Tecnologia Dialup: Panoramiche e spiegazioni

Sommario

Introduzione

In questo capitolo vengono descritte alcune delle tecnologie utilizzate nelle reti di connessione remota. Sono disponibili suggerimenti per la configurazione e interpretazioni di alcuni comandi **show** che sono utili per verificare il corretto funzionamento della rete. Le procedure di risoluzione dei problemi esulano dall'ambito di questo documento e sono disponibili nel documento *Risoluzione dei problemi in remoto*.

Operazioni preliminari

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni

nei suggerimenti tecnici.

Prerequisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Operazioni modem

In questa sezione vengono illustrati i problemi relativi alla configurazione, alla verifica e all'utilizzo dei modem con router Cisco.

Uso del comando Modem Autoconfigure

Se si utilizza Cisco Internetwork Operating System (Cisco IOS) versione 11.1 o successive, è possibile configurare il router Cisco in modo che comunichi con il modem e lo configuri automaticamente.

Per configurare un router Cisco in modo che tenti automaticamente di individuare il tipo di modem collegato alla linea e quindi di configurare il modem, attenersi alla procedura descritta di seguito.

1. Per individuare il tipo di modem collegato al router, utilizzare il comando di configurazione della riga di **rilevamento della configurazione automatica del modem**.
2. Una volta individuato il modem, configurarlo automaticamente utilizzando il comando di configurazione **modem autoconfigure type** *nome-modem* line.

Per visualizzare l'elenco dei modem per cui il router ha delle voci, usare il comando **show modemcap** *modem-name*. Se si desidera modificare il valore di un modem restituito dal comando **show modemcap**, utilizzare il comando di configurazione riga di *valore* ***modemcap edit*** *modem-name attribute*.

Per informazioni complete sull'uso di questi comandi, consultare la *guida alla configurazione delle soluzioni di composizione della documentazione di Cisco IOS e la guida di riferimento ai comandi delle soluzioni di composizione*.

Nota: *non* immettere **&W** nella voce modemcap utilizzata per la configurazione automatica. In questo modo, la NVRAM verrà riscritta ogni volta che si esegue la configurazione automatica di un modem e il modem verrà eliminato.

Creazione di una sessione Telnet inversa su un modem

Per scopi diagnostici o per configurare inizialmente il modem se si esegue Cisco IOS versione

11.0 o precedenti, è necessario stabilire una sessione Telnet inversa per configurare un modem in modo che comunichi con un dispositivo Cisco. Finché si blocca la velocità del modem laterale dell'apparecchiatura terminale dati (DTE), il modem comunica sempre con il server di accesso o il router alla velocità desiderata. Fare riferimento alla Tabella 16-5 per informazioni sul blocco della velocità del modem. Accertarsi quindi che la velocità della periferica Cisco sia configurata prima di inviare i comandi al modem tramite una sessione Telnet inversa. Anche in questo caso, fare riferimento alla tabella 16-5 per informazioni sulla configurazione della velocità del server di accesso o del router.

Per configurare il modem per una sessione telnet inversa, utilizzare il comando di configurazione della riga **transport input telnet**. Per impostare un gruppo rotante (in questo caso, sulla porta 1), immettere il comando di configurazione della linea **rotary 1**. Se si inseriscono questi comandi nella configurazione della linea, IOS alloca i listener IP per le connessioni in ingresso negli intervalli di porte che iniziano con i seguenti numeri di base:

2000	protocollo Telnet
3000	protocollo Telnet con rotativo
4000	Protocollo TCP raw
5000	Protocollo TCP raw con rotary
6000	protocollo Telnet, modalità binaria
7000	protocollo Telnet, modalità binaria con rotazione
9000	protocollo Xremote
10000	Protocollo XRemote con rotativo

Per avviare una sessione Telnet inversa con il modem, effettuare le seguenti operazioni:

1. Dal terminale, usare il comando **telnet ip-address 20yy** dove *ip-address* è l'indirizzo IP di qualsiasi interfaccia attiva e connessa sul dispositivo Cisco e yy è il numero di linea a cui il modem è connesso.Ad esempio, il comando seguente permette di connettersi alla porta ausiliaria su un router Cisco 2501 con indirizzo IP 192.169.53.52: **telnet 192.169.53.52 2001**. In genere, un comando Telnet di questo tipo può essere emesso da qualsiasi punto della rete, se è possibile eseguire il **ping** dell'indirizzo IP in questione.**Nota:** sulla maggior parte dei router Cisco, la porta 01 è la porta ausiliaria. Su un server di accesso Cisco, la porta ausiliaria è l'ultima TTY +1. Ad esempio, la porta ausiliaria su uno switch 2511 è la porta 17 (16 porte TTY + 1). Utilizzare sempre il comando **show line** exec per trovare il numero di porta ausiliaria, in particolare sulle serie 2600 e 3600, che utilizzano numeri di porta non contigui per supportare moduli asincroni di dimensioni diverse.
2. Se la connessione viene rifiutata, è possibile che non vi sia alcun listener all'indirizzo e alla porta specificati o che un utente sia già connesso a tale porta. Verificare l'indirizzo di connessione e il numero di porta. Inoltre, accertarsi che il comando **modem in out** o **modem DTR-active** , così come il comando **transport input all**, siano visualizzati nella configurazione della linea per le linee raggiunte.Se si utilizza la funzione rotary, assicurarsi che il comando *rotary n* venga visualizzato anche nella configurazione della linea, dove n è il numero del gruppo rotary. Per verificare se un utente è già connesso, connettersi al router in modalità telnet e utilizzare il comando **show line** n. Cercare un asterisco per indicare che la linea è in uso. Assicurarsi che CTS sia alto e DSR no. Utilizzare il comando **clear line *n*** per disconnettere la sessione corrente dalla porta n. Se la connessione viene ancora rifiutata, è

possibile che il modem richieda continuamente il rilevamento della portante (CD). Scollegare il modem dalla linea, stabilire una sessione Telnet inversa e quindi collegare il modem.

3. Dopo aver effettuato correttamente la connessione Telnet, immettere AT e assicurarsi che il modem risponda con OK.
4. Se il modem non risponde, fare riferimento alla tabella seguente.

La tabella 16-1 seguente delinea le possibili cause dei sintomi dei problemi di connettività da modem a router e descrive le soluzioni a tali problemi.

Tabella 16-1: Nessuna connettività tra modem e router

Possibili cause	Azioni consigliate

Il controllo del modem non è abilitato sul server o sul router di accesso	1. Usare il comando **show line** exec sul server o sul router di accesso. L'output per la porta ausiliaria deve essere visualizzato **InOut** o **RIisCD** nella colonna Modem. Ciò indica che il controllo del modem è abilitato sulla linea del server o del router di accesso. Per una spiegazione dell'output della **riga di comando**, vedere "Uso dei comandi di debug" nel capitolo 15.
	2. Configurare la linea per il controllo del modem utilizzando il comando di configurazione della linea di **inout del modem**. Il controllo del modem è ora abilitato sul server di accesso.
	Esempio: Nell'esempio seguente viene illustrato come configurare una linea per le chiamate in entrata e in uscita:
	`line 5`
	`modem inout`
	Nota: accertarsi di utilizzare il comando **modem inout** e non il comando **modem dialin** quando la connettività del modem è in dubbio. Quest'ultimo comando consente alla riga di accettare solo chiamate in ingresso. Le chiamate in uscita verranno rifiutate e sarà impossibile stabilire una sessione Telnet con il modem per configurarlo. Se si desidera utilizzare il comando **modem dialin**, eseguire questa operazione solo dopo aver verificato il corretto funzionamento del modem.

