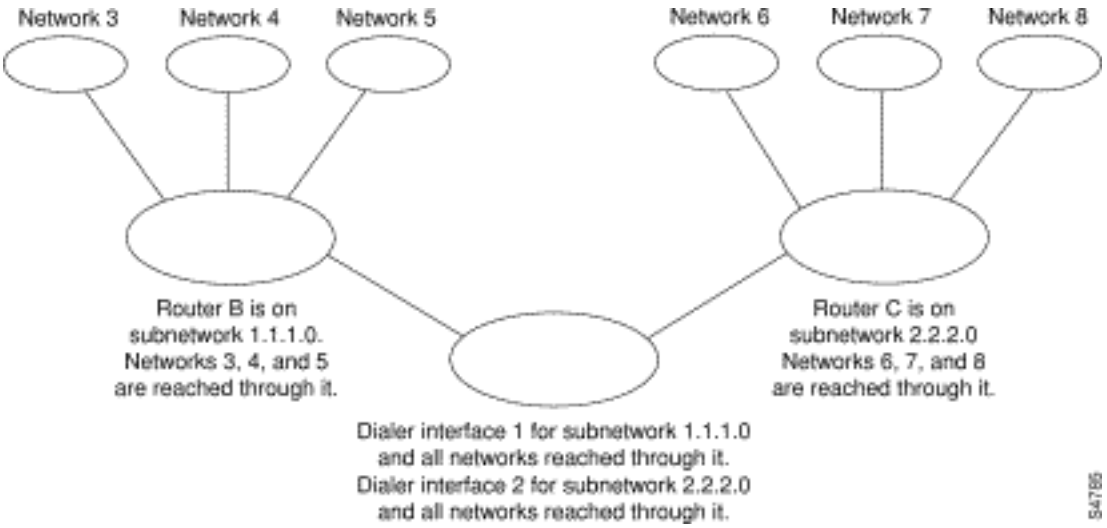

Abbildung 16-8: Typische Dialer-Profilanwendung

Eine Dialer-Schnittstelle verwendet nur einen Dialer-Pool. Eine physische Schnittstelle kann jedoch Mitglied eines oder mehrerer Dialer-Pools sein, und ein Dialer-Pool kann mehrere physische Schnittstellen als Mitglieder haben.

Abbildung 16-9 veranschaulicht die Beziehungen zwischen den Konzepten Dialer-Schnittstelle, Dialer-Pool und physische Schnittstellen. Dialer-Schnittstelle 0 verwendet Dialer-Pool 2. Die physische Schnittstelle BRI 1 gehört zum Dialer-Pool 2 und hat eine besondere Priorität im Pool. Die physische Schnittstelle BRI 2 gehört auch zum Dialer-Pool 2. Da der Konflikt auf der Grundlage der Prioritätsstufen der physischen Schnittstellen im Pool gelöst wird, müssen BRI 1 und BRI 2 im Pool unterschiedliche Prioritäten zugewiesen werden. Möglicherweise wird BRI 1 die Priorität 100 zugewiesen, BRI 2 die Priorität 50 im Dialer-Pool 2 (eine Priorität von 50 ist höher als eine Priorität von 100). BRI 2 hat im Pool eine höhere Priorität, und die entsprechenden Anrufe werden zuerst getätigt.

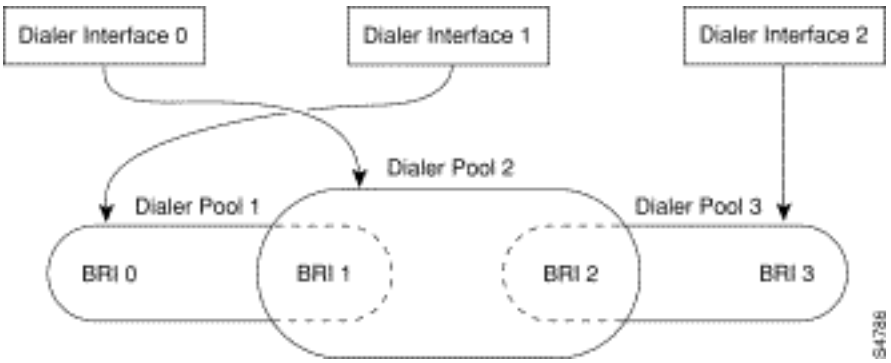

Abbildung 16-9: Beziehungen zwischen Dialer-Schnittstellen, Dialer-Pools und physischen Schnittstellen

[Konfigurationsschritte für das Dialer-Profil]

Befehl	Zweck
Schnittstellenwählnummer	Erstellen Sie eine Dialer-Schnittstelle.
IP-*Adressmaske*	Geben Sie die IP-Adresse und die Maske der Dialer-Schnittstelle als Knoten im Zielnetzwerk an, der aufgerufen werden soll.
Kapselung ppp	Geben Sie PPP-Kapselung an.
Dialer-Remote-*Benutzername*	Geben Sie den CHAP-Authentifizierungsnamen des Remote-Routers an.
Dialer-Zeichenfolge *Dial-String-Klassenname*	Geben Sie das anzurufende Remote-Ziel und die Zuordnungsklasse an, die die Eigenschaften für Anrufe an dieses Ziel definiert.
Dialer-*Poolnummer*	Geben Sie den Nummernpool an, der für Anrufe an dieses Ziel verwendet werden soll.
Dialer-Gruppen-*Gruppennummer*	Weisen Sie die Dialer-Schnittstelle einer Dialer-Gruppe zu.
dialer-list *dialer-group* protocol *protocol-name* {permit | Ablehnen | list *access-list-number*}	Geben Sie eine Zugriffsliste nach Listennummer oder Protokoll- und Listennummer an, um die "interessanten" Pakete zu definieren, die einen Anruf auslösen können.