Il modem potrebbe non essere configurato	Immettere **AT&FE1Q0** per ripristinare le impostazioni predefinite e verificare che il modem sia impostato sui caratteri echo e restituisca l'output. Il modem potrebbe avere una sessione sospesa. Utilizzare "**^U**" per cancellare la linea e "**^Q**" per aprire il controllo del flusso (XON). Verificare le impostazioni di

correttamente o avere una sessione bloccata.	parità.
Cablaggio non corretto	1. Controllare il cablaggio tra il modem e il server o il router di accesso. Verificare che il modem sia collegato alla porta ausiliaria sul server di accesso o sul router con un cavo RJ-45 e un adattatore DB-25 MMOD. Questa configurazione di cablaggio è consigliata e supportata da Cisco per le porte RJ-45. (Questi connettori sono in genere chiamati "Modem"). 2. Per verificare la correttezza del cablaggio, usare il comando **show line** exec. Vedere la spiegazione dell'output del comando **show line** nel capitolo 15 della sezione "Uso dei comandi di debug".
Problema hardware	1. Verificare che i cavi utilizzati siano corretti e che tutte le connessioni siano funzionanti. 2. Verificare che tutto l'hardware non sia danneggiato, inclusi i cavi (fili rotti), gli adattatori (pin allentati), le porte del server di accesso e il modem. 3. Per ulteriori informazioni sulla risoluzione dei problemi hardware, vedere il capitolo 3, "Risoluzione dei problemi hardware e di avvio".

Utilizzo dei gruppi di rotazione

Per alcune applicazioni, i modem su un determinato router devono essere condivisi da un gruppo di utenti. Cisco Dialout Utility è un esempio di questo tipo di applicazione. In pratica, gli utenti si connettono a una porta che li connette a un modem disponibile. Per aggiungere una linea asincrona a un gruppo rotante, immettete **rotary *n*** dove *n* è il numero del gruppo rotante nella configurazione della linea asincrona. Fare riferimento all'esempio riportato di seguito.

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

La configurazione della linea sopra descritta consente agli utenti di connettersi al gruppo rotante immettendo **telnet 192.169.53.52 3001** per telnet normale. Le alternative includono le porte 5001 per TCP raw, 7001 per telnet binario (utilizzato da Cisco Dialout Utility) e 10001 per le connessioni Xremote.

Nota: per verificare la configurazione di Cisco Dialout Utility, fare doppio clic sull'icona dell'utility nella parte inferiore destra della schermata e premere il pulsante More>. Quindi, premere il pulsante Configure Ports>. Verificare che la porta sia compresa nell'intervallo 7000, se si utilizzano gruppi rotanti, e nell'intervallo 6000, se l'utilità Dialout ha come destinazione un singolo modem. È inoltre consigliabile attivare la registrazione tramite modem sul PC. A tale scopo, selezionare la sequenza seguente: **Start->Pannello di controllo-> Modem**->(scegliere il modem Cisco Dialout)->**Proprietà**->**Connessione**->**Avanzate**...->**Registrare un file registro**.

Interpretazione di Show Line Output

L'output del comando **show line *-number*** exec è utile per risolvere i problemi di connessione tra modem e server di accesso o router. Di seguito viene riportato l'output del comando **show line**.

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

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

Quando si verificano problemi di connettività, viene visualizzato un output importante nei campi

Stato modem e Stato hardware modem.

Nota: il campo Stato hardware modem non viene visualizzato nell'output **show line** per ciascuna piattaforma. In alcuni casi, le indicazioni per gli stati del segnale verranno visualizzate nel campo Stato modem.

La Tabella 16-2 mostra le stringhe tipiche dello stato del modem e dello stato dell'hardware del modem come risultato del comando **show line**. Spiega anche il significato di ogni stato.

Tabella 16-2: Stati di modem e hardware modem in Mostra output di linea

Stato modem	Stato hardware modem	Significato
Inattivo	CTS noDSR DTR RTS	Questi sono gli stati appropriati del modem per le connessioni tra un server o un router di accesso e un modem (quando non è presente alcuna chiamata in arrivo). Output di qualsiasi altro tipo generalmente indica un problema.
Pronto	-	Se lo stato del modem è Pronto, anziché Inattivo, considerare quanto segue: 1. Il controllo del modem non è configurato sul server o sul router di accesso. Configurare il server o il router di accesso con il comando di configurazione in linea **inout del modem**. 2. Sessione sulla linea. Se desiderato, utilizzare il comando **show users** exec e il comando **clear line** privileged exec per interrompere la sessione. 3. DSR è elevato. Questo può essere dovuto a due motivi: Problemi di cablaggio. Se il connettore utilizza il pin 6 DB-25 e non ha il pin 8, è necessario spostare il pin da 6 a 8 o ottenere il connettore appropriato.Il modem configurato per DCD è sempre alto. Il modem deve essere riconfigurato in modo da avere un solo CD(1) con DCD alto. Questa operazione viene in genere eseguita con il comando **&C1** modem, ma per informazioni sulla sintassi esatta del modem, vedere la documentazione

		del modem. Se il software in uso non supporta il controllo del modem, è necessario configurare la linea del server di accesso a cui il modem è connesso con il comando di configurazione **no exec** line. Cancellare la riga con il comando **clear line** privileged exec, avviare una sessione Telnet inversa con il modem e riconfigurare il modem in modo che DCD sia alto solo su CD. Per terminare la sessione Telnet, immettere **disconnect** e riconfigurare la riga del server di accesso con il comando exec line configuration.
Pronto	noCTS noDSR DTR RTS(2)	La stringa noCTS viene visualizzata nel campo Stato hardware modem per uno dei quattro motivi seguenti: 1. Il modem è spento. 2. Il modem non è collegato correttamente al server di accesso. Controllare le connessioni del modem al server di accesso. 3. Cablaggio errato (MDCE a rulli o MDTE diritto, ma senza lo spostamento dei pin). La configurazione di cablaggio consigliata è illustrata nella tabella precedente. 4. Il modem non è configurato per il controllo del flusso hardware. Utilizzare il comando **no flowcontrol hardware** line configuration per disabilitare il controllo del flusso hardware sul server di accesso. Quindi attivare il controllo del flusso hardware sul modem tramite una sessione Telnet inversa. Consultare la documentazione del modem e la sezione "Impostazione di una sessione Telnet inversa su un modem" più indietro in questo capitolo. Riattivare il controllo del flusso hardware sul server di accesso con il comando **flowcontrol hardware** line configuration.
Pronto	CTS DSR DTR RT	La stringa DSR (anziché la stringa noDSR) viene visualizzata nel campo Stato hardware modem per uno dei motivi seguenti: 1. Cablaggio errato (MDCE a rulli o MDTE diritto, ma senza lo spostamento dei pin). La configurazione di cablaggio

	S(2)	consigliata è illustrata nella tabella precedente. 2. Il modem è configurato per DCD sempre in alto. Riconfigurare il modem in modo che il DCD sia alto solo su CD. Questa operazione viene in genere eseguita con il comando **&C1** modem, ma per informazioni sulla sintassi esatta del modem, vedere la documentazione del modem. Configurare la riga del server di accesso a cui è connesso il modem con il comando di configurazione **no exec** line. Cancellare la riga con il comando **clear line** privileged exec, avviare una sessione Telnet inversa con il modem e riconfigurare il modem in modo che DCD sia alto solo su CD. Per terminare la sessione Telnet, immettere **disconnect**. Riconfigurare la riga del server di accesso con il comando exec line configuration.
Pronto	CTS* DSR* DTR RTS(2)	Se questa stringa viene visualizzata nel campo Stato hardware modem, è probabile che il controllo del modem non sia abilitato sul server di accesso. Utilizzare il comando **modem inout** line configuration per attivare il controllo del modem sulla linea. Ulteriori informazioni sulla configurazione del controllo del modem su un server di accesso o su una linea di router sono fornite nelle sezioni precedenti di questa tabella.