PPP-Betrieb

Das Point-to-Point Protocol (PPP) ist das weit verbreitete Link-Layer-Transportprotokoll und hat SLIP vollständig als das Protokoll der Wahl für synchrone und asynchrone (und in vielen Fällen auch nicht wählbare) serielle Verbindungen verwendet. PPP wurde ursprünglich 1989 von RFC 1134 definiert, der seither durch eine Reihe von RFCs überholt wurde, die in RFC1661 gipfelten. Es gibt auch zahlreiche RFCs, die Elemente des Protokolls definieren, wie RFC1990 (das PPP Multilink Protocol), RFC2125 (das PPP Bandwidth Allocation Protocol) und viele andere. Ein Online-Repository mit RFCs finden Sie unter:

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

Die beste Definition von PPP finden Sie möglicherweise in RFC 1661, in dem Folgendes steht:

Das Point-to-Point Protocol (PPP) stellt eine Standardmethode für die Übertragung von Multi-Protokoll-Datagrammen über Point-to-Point-Verbindungen bereit. PPP besteht aus drei Hauptkomponenten:

1. Eine Methode zum Kapseln von Multi-Protokoll-Datagrammen.
2. Ein Link Control Protocol (LCP) für die Einrichtung, Konfiguration und das Testen der Datenverbindung.

3. Eine Familie von Netzwerksteuerungsprotokollen (Network Control Protocols, NCPs) zum Einrichten und Konfigurieren verschiedener Netzwerkschichtprotokolle.

Phasen der PPP-Verhandlungen

Die PPP-Aushandlung erfolgt in drei Phasen: Link Control Protocol (LCP), Authentifizierung und Network Control Protocol (NCP). Jeder geht in der Reihenfolge nach der Einrichtung der asynchronen oder ISDN-Verbindung weiter.

LCP

PPP folgt nicht einem Client-/Servermodell. Alle Verbindungen sind Peer-to-Peer. Wenn also ein Anrufer und ein Empfänger vorhanden sind, müssen beide Enden der Punkt-zu-Punkt-Verbindung die ausgehandelten Protokolle und Parameter vereinbaren.

Wenn die Verhandlung beginnt, muss jeder Peer, der eine PPP-Verbindung herstellen möchte, eine Konfigurationsanfrage senden (siehe **Debug-PPP-Aushandlung** und nachfolgend CONFREQ genannt). Im CONFREQ sind alle Optionen enthalten, die nicht der Link Standard sind. Dazu gehören häufig die Maximum Receive Unit (MRU), die Async Control Character Map (ACCM), das Authentication Protocol (AuthProto) und die Magic Number. Ebenfalls sichtbar sind die für Multilink PPP verwendete Maximum Receive Reconstructed Unit (MRRU) und Endpoint Diskriminator (EndpointDisc).

Es gibt drei mögliche Antworten auf alle CONFREQ:

- Wenn der Peer die Optionen erkennt und den Werten in der CONFREQ zustimmt, muss eine Bestätigung für die Konfiguration (CONFACK) ausgestellt werden.
- Wenn eine der Optionen im CONFREQ nicht erkannt wird (z. B. einige anbieterspezifische Optionen) oder wenn die Werte für eine der Optionen in der Konfiguration des Peers explizit deaktiviert wurden, muss eine Configure-Reject (CONFREJ) gesendet werden.
- Wenn alle Optionen in der CONFREQ erkannt werden, muss eine CONFNAK (Configure-Negative-Bestätigung) gesendet werden. Die Werte können jedoch für den Peer nicht akzeptiert werden.

Die beiden Peers tauschen CONFREQs, CONFREJs und CONFNAKs so lange aus, bis jeder einen CONFACK sendet, bis die Wählverbindung unterbrochen ist, oder bis einer oder beide Peers anzeigen, dass die Verhandlung nicht abgeschlossen werden kann.

Authentifizierung

Nach dem erfolgreichen Abschluss der LCP-Aushandlung und der Erzielung einer Vereinbarung über AuthProto ist der nächste Schritt die Authentifizierung. Die Authentifizierung ist zwar nicht gemäß RFC1661 obligatorisch, wird jedoch für alle Wählverbindungen dringend empfohlen. In einigen Fällen ist dies eine Voraussetzung für einen ordnungsgemäßen Betrieb. Dialer-Profile sind ein Paradebeispiel.

Die beiden Hauptauthentifizierungstypen in PPP sind das Password Authentication Protocol (PAP) und das Challenge Handshake Authentication Protocol (CHAP), definiert durch RFC 1334 und aktualisiert durch RFC 1994.

PAP ist die einfachere von beiden, ist jedoch weniger sicher, da das Klartext-Kennwort über die

Wählverbindung gesendet wird. CHAP ist sicherer, da das Klartext-Kennwort niemals über die Wählverbindung gesendet wird.

PAP kann in einer der folgenden Umgebungen erforderlich sein:

- Eine große Anzahl von Client-Anwendungen, die CHAP nicht unterstützen
- Inkompatibilitäten zwischen verschiedenen CHAP-Implementierungen verschiedener Anbieter

Bei der Diskussion über die Authentifizierung ist es hilfreich, die Begriffe "Anforderer" und "Authentifizierer" zu verwenden, um die Rollen zu unterscheiden, die von den Geräten an beiden Enden der Verbindung übernommen werden, obwohl beide Peers in beiden Rollen agieren können. "Antragsteller" beschreibt das Gerät, das Netzwerkzugriff anfordert und Authentifizierungsinformationen bereitstellt. Der "Authentifizierer" überprüft die Gültigkeit der Authentifizierungsinformationen und lässt die Verbindung entweder zu oder unterbinden sie. Beide Peers agieren häufig in beiden Rollen, wenn eine DDR-Verbindung zwischen Routern hergestellt wird.

PAP

PAP ist recht einfach. Nach erfolgreichem Abschluss der LCP-Aushandlung sendet der Antragsteller wiederholt seine Kombination aus Benutzername und Kennwort über die Verbindung, bis der Authentifizierer mit einer Bestätigung antwortet oder bis der Link beschädigt ist. Der Authentifizierer kann die Verbindung trennen, wenn er feststellt, dass die Kombination aus Benutzername und Kennwort ungültig ist.

CHAP

CHAP ist etwas komplizierter. Der Authentifizierer sendet eine Herausforderung an den Antragsteller, der dann mit einem Wert antwortet. Dieser Wert wird mithilfe einer unidirektionalen Hash-Funktion berechnet, um die Herausforderung und das CHAP-Kennwort gemeinsam zu hash. Der resultierende Wert wird zusammen mit dem CHAP-Hostnamen des Antragstellers (der sich von seinem tatsächlichen Hostnamen unterscheiden kann) in einer **Antwortnachricht** an den Authentifizierer gesendet.

Der Authentifizierer liest den Hostnamen in der Antwortnachricht ein, sucht das erwartete Kennwort für diesen Hostnamen und berechnet dann den Wert, den er erwartet, dass der Anforderer in seiner Antwort gesendet wird, indem er dieselbe Hashfunktion ausführt, die der Anforderer ausgeführt hat. Wenn die resultierenden Werte übereinstimmen, ist die Authentifizierung erfolgreich. Der Ausfall sollte zu einer Verbindungstrennung führen.

AAA

Für die Durchführung von PAP oder CHAP kann ein AAA-Service (Authentication, Authorization and Accounting) wie TACACS+ oder RADIUS verwendet werden.

NCP

Nach erfolgreicher Authentifizierung beginnt die NCP-Phase. Wie bei LCP tauschen die Peers CONFREQs, CONFREJs, CONFNAKs und CONFACKs aus. In dieser Verhandlungsphase haben die Elemente, über die verhandelt wird, jedoch mit höheren Layer-Protokollen zu tun - IP, IPX, Bridging, CDP usw. Ein oder mehrere dieser Protokolle können ausgehandelt werden. Da es sich

hierbei um das am häufigsten verwendete Protokoll handelt und andere Protokolle auf die gleiche Weise arbeiten, steht das in RFC 1332 definierte Internet Protocol Control Protocol (IPCP) im Mittelpunkt dieser Diskussion. Weitere relevante RFCs sind u. a.:

- RFC1552 (IPX Control Protocol)
- RFC 1378 (AppleTalk Control Protocol)
- RFC1638 (Bridging Control Protocol)
- RFC 1762 (DECnet Control Protocol)
- RFC 1763 (Vines Control Protocol)

Darüber hinaus kann das Cisco Discovery Protocol Control Protocol (CDPCP) während des NCP ausgehandelt werden, obwohl dies nicht üblich ist. Cisco TAC-Techniker werden in der Regel empfehlen, den Befehl no cdp enable auf allen Dialer-Schnittstellen zu konfigurieren, um zu verhindern, dass CDP-Pakete einen Anruf auf unbestimmte Zeit weiterleiten.

Das Schlüsselelement, das in IPCP ausgehandelt wird, ist die Adresse jedes Peers. Jeder Peer befindet sich in einem von zwei möglichen Zuständen. entweder über eine IP-Adresse verfügen oder nicht. Wenn der Peer bereits über eine Adresse verfügt, sendet er diese Adresse in einem CONFREQ an den anderen Peer. Wenn die Adresse für den anderen Peer akzeptabel ist, wird ein CONFACK zurückgegeben. Wenn die Adresse nicht akzeptiert werden kann, ist die Antwort ein CONFNAK mit einer Adresse, die der Peer verwenden kann.

Wenn der Peer keine Adresse hat, sendet er ein CONFREQ mit der Adresse 0.0.0.0. Dies weist den anderen Peer an, eine Adresse zuzuweisen, die durch das Senden eines CONFNAK mit der richtigen Adresse erreicht wird.

Weitere Optionen können im IPCP ausgehandelt werden. Häufig werden die primären und sekundären Adressen für den Domänennamen-Server und den NetBIOS-Namenserver angezeigt, wie in Informational RFC 1877 beschrieben. Das IP Compression Protocol (RFC 1332) ist ebenfalls ein gängiges Protokoll.

Alternative PPP-Methoden

Alternative PPP-Methoden umfassen Multilink PPP, Multi-Chassis PPP und virtuelle Profile.

Multilink PPP

Die MLP-Funktion (Multilink Point-to-Point Protocol) bietet Load Balancing-Funktionen für mehrere WAN-Links. Gleichzeitig werden Interoperabilität, Paketfragmentierung und korrekte Sequenzierung sowie Lastberechnung für eingehenden und ausgehenden Datenverkehr von mehreren Anbietern bereitgestellt. Die Cisco Implementierung von Multilink PPP unterstützt die Spezifikationen für Fragmentierung und Paketsequenzierung in RFC 1717.

Multilink PPP ermöglicht die Fragmentierung von Paketen. Diese Fragmente können gleichzeitig über mehrere Point-to-Point-Links an dieselbe Remote-Adresse gesendet werden. Die verschiedenen Links werden als Reaktion auf einen von Ihnen definierten Dialer-Lastengrenzwert angezeigt. Die Last kann für eingehenden Datenverkehr, ausgehenden Datenverkehr oder je nach Bedarf für den Datenverkehr zwischen den einzelnen Standorten berechnet werden. MLP stellt Bandbreite bei Bedarf bereit und reduziert die Latenz bei der Übertragung über WAN-Verbindungen.

Multilink PPP arbeitet mit den folgenden Schnittstellentypen (Single oder Multiple), die so

konfiguriert sind, dass sie sowohl Dial-on-Demand-Rotationsgruppen als auch PPP-Kapselung unterstützen:

- asynchrone serielle Schnittstellen
- BRIs
- PRIs

Konfiguration

Um Multilink PPP auf asynchronen Schnittstellen zu konfigurieren, konfigurieren Sie die asynchronen Schnittstellen zur Unterstützung der DDR- und PPP-Kapselung. Anschließend konfigurieren Sie eine Dialer-Schnittstelle, um PPP-Kapselung, Bandbreite bei Bedarf und Multilink PPP zu unterstützen. Das Hinzufügen weiterer asynchroner Schnittstellen führt jedoch zu keiner Leistungssteigerung. Mit der MTU-Standardgröße sollte Multilink PPP drei asynchrone Schnittstellen mit V.34-Modems unterstützen. Pakete können jedoch gelegentlich verworfen werden, wenn die MTU-Größe klein ist oder wenn große Spitzen von kurzen Frames auftreten.

Um Multilink PPP auf einer einzigen ISDN BRI- oder PRI-Schnittstelle zu aktivieren, müssen Sie eine Dialer-Rotationengruppe nicht separat definieren, da ISDN-Schnittstellen standardmäßig Wählrotiergruppen sind. Wenn Sie keine PPP-Authentifizierungsverfahren verwenden, muss Ihr Telefondienst die Anrufer-ID-Informationen weitergeben.