(1) CD = Rilevamento portante

(2) Un * accanto a un segnale indica uno dei due elementi seguenti: Il segnale è cambiato negli ultimi secondi oppure non è utilizzato dal metodo di controllo del modem selezionato.

Raccolta delle informazioni sulle prestazioni del modem

In questa sezione vengono illustrati i metodi per la raccolta dei dati sulle prestazioni dei modem digitali MICA disponibili nella famiglia di server di accesso Cisco AS5x00. I dati sulle prestazioni possono essere utilizzati per l'analisi delle tendenze e sono utili per la risoluzione dei problemi di prestazioni che possono verificarsi. Se si guardano i numeri presentati di seguito, bisogna ricordare che la perfezione non è possibile nel mondo reale. La possibile percentuale di successo delle chiamate (CSR) è una funzione della qualità dei circuiti, della base utenti del modem client e dell'insieme di modulazioni utilizzate. Una tipica percentuale di CSR per chiamate V.34 è del 95%. Per le chiamate V.90 è prevista una connessione riuscita il 92% delle volte. È probabile che cadano premature il 10% delle volte.

Utilizzare i comandi seguenti per ottenere una vista generale del comportamento del modem sul server di accesso:

- **mostra modem**
- **mostra riepilogo modem**
- **mostra velocità di connessione del modem**
- **show modem call-stats**

Le informazioni seguenti sono utili per la risoluzione dei problemi relativi a una singola connessione modem o per la raccolta di dati per l'analisi delle tendenze:

- debug modem csm
- modem call-record terse
- mostra modem op (MICA) / AT@E1 (Microcom) durante la connessione
- mostra registro modem per la sessione di interesse dopo la disconnessione
- ANI (numero chiamante)
- Ora
- Versione hardware/firmware del modem client
- Informazioni interessanti dal client (dopo la disconnessione): ATI6, ATI11, AT&V, AT&V1 e così via
- Registrazione audio (file .wav) del tentativo di addestramento dal modem client

Nelle sezioni seguenti, i comandi verranno spiegati più dettagliatamente e verranno descritte alcune tendenze comuni.

Mostra modem/Mostra riepilogo modem

Il comando **show modem** permette di visualizzare i singoli modem. Da questi numeri è possibile visualizzare lo stato dei singoli modem.

```
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%
```

Per visualizzare i numeri aggregati di tutti i modem sul router, usare il comando **show modem summary**.

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

Tabella 16-3: Mostra campi modem

Campi	Descrizioni
Chiamate in arrivo e in uscita	Chiamate in ingresso e in uscita dal modem. • Utilizzo: percentuale del tempo di attività totale del sistema in cui tutti i modem sono in uso. • Succ - Totale chiamate connesse. • Non riuscito - Totale chiamate non riuscite. • Disp. - Totale modem disponibili per l'utilizzo nel sistema.
Occupato	Numero totale di volte in cui i modem sono stati messi fuori servizio con il comando **modem occupato** o il comando **modem shutdown**.
Composizione non riuscita	Numero totale di tentativi di disconnessione dei modem o assenza di segnale.
Nessuna Ans	Numero totale di volte in cui è stata rilevata una chiamata di chiamata, ma un modem non ha risposto alle chiamate.
Pct.	Percentuale di connessioni riuscite del totale di modem disponibili.

[Mostra output stato chiamata modem]

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

Tabella 16-4. Mostra campi statistiche chiamate modem

rmt Link	Ciò indica che la correzione degli errori era attiva e che la chiamata è stata interrotta dal sistema client collegato al modem remoto.
hostDrop	Ciò indica che la chiamata è stata interrotta dal sistema host IOS. Alcuni dei motivi più comuni sono: timeout di inattività, circuito non protetto dalla compagnia telefonica o termineq LCP PPP del client. Il modo migliore per determinare la causa della disconnessione consiste nell'utilizzare il

	terminale di registrazione delle chiamate del modem o l'accounting AAA.

Gli altri motivi di disconnessione dovrebbero ammontare a meno del 10% del totale.

Mostra output velocità connessione modem

```
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
```

Prevediamo una distribuzione delle velocità V.34. Se i T1 utilizzano il sistema di segnalazione associato al canale (CAS, Channel Associated Signaling), il picco dovrebbe essere 26,4. Per ISDN (PRI) T1, il picco dovrebbe essere a 31.2. Inoltre, cercare alcune velocità K56Flex, V.90. Se non sono presenti connessioni V.90, è possibile che si sia verificato un problema di topologia di rete.

Informazioni sul comando Modem Call-Record Terse (11.3AA/12.0T)

Piuttosto che un comando exec, si tratta di un comando di configurazione posizionato a livello di sistema del server di accesso in questione. Quando un utente si disconnette, viene visualizzato un messaggio simile al seguente:

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

Comando Show Modem Operational-Status

Il comando exec **show modem operating-status** permette di visualizzare i parametri correnti (o più recenti) relativi alla connessione del modem.

La documentazione relativa a questo comando è disponibile nella *guida di riferimento dei comandi di Cisco IOS versione 12.0 Dial Solutions*. **show modem operating-status** è solo per modem MICA. Il comando equivalente per i modem Microcom è **modem at-mode / AT@E1**. Utilizzare il comando **modem at-mode <slot>/<porta>** per connettersi al modem, quindi eseguire il comando **AT@E1**. La documentazione completa per il comando **modem at-mode** è disponibile nella *guida alla configurazione del software Cisco AS5300*, mentre la documentazione per il comando **AT@E1** è disponibile nella guida di riferimento dei comandi *AT Command Set and Register Summary for Microcom Modem Modules*.

Per determinare i modem utilizzati da un utente, attenersi alla procedura descritta di seguito.

1. Eseguire il comando **show user** e cercare il server TTY a cui sono connessi.
2. Usare il comando **show line** per cercare i numeri di slot/porta del modem.

Raccolta dei dati sulle prestazioni lato client

Per l'analisi delle tendenze è molto importante raccogliere dati sulle prestazioni lato client. Cercare sempre di ottenere le seguenti informazioni:

- versione hardware/firmware del client (ottenibile con il comando **ATI3I7** sul modem del client)
- motivi di disconnessione segnalati dal client (utilizzare **ATI6** o **AT&V1**)

Altre informazioni disponibili sul lato client includono i file modemlog.txt e ppplog.txt del PC. È necessario configurare il PC per la generazione di questi file.

Analisi dei dati delle prestazioni

Dopo aver raccolto e compreso i dati sulle prestazioni del sistema modem, è necessario esaminare i modelli e i componenti rimanenti che potrebbero richiedere miglioramenti.

Problemi con determinati modem server

Utilizzare **show modem** o **show modem call-status** per identificare i modem che presentano una frequenza eccessivamente alta di errori di training o una frequenza di disconnessione errata (MICA). Se si verificano problemi con coppie di modem adiacenti, è probabile che il DSP sia bloccato/inattivo. Per il ripristino, usare il **modem flash copy** sull'HMM interessato. Accertarsi che sui modem sia in esecuzione l'ultima versione di portware. Per verificare che tutti i modem siano configurati correttamente, usare il comando di configurazione **modem autoconfigure type mica/microcom_server** nella configurazione della linea. Per verificare che i modem siano configurati automaticamente quando una chiamata viene interrotta, usare il comando exec **debug confmodem**. Per risolvere i problemi relativi a una configurazione errata dei modem, potrebbe essere necessario stabilire una sessione Telnet inversa.