Eine Lastengrenzwertnummer ist erforderlich. Ein Beispiel für die Konfiguration von Multilink PPP auf einer einzelnen ISDN BRI-Schnittstelle finden Sie im *Beispiel für Multilink PPP auf einer ISDN-Schnittstelle* unten.

Wenn Multilink PPP konfiguriert ist und Sie ein Multilink-Bündel unbegrenzt anschließen möchten, verwenden Sie den Befehl **Dialer idle-timeout**, um einen sehr hohen Inaktivitätszeitgeber festzulegen. Der Befehl **Dialer-load threshold 1** (**Dialer-Load-Grenzwert 1)** behält kein Multilink-Bündel von *n-Verbindungen unbegrenzt verbunden*, und der Befehl **Dialer-load threshold-2** behält kein Multilink-Bündel mit zwei Verbindungen unbegrenzt verbunden.

Um Multilink PPP auf mehreren ISDN BRI- oder PRI-Schnittstellen zu aktivieren, richten Sie eine Dialer-Rundschnittstelle ein und konfigurieren diese für Multilink PPP. Sie konfigurieren die BRIs dann separat und fügen sie jeweils derselben Rotationsgruppe hinzu. Siehe *Beispiel für Multilink-PPP an mehreren ISDN-Schnittstellen* unten.

Beispiel für Multilink-PPP an einer ISDN-Schnittstelle

Im folgenden Beispiel wird Multilink PPP auf der BRI-Schnittstelle 0 aktiviert. Wenn ein BRI konfiguriert wird, ist keine Konfiguration der Wählergruppen erforderlich (ISDN-Schnittstelle ist standardmäßig eine Rotationsgruppe).

```
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
```

Beispiel für Multilink PPP an mehreren ISDN-Schnittstellen

Im folgenden Beispiel werden mehrere ISDN-BRIs so konfiguriert, dass sie zur gleichen Wählrotationsgruppe für Multilink PPP gehören. Verwenden Sie den Befehl **Dialer-Rundgruppen**, um jeder ISDN-BRI dieser Wählrotiergruppe zuzuweisen, die der Nummer der Dialer-Schnittstelle entsprechen muss (in diesem Fall Nummer 0).

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

Multichassis Multilink PPP

Multilink PPP bietet die Möglichkeit, Pakete zu einem einzelnen Endsystem über eine logische Leitung (auch als *Bündel* bezeichnet) zu verteilen und neu zu kombinieren, die aus mehreren Verbindungen besteht. Multilink PPP bietet Bandbreite nach Bedarf und reduziert die Latenz bei der Übertragung über WAN-Verbindungen.

Multichassis Multilink PPP (MMP) hingegen bietet zusätzliche Funktionen für Verbindungen, die an mehreren Routern mit unterschiedlichen Remote-Adressen enden. MMP kann auch analogen und digitalen Datenverkehr verarbeiten.

Diese Funktion ist für Situationen vorgesehen, in denen es große Pools von Einwahlbenutzern gibt, in denen ein einzelner Zugriffsserver nicht genügend Einwahlports bereitstellen kann. Mit MMP können Unternehmen ihren Benutzern eine einzige Einwahlnummer bereitstellen und dieselbe Lösung auf analoge und digitale Anrufe anwenden. So können Internet-Dienstanbieter beispielsweise mehreren ISDN PRIs über mehrere Router eine einzige ISDN-Rufnummer zuweisen.

Eine vollständige Beschreibung der in diesem Dokument erwähnten MMP-Befehle finden Sie in der *Cisco Dial Solutions Command Reference*. Wenn Sie die Dokumentation anderer Befehle in diesem Kapitel anzeigen möchten, verwenden Sie den Master-Index für Befehlsreferenzen, oder suchen Sie online.

MMP wird von den Cisco Plattformen der Serien 7500, 4500 und 2500 sowie von synchronen seriellen, asynchronen Schnittstellen, ISDN BRI, ISDN PRI und Dialer unterstützt.

Für MMP ist keine Neukonfiguration der Telefongesellschaft-Switches erforderlich.

Konfiguration

Router oder Zugriffsserver sind so konfiguriert, dass sie zu Peer-Gruppen gehören, die als *Stack-Gruppen* bezeichnet werden. Alle Mitglieder der Stack-Gruppe sind Peers. Stack-Gruppen benötigen keinen permanenten Lead-Router. Jedes Stack-Gruppenmitglied kann Anrufe von einer einzigen Zugriffsnummer annehmen, bei der es sich in der Regel um eine ISDN PRI-Sammelgruppe handelt. Anrufe können von Remote-Benutzergeräten eingehen, z. B. von Routern, Modems, ISDN-Terminaladaptern oder PC-Karten.

Sobald eine Verbindung mit einem Mitglied einer *Stack-Gruppe* hergestellt wurde, ist dieser Teilnehmer Eigentümer des Anrufs. Wenn ein zweiter Anruf vom gleichen Client eingeht und ein anderer Router den Anruf entgegennimmt, stellt der Router einen Tunnel her und leitet alle zum Anruf gehörenden Pakete an den Router weiter, der den Anruf besitzt. Die Einrichtung eines Tunnels und die Weiterleitung von Anrufen an den Router, der den Anruf führt, werden manchmal als *Projektion der PPP-Verbindung an den Anrufermaster* bezeichnet.

Wenn ein leistungsfähigerer Router verfügbar ist, kann er als Mitglied der Stack-Gruppe konfiguriert werden, und die anderen Stack-Gruppenmitglieder können Tunnel einrichten und alle Anrufe an diesen weiterleiten. In diesem Fall beantworten die anderen Stack-Gruppenmitglieder lediglich Anrufe und leiten den Datenverkehr an den leistungsstärkeren *Offload*-Router weiter.

Hinweis: WAN-Leitungen mit hoher Latenz zwischen Stack-Gruppenelementen können den Stack-Gruppenbetrieb ineffizient gestalten.

Die Verarbeitung von MMP-Anrufen, die Gebote und die Layer-2-Weiterleitung in der Stack-Gruppe werden wie folgt ausgeführt. Sie ist auch in Abbildung 16-10 dargestellt.