Problemi con particolari DS0s

I problemi DS0 sono rari, ma possibili. Per individuare i DS0s malfunzionanti, usare il comando **show controller t1 call-counters** e cercare i DS0s con TotalCalling anormalmente alto e TotalDuration anormalmente basso. Per individuare i DS0s di cui si sospetta la presenza, potrebbe essere necessario occupare altri DS0s con il comando di configurazione **isdn service dsl, ds0 busyout** sotto l'interfaccia seriale per T1. L'output dei **contatori di chiamata t1 di show controller** è simile al seguente:

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

Ovviamente, in questo caso, la timeslot 3 è il canale sospetto.

Tendenze comuni aggiuntive

Di seguito sono riportate alcune delle tendenze più comuni rilevate da Cisco TAC.

1. Percorsi di circuito non validiÈpossibile che vengano rilevati percorsi di circuito errati attraverso la rete PSTN (Public Switched Telephone Network) se si verificano i problemi seguenti:problemi nelle chiamate interurbane, ma non nelle chiamate locali (o viceversa)le chiamate in determinati orari hanno problemidifficoltà per le chiamate provenienti da scambi remoti specifici
2. Problemi relativi alle chiamate interurbaneSe il servizio a lunga distanza non funziona correttamente o non funziona affatto (ma il servizio locale è corretto):Accertarsi che la linea digitale sia collegata a uno switch digitale, non a una banca di canali.Chiedere alle compagnie telefoniche di esaminare i percorsi di circuito utilizzati per le lunghe distanze.
3. Problemi relativi alle chiamate provenienti da aree di chiamata specifiche.Se le chiamate da aree geografiche o scambi specifici tendono ad avere problemi, è necessario rivolgersi alla società telefonica per la topologia di rete.Se sono necessarie più conversioni da analogico a digitale, le connessioni modem V.90/K56flex non saranno possibili e V.34 potrebbe risultare leggermente degradato. Le conversioni da analogico a digitale sono necessarie nelle aree servite da switch digitali non integrati o da switch analogici.

Operazioni ISDN

Per ISDN si intende un insieme di servizi digitali disponibili per gli utenti finali. La connessione ISDN comporta la digitalizzazione della rete telefonica in modo che voce, dati, testo, grafica, musica, video e altre fonti possano essere fornite agli utenti finali da un unico terminale attraverso i cavi telefonici esistenti. I sostenitori dell'ISDN immaginano una rete mondiale simile all'attuale rete telefonica, ma con una trasmissione digitale e una varietà di nuovi servizi.

L'ISDN è un progetto volto a standardizzare i servizi degli utenti, le interfacce utente/rete e le funzionalità di rete e interrete. La standardizzazione dei servizi per gli utenti cerca di garantire un livello di compatibilità internazionale. La standardizzazione dell'interfaccia utente/rete stimola lo sviluppo e la commercializzazione di queste interfacce da parte di produttori terzi. La standardizzazione delle funzionalità di rete e interrete contribuisce a raggiungere l'obiettivo della connettività globale, garantendo che le reti ISDN possano comunicare facilmente tra loro.

Le applicazioni ISDN includono applicazioni per immagini ad alta velocità (come il fax del Gruppo IV), linee telefoniche aggiuntive utilizzate in casa per il settore del telelavoro, trasferimento di file ad alta velocità e videoconferenze. La voce, ovviamente, è anche un'applicazione molto diffusa per le reti ISDN.

Il mercato dell'accesso domestico è attualmente suddiviso in varie tecnologie. Nelle aree in cui sono disponibili tecnologie più recenti e meno costose, come DSL e Cable, il mercato domestico si sta allontanando dalla linea ISDN. Le aziende, tuttavia, continuano a utilizzare l'ISDN sotto forma di PRI T1/E1 per trasportare grandi quantità di dati o per fornire accesso dial v.90.

Componenti ISDN

I componenti ISDN includono terminali, schede di terminazione di rete, apparecchiature di terminazione di linea e apparecchiature di terminazione di scambio. I terminali ISDN sono di due

tipi. I terminali ISDN specializzati sono chiamati terminali di tipo 1 (TE1). I terminali non ISDN, come il DTE che precede gli standard ISDN, sono chiamati terminali di tipo 2 (TE2). Gli TE1 si connettono alla rete ISDN attraverso un collegamento digitale a quattro fili e doppino intrecciato. TE2s si connette alla rete ISDN attraverso una scheda terminale. ISDN TA può essere un dispositivo standalone o una scheda all'interno di TE2. Se TE2 è implementato come dispositivo standalone, si collega all'AT tramite un'interfaccia standard a livello fisico. Gli esempi includono EIA/TIA-232-C (in precedenza RS-232-C), V.24 e V.35.

Oltre ai dispositivi TE1 e TE2, il punto di connessione successivo nella rete ISDN è il dispositivo con terminazione di rete di tipo 1 (NT1) o 2 (NT2). Questi sono dispositivi di terminazione di rete che connettono il cablaggio dell'utente a quattro fili all'anello locale a due fili convenzionale. In Nord America, NT1 è un dispositivo CPE (Customer Premise Equipment). Nella maggior parte delle altre parti del mondo, NT1 fa parte della rete fornita dal vettore. Il NT2 è un dispositivo più complesso, che si trova in genere nei PBX (Digital Private Branch Exchange), che esegue funzioni di protocollo di layer 2 e 3 e servizi di concentrazione. Esiste anche un dispositivo NT1/2; è un singolo dispositivo che combina le funzioni di un NT1 e di un NT2.

In ISDN sono specificati diversi punti di riferimento. Questi punti di riferimento definiscono le interfacce logiche tra gruppi funzionali, quali AT e NT1. I punti di riferimento ISDN includono:

- R-Punto di riferimento tra apparecchiature non ISDN e TA
- S-Il punto di riferimento tra i terminali utente e NT2
- T - Il punto di riferimento tra le periferiche NT1 e NT2
- U - Il punto di riferimento tra i dispositivi NT1 e le apparecchiature di terminazione di linea nella rete portante. Il punto di riferimento U è rilevante solo in Nord America, dove la funzione NT1 non è fornita dalla rete portante

Di seguito è riportato un esempio di configurazione ISDN. In questo esempio vengono mostrati tre dispositivi collegati a uno switch ISDN nell'ufficio centrale. Due di questi dispositivi sono compatibili con ISDN, quindi possono essere collegati tramite un punto di riferimento S ai dispositivi NT2. Il terzo dispositivo (un telefono standard non ISDN) viene collegato tramite il punto di riferimento R a un AT. Ognuna di queste periferiche può anche essere collegata a una periferica NT1/2, che sostituirebbe sia NT1 che NT2. Inoltre, anche se non sono visualizzate, stazioni utente simili sono collegate allo switch ISDN di estrema destra.

Esempio di configurazione ISDN

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

Current configuration:
!
version 11.1
service timestamps debug datetime msec
service udp-small-servers
service tcp-small-servers
!
hostname 2503B
!
!
username 2503A password
ip subnet-zero
isdn switch-type basic-5ess
!
interface Ethernet0
```

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

2503B#
```

Servizi ISDN

Il servizio ISDN Basic Rate Interface (BRI) offre due canali B e un canale D (2B+D). Il servizio del canale B BRI funziona a 64 kbps ed è destinato a trasmettere i dati degli utenti; Il servizio del canale D BRI funziona a 16 kbps ed è destinato a trasportare informazioni di controllo e segnalazione, anche se può supportare la trasmissione dei dati utente in determinate circostanze. Il protocollo di segnalazione del canale D comprende i livelli da 1 a 3 del modello di riferimento OSI. BRI fornisce anche il controllo del frame e altro overhead, portando il suo bit rate totale a 192 kbps. La specifica del livello fisico BRI è International Telecommunication Union Telecommunication Standardisation Sector (ITU-T; già Comitato consultivo per il telegrafo e il telefono internazionali (CCITT) I.430.

Il servizio PRI (Primary Rate Interface) ISDN offre 23 canali B e un canale D in Nord America e Giappone, con un bit rate totale di 1,544 Mbps (il canale D PRI funziona a 64 kbps). ISDN PRI in Europa, Australia e in altre parti del mondo fornisce 30 MB più un canale D a 64 kbps e una velocità di interfaccia totale di 2,048 Mbps. La specifica del livello fisico PRI è ITU-T I.431.

Livello 1

I formati dei frame del livello fisico ISDN (livello 1) variano a seconda che il frame sia in uscita (da un terminale alla rete) o in entrata (da una rete al terminale). Entrambe le interfacce dei livelli fisici sono mostrate nella Figura 16-1.

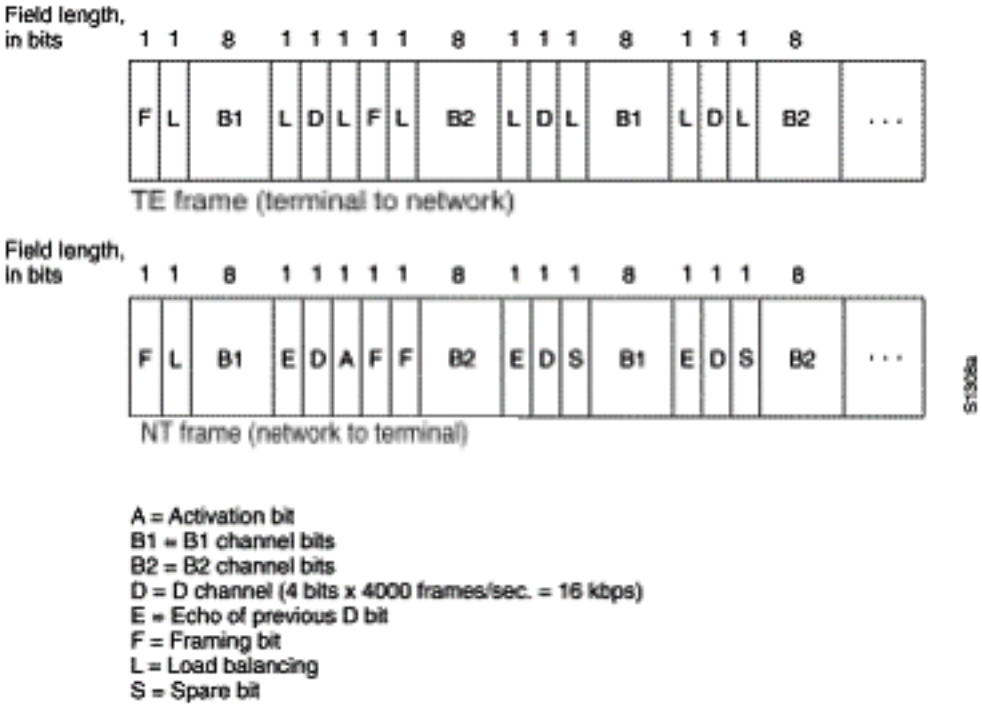

Figura 16-1: Formati frame livello fisico ISDN

I frame sono lunghi 48 bit, di cui 36 bit rappresentano i dati. I bit di un frame del livello fisico ISDN vengono utilizzati come segue:

- F - Consente la sincronizzazione.
- L - Regola il valore bit medio.
- E - Utilizzato per la risoluzione dei conflitti quando più terminali su un bus passivo si contendono un canale.
- A - Attiva le periferiche.
- S - Non assegnato.
- B1, B2 e D: per i dati utente.

Èpossibile collegare fisicamente più dispositivi utente ISDN a un circuito. In questa configurazione, si possono verificare collisioni se due terminali trasmettono contemporaneamente. Pertanto, ISDN fornisce delle funzioni per determinare la contesa dei collegamenti. Quando un NT riceve un bit D dall'TE, il bit torna indietro nella posizione E-bit successiva. Il TE si aspetta che il bit E successivo sia lo stesso dell'ultimo bit D trasmesso.

I terminali non possono trasmettere nel canale D a meno che non rilevino un numero specifico di segnali (che indica "nessun segnale") corrispondente a una priorità prestabilita. Se il TE rileva un bit nel canale echo (E) diverso dai bit D, deve interrompere immediatamente la trasmissione. Questa semplice tecnica assicura che solo un terminale possa trasmettere il proprio messaggio D alla volta. Dopo un'efficace trasmissione del messaggio HD, la priorità del terminale viene ridotta in quanto prima della trasmissione è necessario rilevare altre trasmissioni continue. I terminali non possono aumentare la priorità fino a quando tutti gli altri dispositivi della stessa linea non hanno avuto l'opportunità di inviare un messaggio D. Le connessioni telefoniche hanno una priorità più alta di tutti gli altri servizi e le informazioni di segnalazione hanno una priorità più alta rispetto alle informazioni di non segnalazione.

Livello 2

Il layer 2 del protocollo di segnalazione ISDN è Link Access Procedure sul canale D, noto anche come LAPD. La funzione LAPD è simile alle HDLC (High-Level Data Link Control) e LAPB (Link Access Procedure, Procedura di accesso ai collegamenti, Bilanciato). Come indica l'espansione dell'abbreviazione LAPD, questa viene utilizzata attraverso il canale D per garantire che le informazioni di controllo e segnalazione fluiscano e vengano ricevute correttamente. Il formato del frame LAPD (vedere Figura 16-2) è molto simile a quello di HDLC e, come HDLC, LAPD utilizza i frame di supervisione, di informazione e senza numero. Il protocollo LAPD è formalmente specificato in ITU-T Q.920 e ITU-T Q.921.

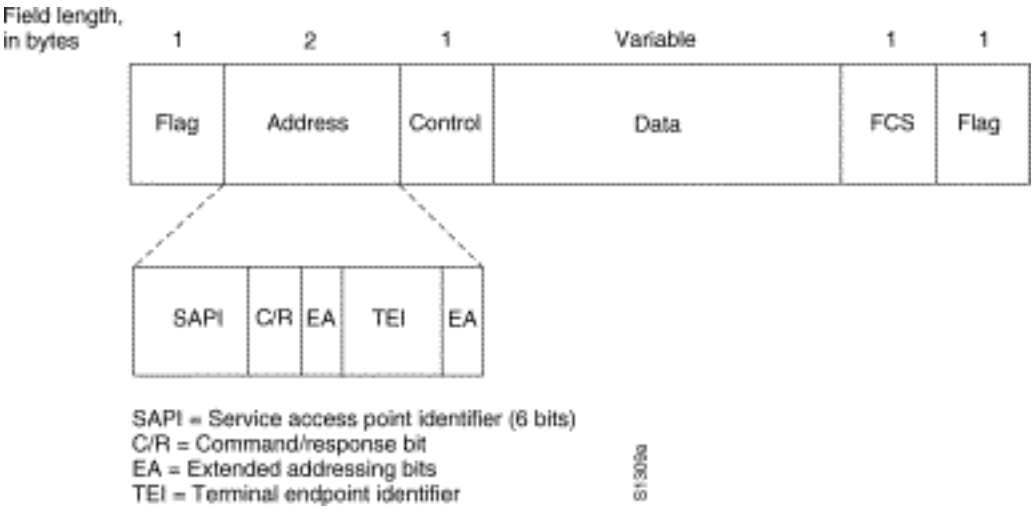

Figura 16-2: Formato frame LAPD

I campi Contrassegno e Controllo LAPD sono identici a quelli di HDLC. Il campo Indirizzo LAPD può avere una lunghezza di 1 o 2 byte. Se il bit dell'indirizzo esteso del primo byte è impostato, l'indirizzo è 1 byte; se non è impostato, l'indirizzo è di 2 byte. Il primo byte del campo indirizzo contiene l'identificatore del punto di accesso al servizio (SAPI), che identifica il portale in cui i servizi LAPD vengono forniti al layer 3. Il bit C/R indica se il frame contiene un comando o una risposta. Il campo TEI (Terminal Endpoint Identifier) identifica uno o più terminali. Un TEI di tutti indica una trasmissione.