1. Wenn der erste Anruf bei der Stack-Gruppe eingeht, antwortet Router A.
2. Bei der Ausschreibung gewinnt Router A, da er bereits den Anruf hat. Router A wird zum *Anrufmaster* für diese Sitzung mit dem Remote-Gerät. Router A kann auch als *Host für die Master-Bündelschnittstelle* bezeichnet werden.
3. Wenn das Remote-Gerät, das den Anruf initiiert hat, mehr Bandbreite benötigt, führt es einen zweiten Multilink PPP-Anruf an die Gruppe aus.
4. Wenn der zweite Anruf eingeht, beantwortet Router D diesen Anruf und informiert die Stack-Gruppe. Router A gewinnt das Angebot, da er die Sitzung bereits mit diesem Remote-Gerät verarbeitet.
5. Router D stellt einen Tunnel zu Router A her und leitet die PPP-Rohdaten an Router A weiter.
6. Router A reassembliert und sequenziert die Pakete.
7. Wenn mehr Anrufe an Router D eingehen und zu Router A gehören, vergrößert sich der Tunnel zwischen A und D, um den hinzugefügten Datenverkehr zu verarbeiten. Router D stellt keinen zusätzlichen Tunnel zu A her.
8. Wenn mehr Anrufe eingehen und von einem anderen Router beantwortet werden, erstellt dieser Router auch einen Tunnel zu A und leitet die ursprünglichen PPP-Daten weiter.
9. Die wieder zusammengestellten Daten werden im Unternehmensnetzwerk weitergegeben, als ob sie alle über eine physische Verbindung übertragen worden wären.

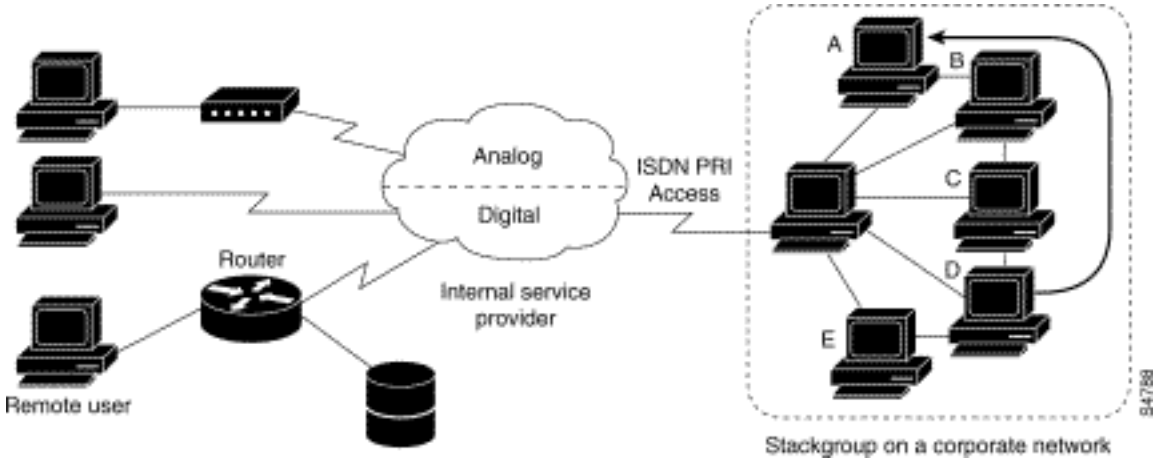

Abbildung 16-10: Typisches Multichassis Multilink PPP-Szenario

Im Gegensatz zur vorherigen Abbildung verfügt die Abbildung 16-11 über einen Offload-Router. Zugriff auf Server, die zu einer Stack-Gruppe gehören, die Anrufe entgegennehmen, Tunnel einrichten und Anrufe an einen Cisco 4700-Router weiterleiten, der die Ausschreibung gewinnt und der Anrufmaster für alle Anrufe ist. Die Cisco Serie 4700 reassembliert und sequenziert alle Pakete, die über die Stack-Gruppe eingehen.

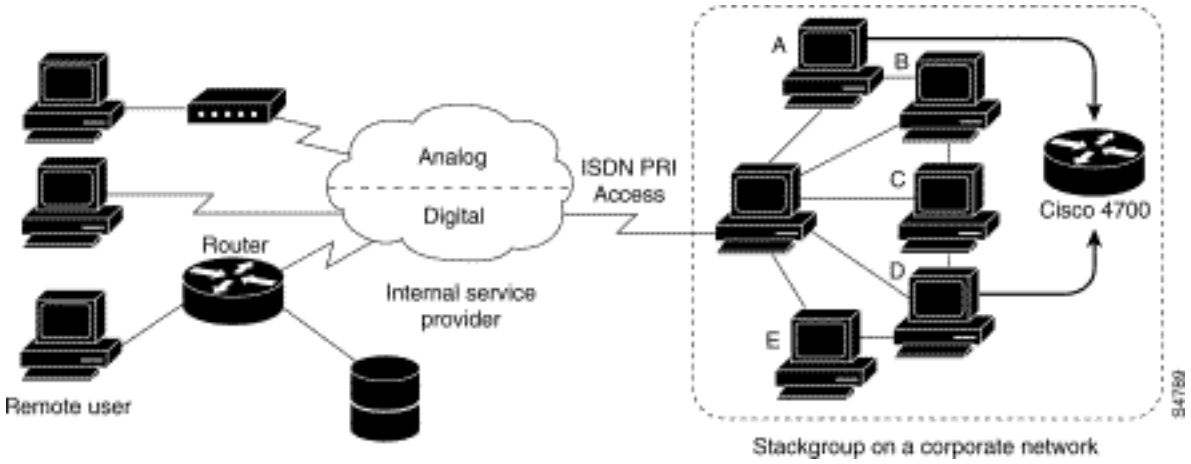

Abbildung 16-11: Multichassis Multilink PPP mit einem Offload-Router als Stack-Gruppenmitglied

Hinweis: Sie können Stack-Gruppen mithilfe verschiedener Zugriffs-Server-, Switching- und Router-Plattformen erstellen. Universal Access Server wie der Cisco AS5200 sollten jedoch nicht mit ISDN kombiniert werden. Dies sollte nur mit Zugriffsservern wie der 4x00-Plattform erfolgen. Da Anrufe von der Zentrale willkürlich zugewiesen werden, kann diese Kombination dazu führen, dass ein analoger Anruf an einen Server für den digitalen Zugriff weitergeleitet wird, der den Anruf nicht verarbeiten kann.