Livello 3

Per la segnalazione ISDN vengono utilizzate due specifiche di layer 3: ITU-T (in precedenza CCITT) I.450 (noto anche come ITU-T Q.930) e ITU-T I.451 (noto anche come ITU-T Q.931). Insieme, questi protocolli supportano connessioni utente-utente, a commutazione di circuito e a commutazione di pacchetto. Vengono specificati diversi tipi di messaggi, tra cui SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS e DISCONNECT.

Questi messaggi sono funzionalmente simili a quelli forniti dal protocollo X.25 (per ulteriori informazioni, vedere il Capitolo 19, "Risoluzione dei problemi relativi alle connessioni X.25"). La Figura 16-3, tratta da ITU-T I.451, mostra le fasi tipiche di una chiamata ISDN a commutazione di circuito.

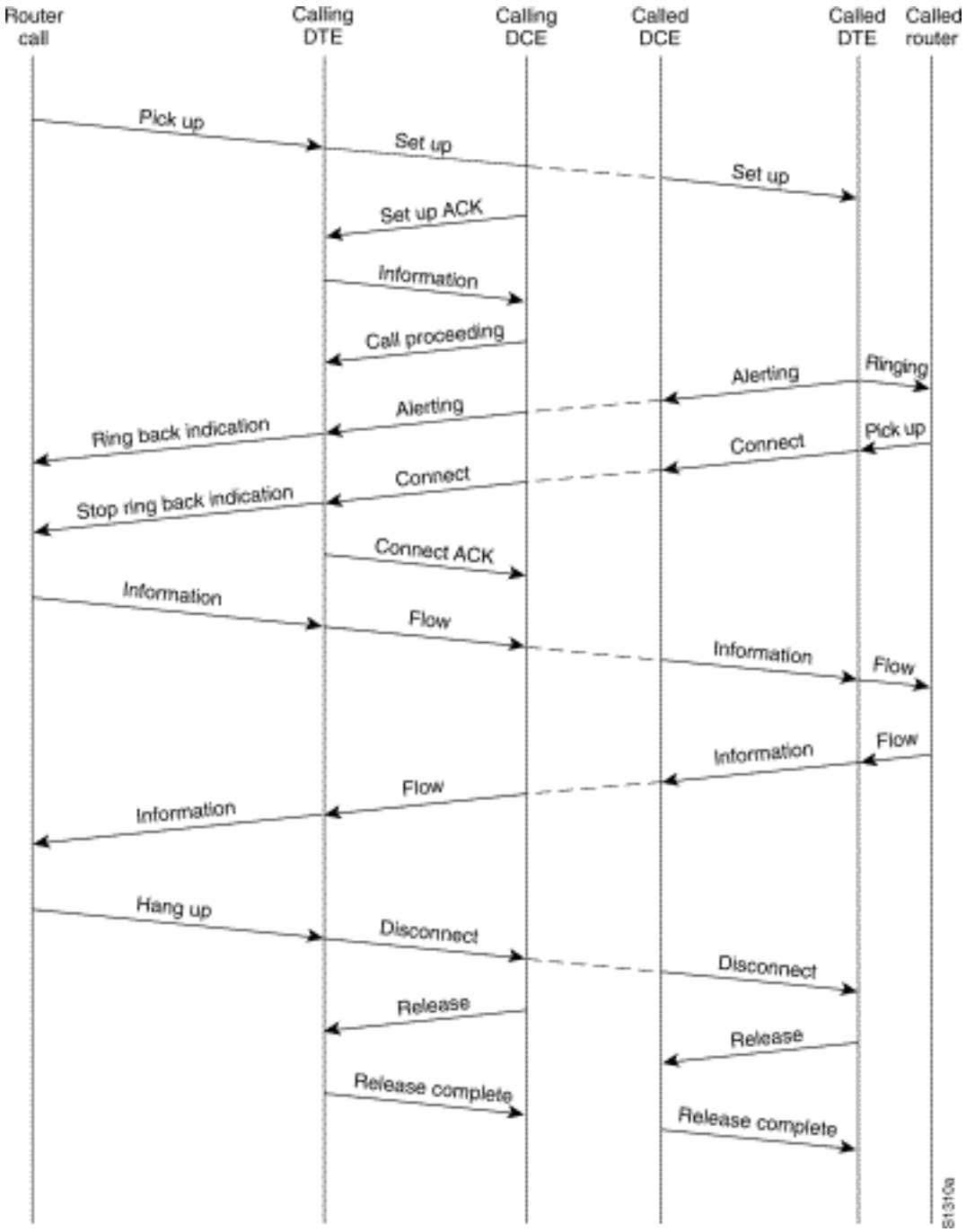

Figura 16-3. Stadi di chiamata con commutazione di circuito ISDN

Interpretazione dell'output Show ISDN Status

Per verificare la condizione corrente della connessione ISDN tra il router e lo switch della società di telefonia, usare il comando **show isdn status**. I due tipi di interfacce supportati da questo comando sono BRI e 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
```

Tabella 16-5:- mostra stato isdn per BRI

Campo	Importanza
Stato livello 1: DISATTIVATO	Ciò indica che l'interfaccia BRI non visualizza alcun segnale sulla linea. Le cause possibili sono cinque. • L'interfaccia BRI è chiusa. Controllare la configurazione del comando **shutdown** nell'interfaccia BRI o cercare un'indicazione disattivata a livello amministrativo dal comando **show interface**. Usare l'utility di configurazione e immettere **no shutdown** nell'interfaccia BRI. Immettere il comando **clear interface bri** al prompt di exec per verificare che l'interfaccia BRI venga riavviata. • Problema con il cablaggio. Sarà necessario sostituire il cavo. Utilizzare un cavo RJ-45 straight-through. Per controllare il cavo, tenere le estremità del cavo RJ-45 fianco a fianco. Se i pin sono nello stesso ordine, il cavo è diritto. Se l'ordine dei pin è invertito, il cavo viene arrotolato. Sostituire il cavo. • La porta ISDN BRI di un router potrebbe richiedere un dispositivo NT1. In ISDN, NT1 è un dispositivo che fornisce l'interfaccia tra le apparecchiature della sede del cliente e le apparecchiature di commutazione degli uffici centrali. Se il router non dispone di un NT1 interno, ottenere e collegare un NT1 alla porta BRI. Assicurarsi che l'adattatore BRI o terminale sia collegato alla porta S/T di NT1. Consultare la documentazione del produttore per verificare il corretto funzionamento di NT1 esterno. • La linea potrebbe non funzionare. Contattare il vettore per confermare il

	funzionamento della connessione e per verificare le impostazioni del tipo di switch. • Verificare che il router funzioni correttamente. In caso di guasto o malfunzionamento dell'hardware, sostituire se necessario.

Stato livello 2: Stato = TEI_ASSIGNMENT	Controllare l'impostazione del tipo di interruttore e SPIDS. L'impostazione dello switch ISDN specifica dell'interfaccia ha la precedenza sull'impostazione dello switch globale. Lo stato SPID indica se lo switch ha accettato il SPIDS (valido o non valido). Contattare il provider di servizi per verificare l'impostazione configurata sul router. Per modificare le impostazioni SPID, usare il comando di configurazione dell'interfaccia **isdn *spidn***. Dove *n* è 1 o 2, a seconda del canale in questione. Utilizzare la forma **no** di questo comando per rimuovere lo SPID specificato.
	`isdn spidn spid-number [ldn]`
	`no isdn spidn spid-number [ldn]`
	Descrizione sintassi:
	`spid-number`
	Numero che identifica il servizio a cui è stata effettuata la sottoscrizione. Questo valore viene assegnato dal provider di servizi ISDN e in genere è un numero telefonico di 10 cifre con cifre aggiuntive.
	`ldn`
	(Facoltativo) LDN (Local Directory Number), un numero di 7 cifre assegnato dal provider di servizi. Lo switch nel messaggio di installazione in arrivo fornisce queste informazioni. Se non si include la directory locale, l'accesso allo switch è consentito, ma l'altro canale B potrebbe non essere in grado di ricevere chiamate in ingresso. Per visualizzare le negoziazioni di layer 2 tra lo switch e il router, usare il comando **debug isdn q921** in modalità di esecuzione privilegiata. I debug di q921 sono documentati nella *guida di riferimento dei comandi di debug*. Poiché i debug dipendono in larga misura dalle risorse della CPU, è necessario prestare attenzione quando vengono utilizzati.

```
5200-1# show isdn status
Global ISDN Switchtype = primary-5ess
ISDN Serial0:23 interface
        dsl 0, interface ISDN Switchtype = primary-5ess
    Layer 1 Status:
```

```
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    The Free Channel Mask:  0x807FFFFF
    Total Allocated ISDN CCBs = 0
5200-1#
```

Se il comando **show isdn status** non funziona o non visualizza il PRI, provare a usare il comando **show isdn service**. Verificare che il comando **pri-group** venga visualizzato nella configurazione sotto il controller T1/E1 nella configurazione. Se il comando non è presente, configurare il controller con il comando **pri-group**.

L'esempio seguente mostra una configurazione di un router Cisco con un controller T1/PRI canalizzato:

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

Tabella 16-6: show isdn status per PRI

Campo	Importanza
Stato livello 1: DISATTIVATO	Ciò indica che l'interfaccia PRI non vede il frame T1/E1 sulla linea. Considerare le possibili cause seguenti per questa condizione: • L'interfaccia PRI è chiusa. Controllare la configurazione del comando **shutdown** nell'interfaccia serial0:23 o cercare un'indicazione disattivata a livello amministrativo dal comando **show interface**. Usare l'utility di configurazione e immettere **no shutdown** nell'interfaccia in questione. Immettere il comando **clear controller T1/E1** *n* al prompt di exec per assicurarsi che l'interfaccia PRI venga riavviata. • Problema con il cablaggio. Sarà necessario sostituire il cavo. Utilizzare un cavo RJ-45 straight-through. Per controllare il cavo, tenere le estremità del cavo RJ-45 fianco a fianco. Se i pin sono nello stesso ordine, il cavo è diritto. Se l'ordine dei pin è invertito, il cavo viene arrotolato. Sostituire il cavo. • La linea potrebbe non funzionare.

	Contattare il vettore per confermare il funzionamento della connessione e per verificare le impostazioni del tipo di switch. • Verificare che il router funzioni correttamente. In caso di guasto o malfunzionamento dell'hardware, sostituire se necessario.
Stato livello 2: Stato = TEI_ASSIGNMENT	Controllare l'impostazione switchtype. L'impostazione dello switch ISDN specifica dell'interfaccia ha la precedenza sull'impostazione dello switch globale. Verificare che T1/E1 sia configurato in modo da corrispondere allo switch del provider (i problemi di T1/E1 sono trattati nel Capitolo 15). Per visualizzare le negoziazioni di layer 2 tra lo switch e il router, usare il comando **debug isdn q921** in modalità di esecuzione privilegiata. I debug di q921 sono documentati nella *guida di riferimento dei comandi di debug*. Poiché i debug dipendono in larga misura dalle risorse della CPU, è necessario prestare attenzione quando vengono utilizzati.
Numero di chiamate / blocchi di controllo delle chiamate in uso / totale blocchi di controllo delle chiamate ISDN allocati	Questi numeri indicano il numero di chiamate in corso e il numero di risorse allocate per supportare tali chiamate. Se il numero di BCC assegnate è superiore al numero di BCC utilizzate, si consideri che potrebbe esserci un problema nel rilasciare le BCC. Accertarsi che siano disponibili CCB per le chiamate in arrivo.

Routing su chiamata su richiesta: Operazioni interfaccia dialer

Il routing DDR (Dial on Demand Routing) è un metodo per fornire la connettività WAN a costi contenuti in base alle necessità, come collegamento principale o come backup per un collegamento seriale non di composizione.

Per **interfaccia dialer** si intende un'interfaccia router in grado di effettuare o ricevere una chiamata. Questo termine generico deve essere distinto dal termine **interfaccia Dialer** (con la lettera D maiuscola), che si riferisce a un'interfaccia logica configurata per controllare una o più interfacce fisiche di un router e che viene visualizzata in una configurazione router come interfaccia Dialer X. A partire da questo punto, se non diversamente specificato, utilizzeremo il termine dialer nel suo

significato generico.

La configurazione dell'interfaccia dialer è disponibile in due versioni: dialer map-based (talvolta denominati DDR legacy) e profili dialer. Il metodo da utilizzare dipende dalle circostanze in cui è necessaria la connettività di composizione. Il DDR basato su mappa dialer è stato introdotto per la prima volta in IOS versione 9.0, i profili dialer in IOS versione 11.2.

Attivazione di una composizione

Alla base, il DDR è solo un'estensione del routing in cui *i pacchetti interessanti* vengono indirizzati a un'interfaccia dialer, innescando un tentativo di composizione. Nelle sezioni seguenti vengono illustrati i concetti relativi alla definizione di traffico interessante e viene spiegato il routing utilizzato per le connessioni DDR.

Pacchetti interessanti

Interessante è il termine usato per descrivere pacchetti o traffico che attiveranno un tentativo di composizione o, se un collegamento è già attivo, reimposteranno il timer di inattività sull'interfaccia della connessione. Per considerare interessante un pacchetto:

- il pacchetto deve soddisfare i criteri di "autorizzazione" definiti da un elenco degli accessi
- l'elenco degli accessi deve essere referenziato dall'elenco dei dialer o il pacchetto deve essere di un protocollo universalmente autorizzato dall'elenco dei dialer
- l'elenco di composizione deve essere associato a un'interfaccia di composizione utilizzando un gruppo di composizione

Per impostazione predefinita, i pacchetti non vengono mai considerati automaticamente interessanti. Le definizioni dei pacchetti interessanti devono essere dichiarate esplicitamente in una configurazione di router o server di accesso.

Gruppo dialer

Per configurare ciascuna interfaccia di connessione sul router o sul server di accesso, occorre usare un comando **dialer-group**. Se il comando **dialer-group** non è presente, non vi è alcun collegamento logico tra le definizioni del pacchetto interessante e l'interfaccia. La sintassi del comando:

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

Il numero di gruppo è il numero del gruppo di accesso dialer a cui appartiene l'interfaccia specifica. Questo gruppo di accesso viene definito con il comando **dialer-list**. I valori accettabili sono diversi da zero e sono numeri interi positivi compresi tra 1 e 10.

Un'interfaccia può essere associata solo a un singolo gruppo di accesso dialer; l'assegnazione di più gruppi di dialer non è consentita. Una seconda assegnazione di gruppo di accesso dialer sostituirà la prima. Per definire un gruppo di accesso dialer, usare il comando **dialer-group**. Il comando **dialer-list** associa un elenco degli accessi a un gruppo di accesso dialer.

I pacchetti corrispondenti al gruppo di dialer specificato attivano una richiesta di connessione.

L'indirizzo di destinazione del pacchetto viene valutato sulla base dell'elenco degli accessi

specificato nel comando **dialer-list** associato. Se l'esito è positivo, viene avviata una chiamata (se non è già stata stabilita una connessione) oppure viene reimpostato il timer di inattività (se è attualmente connessa una chiamata).

Elenco dialer

Il comando di configurazione globale **dialer-list** viene usato per definire un elenco di dialer DDR per controllare la composizione per protocollo o per combinazione di protocollo e elenco degli accessi. I pacchetti interessati sono quelli che corrispondono ai permessi a livello di protocollo o che sono permessi dall'elenco nel comando **dialer-list**: **dialer-list** *dialer-group* **protocol** *nome-protocollo* **{allow | nega | list** *access-list-number* **| access-group}**

dialer-group è il numero di un gruppo di accesso dialer identificato in un comando di configurazione dell'interfaccia dialer-group.

protocol-name è una delle seguenti parole chiave del protocollo: appletalk, bridge, clns, clns_es, clns_is, decnet, decnet_router-L1, decnet_router-L2, decnet_node, ip, ipx, vines o xns.

allow consente di accedere a un intero protocollo.

nega nega l'accesso a un intero protocollo.

list specifica che verrà utilizzato un elenco degli accessi per definire una granularità più fine di un intero protocollo.

access-list-number: numeri degli elenchi degli accessi specificati in elenchi standard o estesi DECnet, Banyan VINES, IP, Novell IPX o XNS, inclusi gli elenchi degli accessi e i tipi di bridging di Novell IPX Extended Service Access Point (SAP). Vedere la Tabella 16-7 per i tipi e i numeri degli elenchi degli accessi supportati.

nome dell'elenco dei filtri dei *gruppi di accesso* utilizzato nei comandi **clns filter-set** e **clns access-group**.

Tabella 16-7: Numerazione Degli Elenchi Degli Accessi Per Protocollo

Tipo di elenco accessi	Intervallo numeri elenco accessi (decimale)
AppleTalk	600-699
Banyan VINES (standard)	1-100
Banyan VINES (esteso)	101-200
DECnet	300-399
IP (standard)	1-99
IP (esteso)	100-199
Novell IPX (standard)	800-899
Novell IPX (esteso)	900-999
Bridging trasparente	200-299
XNS	500-599

Elenco accessi

Èpossibile configurare un elenco degli accessi per ogni protocollo di rete da inviare tramite la connessione remota. Ai fini del controllo dei costi, è in genere consigliabile configurare un elenco degli accessi in modo da impedire a determinati traffici, ad esempio gli aggiornamenti del routing, di attivare o mantenere una connessione. Si noti che quando si creano elenchi degli accessi allo scopo di definire il traffico interessante e non interessante, non si dichiara che i pacchetti non interessanti non possono attraversare il collegamento di composizione. Stiamo solo indicando che non resetteranno il timer di inattività, né porteranno una connessione da soli. Finché la connessione remota è attiva, i pacchetti non interessanti potranno comunque passare attraverso il collegamento.

Ad esempio, un router che esegue EIGRP come protocollo di routing può avere un elenco degli accessi configurato in modo da dichiarare i pacchetti EIGRP non interessanti e tutto il resto del traffico IP interessante:

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

Èpossibile configurare gli elenchi degli accessi per tutti i protocolli che potrebbero attraversare il collegamento di composizione. Tenere presente che, per impostazione predefinita, in assenza di un'istruzione **access-list allow** per un protocollo, viene rifiutato tutto il traffico. Se non è presente alcun elenco degli accessi e nessun comando **dialer-list** permette il protocollo, il protocollo non sarà interessante. In pratica, se non ci sono dialer list per un protocollo, quei pacchetti non passeranno attraverso il collegamento.

Esempio - Unire Il Tutto

Con tutti gli elementi posizionati, è possibile esaminare il processo completo in base al quale viene determinato lo stato "interessante" di un pacchetto. Nell'esempio, IP e IPX sono i protocolli che possono attraversare il collegamento di composizione. L'utente desidera impedire che trasmissioni e aggiornamenti di routing avviino una chiamata o mantengano attivo il collegamento.