Für die MMP-Unterstützung einer Gruppe von Routern muss jeder Router so konfiguriert sein, dass er die folgenden Funktionen unterstützt:

- Multilink PPP
- Stack Group Biding Protocol (SGBP)
- Virtuelle Vorlage für die Konfiguration der Klonschnittstelle zur Unterstützung von MMP

Virtuelle Profile

Virtual Profiles ist eine einzigartige Point-to-Point Protocol (PPP)-Anwendung, die eine virtuelle

Zugriffsschnittstelle dynamisch erstellen und konfigurieren kann, wenn ein Einwahlanruf empfangen wird, und die Schnittstelle dynamisch beenden kann, wenn der Anruf beendet wird. Virtuelle Profile arbeiten mit einfachem PPP und Multilink PPP (MLP).

Die Konfigurationsinformationen für eine Virtual Profiles Virtual Access Interface können von einer virtuellen Vorlagenschnittstelle oder von einer benutzerspezifischen Konfiguration stammen, die auf einem AAA-Server (Authentication, Authorization, Accounting) oder auf beiden gespeichert ist.

Die von Virtual Profiles verwendete benutzerspezifische AAA-Konfiguration ist die *Schnittstellenkonfiguration* und wird während der LCP-Aushandlungen heruntergeladen. Eine weitere Funktion, die "Pro-Benutzer-Konfiguration" genannt wird, verwendet auch Konfigurationsinformationen, die von einem AAA-Server erfasst werden. Die benutzerspezifische Konfiguration verwendet jedoch die während der NCP-Verhandlungen heruntergeladene *Netzwerkkonfiguration* (z. B. Zugriffslisten und Routenfilter).

Die Konfiguration der virtuellen Zugriffsschnittstelle wird anhand von virtuellen Profilen, virtuellen Vorlagenschnittstellen und AAA-Konfigurationen anhand von zwei Regeln geregelt:

- Jede Anwendung für den virtuellen Zugriff kann über höchstens eine Vorlage zum Klonen verfügen. Es können jedoch mehrere AAA-Konfigurationen geklont werden (Virtual Profiles AAA-Informationen und AAA Per User Configuration, die wiederum die Konfiguration für mehrere Protokolle beinhalten können).
- Wenn virtuelle Profile von einer virtuellen Vorlage konfiguriert werden, hat ihre Vorlage eine höhere Priorität als jede andere virtuelle Vorlage.

Im Abschnitt "Interoperabilität mit anderen Cisco Wählfunktionen" unten finden Sie eine Beschreibung der möglichen Konfigurationssequenzen, die vom Vorhandensein oder Fehlen von MLP oder einer anderen virtuellen Zugriffsfunktion abhängen, die eine virtuelle Vorlagenschnittstelle klont.

Diese Funktion wird auf allen Cisco IOS-Plattformen ausgeführt, die MLP unterstützen.

Eine vollständige Beschreibung der in diesem Abschnitt erwähnten Befehle finden Sie im Kapitel "Befehle für virtuelle Profile" in der Befehlsreferenz für *Wählösungen* im Cisco IOS-Dokumentationssatz. Um die Dokumentation anderer Befehle zu finden, die in diesem Kapitel aufgeführt sind, können Sie den Master-Index für Befehlsreferenzen verwenden oder online suchen.

Hintergrundinformationen

Dieser Abschnitt enthält Hintergrundinformationen zu virtuellen Profilen, um Ihnen das Verständnis dieser Anwendung zu erleichtern, bevor Sie mit der Konfiguration beginnen.

Einschränkungen

Wir empfehlen die Verwendung nicht nummerierter Adressen in virtuellen Vorlagenschnittstellen, um sicherzustellen, dass auf virtuellen Zugriffsschnittstellen keine doppelten Netzwerkadressen erstellt werden.

Voraussetzungen

Die Verwendung benutzerspezifischer Informationen zur AAA-Schnittstellenkonfiguration mit Virtual Profiles erfordert die Konfiguration des Routers für AAA und die Verwendung benutzerspezifischer AV-Paare für die Schnittstellenkonfiguration durch den AAA-Server. Die relevanten AV-Paare (auf einem RADIUS-Server) beginnen wie folgt:

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

Bei den Informationen, die auf das Gleichheitszeichen (=) folgen, kann es sich um einen beliebigen Cisco IOS-Schnittstellenkonfigurationsbefehl handeln. Beispiel:

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

Für die Verwendung einer virtuellen Vorlagenschnittstelle mit virtuellen Profilen muss eine virtuelle Vorlage speziell für virtuelle Profile definiert werden.

Interoperabilität mit anderen Cisco Wählfunktionen

Virtuelle Profile sind mit Cisco DDR, Multilink PPP (MLP) und Dialern wie ISDN kompatibel.

DDR-Konfiguration physischer Schnittstellen

Virtuelle Profile sind in den folgenden DDR-Konfigurationsstatus vollständig mit physischen Schnittstellen kompatibel, wenn keine andere Anwendung für virtuelle Zugriffsschnittstellen konfiguriert wurde:

- Dialer-Profile werden für die Schnittstelle konfiguriert. Das Wählprofil wird anstelle der Konfiguration der virtuellen Profile verwendet.
- DDR ist auf der Schnittstelle nicht konfiguriert. Virtuelle Profile setzen die aktuelle Konfiguration außer Kraft.
- Legacy-DDR wird auf der Schnittstelle konfiguriert. Virtuelle Profile setzen die aktuelle Konfiguration außer Kraft.

Hinweis: Wenn eine Dialer-Schnittstelle (einschließlich eines ISDN-Dialers) verwendet wird, wird die Konfiguration auf der physischen Schnittstelle anstelle der Virtual Profiles-Konfiguration verwendet.

Multilink PPP-Effekt auf die Konfiguration der virtuellen Zugriffsschnittstelle

Wie in Tabelle 16-8 gezeigt, hängt die genaue Konfiguration einer virtuellen Zugriffsschnittstelle von den folgenden drei Faktoren ab:

- Legt fest, ob virtuelle Profile von Virtual Template, von AAA, von beiden oder von keinem der beiden konfiguriert werden. Diese Zustände werden in der Tabelle als "Nur VP VT", "nur VP AAA", "VP VT und VP AAA" bzw. "Kein VP überhaupt" angezeigt.
- Das Vorhandensein oder Fehlen einer Dialer-Schnittstelle.
- Vorhandensein oder Fehlen von MLP. Die Spaltenbezeichnung "MLP" ist ein Standin für alle virtuellen Zugriffsfunktionen, die MLP und Klone über eine virtuelle Vorlagenschnittstelle unterstützen.

In Tabelle 16-8 bedeutet "Multilink VT", dass eine virtuelle Vorlagenschnittstelle geklont wird,

wenn eine für MLP oder eine virtuelle Zugriffsfunktion, die MLP verwendet, definiert ist.

Tabelle 16-8: Konfigurationsklonsequenz für virtuelle Profile

Konfiguration virtueller Profile	MLP No Dialer	MLP-Dialer	Kein MLP No Dialer	Kein MLP Dialer
Nur VP VT	VP VT	VP VT	VP VT	VP VT
Nur VP AAA	(Multilink VT) VP AAA	(Multilink VT) VP AAA	VP AAA	VP AAA
VP VT und VP AAA	VP VT VP AAA	VP VT VP AAA	VP VT VP AAA	VP VT VP AAA
Kein VP	(Multilink VT)	Dialer	Es wird keine virtuelle Zugriffsschnittstelle erstellt.	Es wird keine virtuelle Zugriffsschnittstelle erstellt.

Die Reihenfolge der Elemente in jeder Zelle der Tabelle ist wichtig. Wenn VP VT über VP AAA angezeigt wird, bedeutet dies, dass zuerst die virtuelle Vorlage für virtuelle Profile auf der Schnittstelle geklont wird und dann die AAA-Schnittstellenkonfiguration für den Benutzer darauf angewendet wird. Die benutzerspezifische AAA-Schnittstellenkonfiguration fügt der Konfiguration hinzu und überschreibt alle in Konflikt stehenden physischen Schnittstellen oder Konfigurationsbefehle für virtuelle Vorlagen.

Interoperabilität mit anderen Funktionen, die virtuelle Vorlagen verwenden

Virtuelle Profile arbeiten auch mit virtuellen Zugriffsanwendungen zusammen, die eine virtuelle Vorlagenschnittstelle klonen. Jede Anwendung für den virtuellen Zugriff kann über höchstens eine Vorlage zum Klonen verfügen, jedoch aus mehreren AAA-Konfigurationen klonen.

Die Interaktion zwischen virtuellen Profilen und anderen virtuellen Vorlagenanwendungen erfolgt wie folgt:

- Wenn virtuelle Profile aktiviert und eine virtuelle Vorlage dafür definiert ist, wird die virtuelle Vorlage Virtual Profiles verwendet.
- Wenn virtuelle Profile nur über AAA konfiguriert werden (für virtuelle Profile ist keine virtuelle Vorlage definiert), kann die virtuelle Vorlage für eine andere Anwendung für den virtuellen Zugriff (z. B. VPDN) auf der virtuellen Zugriffsschnittstelle geklont werden.
- Eine virtuelle Vorlage wird ggf. vor der AAA-Konfiguration für virtuelle Profile oder der AAA-Konfiguration pro Benutzer auf eine virtuelle Zugriffsschnittstelle geklont. Die AAA-benutzerspezifische Konfiguration (falls verwendet) wird zuletzt angewendet.

Terminologie

In diesem Kapitel werden die folgenden neuen oder ungewöhnlichen Begriffe verwendet:

AV-Paar: Ein Konfigurationsparameter auf einem AAA-Server; Teil der Benutzerkonfiguration, die der AAA-Server als Reaktion auf benutzerspezifische Autorisierungsanfragen an den Router sendet. Der Router interpretiert jedes AV-Paar als Konfigurationsbefehl für einen Cisco IOS-Router und wendet die AV-Paare in der Reihenfolge an. In diesem Kapitel bezieht sich der Begriff AV-Paar auf einen Parameter für die Schnittstellenkonfiguration auf einem RADIUS-Server.

Ein AV-Paar für die Schnittstellenkonfiguration für virtuelle Profile kann folgende Formen annehmen:

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

Klonen: Erstellen und Konfigurieren einer virtuellen Zugriffsschnittstelle durch Anwenden von Konfigurationsbefehlen aus einer bestimmten virtuellen Vorlage. Die virtuelle Vorlage ist die Quelle für allgemeine Benutzerinformationen und routerabhängige Informationen. Das Ergebnis des Klonens ist eine virtuelle Zugriffsschnittstelle, die mit allen Befehlen in der Vorlage konfiguriert ist.

Virtual Access Interface: Instanz einer eindeutigen virtuellen Schnittstelle, die dynamisch erstellt wird und vorübergehend existiert. Virtuelle Zugriffsschnittstellen können von verschiedenen Anwendungen, z. B. virtuellen Profilen und virtuellen privaten DFÜ-Netzwerken, erstellt und konfiguriert werden.

Virtual Template Interface: Generische Schnittstellenkonfiguration für bestimmte Benutzer oder für einen bestimmten Zweck sowie Routerabhängige Informationen. Dies erfolgt in Form einer Liste von Cisco IOS-Schnittstellenbefehlen, die bei Bedarf auf die virtuelle Schnittstelle angewendet werden.

Virtuelles Profil: Instanz einer eindeutigen virtuellen Zugriffsschnittstelle, die dynamisch erstellt wird, wenn bestimmte Benutzer anrufen, und dynamisch beendet wird, wenn die Verbindung unterbrochen wird. Das virtuelle Profil eines bestimmten Benutzers kann über eine virtuelle Vorlagenschnittstelle, eine benutzerspezifische, auf einem AAA-Server gespeicherte Schnittstellenkonfiguration oder über eine virtuelle Vorlagenschnittstelle und eine benutzerspezifische Schnittstellenkonfiguration über AAA konfiguriert werden.

Die Konfiguration einer virtuellen Zugriffsschnittstelle beginnt mit einer virtuellen Vorlagenschnittstelle (sofern vorhanden), gefolgt von der Anwendung einer benutzerspezifischen Konfiguration für die Einwahlsitzung des jeweiligen Benutzers (sofern vorhanden).

Erläutertes Beispiel einer PPP-Verhandlung

In diesem Beispiel wird mit einem Ping eine ISDN-Verbindung zwischen den Routern *Montecito* und *Goleta hergestellt*. Beachten Sie, dass in diesem Beispiel zwar kein Timestamping vorhanden ist, es jedoch in der Regel empfohlen wird, den globalen Konfigurationsbefehlsdienst **Zeitstempel für die Debugdatetime msec** zu verwenden.

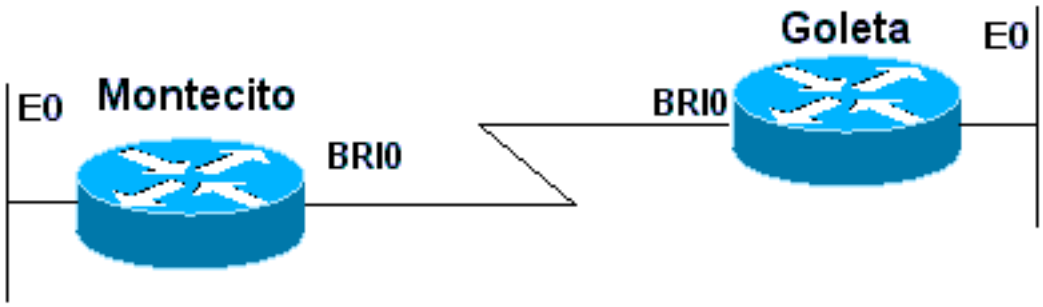

Abbildung 16-12: Router-ISDN-Router

Diese Debuggen werden von *Montecito* übernommen; Allerdings würde das Debuggen auf *Goleta* sehr ähnlich aussehen.

Hinweis: Ihre Debuggen können in einem anderen Format angezeigt werden. Diese Ausgabe ist das ältere PPP-Debugausgabeformat, bevor die Änderungen in IOS Version 11.2(8) eingeführt wurden. In Kapitel 17 finden Sie ein Beispiel für PPP-Debugging in neueren IOS-Versionen.

```
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 - Der Datenverkehr wird generiert, um einen Wählversuch zu initiieren.

B - Die Verbindung wird hergestellt (in diesem Beispiel werden ISDN-Debugger nicht verwendet).

LCP starten:

C - *Montecito* sendet LCP-Konfigurationsanforderungen für AUTHTYPE und für MAGICNUMBER.

D - *Goleta* sendet seine KONFREQs. Wenn der Wert für MAGICNUMBER mit dem von *Montecito* gesendeten Wert übereinstimmt, besteht eine hohe Wahrscheinlichkeit, dass die Linie Schleifen aufweist.

E - Dies zeigt an, dass *Montecito* Bestätigungen an *Goleta's* CONFREQs gesendet hat.

F - *Montecito* erhält CONFACKs von *Goleta*.

Begin der Authentifizierungsphase:

G, H - *Montecito* und *Goleta* fordern einander zur Authentifizierung heraus.

J - *Goleta* reagiert auf die Herausforderung.

K, L - *Goleta* erfolgreich authentifiziert.

M - Nachricht von *Goleta* nach *Montecito*: Authentifizierung erfolgreich.

NCP-Aushandlung beginnt:

N, P - Jeder Router sendet seine konfigurierte IP-Adresse in einer KONFREQUENZ.

Q, R - *Montecito* sendet eine KONFACK an *Goleta's* CONFREQ.

S - ? und umgekehrt.

T, U - Eine Route wird von *Montecito* nach *Goleta* installiert und das Protokoll auf der Schnittstelle ändert sich zu "up", was anzeigt, dass die NCP-Verhandlungen erfolgreich abgeschlossen wurden.

Vor dem Anruf beim Cisco Systems TAC Team

Bevor Sie das Cisco Systems Technical Assistance Center (TAC) anrufen, sollten Sie sich vergewissern, dass Sie dieses Kapitel durchgelesen und die für Ihr Systemproblem vorgeschlagenen Maßnahmen abgeschlossen haben.

Führen Sie außerdem die folgenden Schritte aus, und dokumentieren Sie die Ergebnisse, damit wir Ihnen besser helfen können:

Für alle Probleme sollten Sie die Ausgabe von **show running-config** und **show version** erfassen. Stellen Sie sicher, dass der Befehl **service timestamps debug datetime msec** in der Konfiguration vorhanden ist.

Sammeln Sie bei DDR-Problemen Folgendes:

- **Show Dialer Map**
- **Debug Dialer**
- **Debug-ppp-Aushandlung**
- **Debug-ppp-Authentifizierung**

Falls ISDN beteiligt ist, sammeln Sie Folgendes:

- **show isdn status**
- **debug isdn q931**
- **Debug-ISDN-Ereignisse**

Wenn Modems beteiligt sind, sammeln Sie Folgendes:

- Anzeigen von Zeilen
- show line [x]

- **Modem anzeigen** (wenn integrierte Modems beteiligt sind)
- **Modemversion anzeigen** (wenn integrierte Modems betroffen sind)
- **Debug-Modem**
- **debug modem csm** (wenn integrierte Modems beteiligt sind)
- **Debug-Chat** (bei einem DDR-Szenario)

Wenn T1s oder PRIs beteiligt sind, sammeln Sie Folgendes:

- **Show Controller t1**

Zugehörige Informationen

- Cisco IOS-Leitfaden für Wähllösungen
- Übersicht über Schnittstellen, Controller und Leitungen für den Einwahlzugriff
- Routing über Modemleitungen
- Konfiguration des seriellen Ports und des T1/E1-Trunks
- Entwerfen von DDR Internetworks
- Entscheidung und Vorbereitung für die DDR
- Konfigurieren von DDRtitle
- PPP-Technologie im Überblick
- Entwerfen von ISDN Internetworks
- ISDN-Switch-Typen, -Codes und -Werte
- Bereitstellung der ISDN-Leitung
- Technischer Support und Dokumentation - Cisco Systems