```
!
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
!
```

Per essere considerato *interessante*, un pacchetto deve essere autorizzato dalle istruzioni **access-list 121** prima di attraversare l'**interfaccia asincrona 1**. In questo caso, i pacchetti EIGRP, come tutti gli altri pacchetti broadcast, vengono rifiutati, mentre tutto il resto del traffico IP viene autorizzato. Tenere presente che ciò non impedisce ai pacchetti EIGRP di attraversare il collegamento. Significa solo che questi pacchetti non reimposteranno il timer di inattività o non avvieranno un tentativo di composizione.

Analogamente, **access-list 903** dichiara che le richieste IPX RIP, SAP e GNS non sono interessanti, mentre tutto il resto del traffico IPX è interessante. Senza queste istruzioni deny, la connessione telefonica probabilmente non si interromperebbe mai e il risultato sarebbe una bolletta telefonica molto grande, poiché pacchetti di questo tipo vengono trasmessi costantemente su una rete IPX.

Con **dialer-group 7** configurato sull'interfaccia asincrona, sappiamo che **dialer-list 7** è necessario per collegare i filtri del traffico interessanti (ossia, gli elenchi degli accessi) all'interfaccia. È richiesta un'istruzione **dialer-list** (è possibile configurarne *solo* una) per ciascun protocollo, verificando che il numero dell'elenco di dialer corrisponda al numero del gruppo di dialer sull'interfaccia.

Ancora una volta, è importante ricordare che le istruzioni *deny* negli elenchi degli accessi configurati per definire il traffico interessante ***non*** impediranno ai pacchetti negati di attraversare il collegamento.

Utilizzando il comando **debug dialer**, è possibile visualizzare l'attività che attiva un tentativo di composizione:

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

Qui vediamo che il traffico IP con indirizzo di origine 172.16.1.111 e indirizzo di destinazione 172.16.2.22 ha attivato un tentativo di composizione sull'interfaccia Async1.

Routing

Una volta definiti, i pacchetti interessanti devono essere indirizzati correttamente per poter avviare una chiamata. Il processo di instradamento dipende da due fattori: le voci della tabella di routing e un'interfaccia "verso l'alto" attraverso la quale instradare i pacchetti.

Interfacce - up/up (spoofing)

Per instradare i pacchetti verso e attraverso un'interfaccia, quest'ultima deve essere nello stato attivo/attivo, come mostrato nell'output **show interfaces**:

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

Cosa succede a un'interfaccia di connessione non connessa? Se il protocollo non è attivo e in esecuzione sull'interfaccia, l'implicazione è che l'interfaccia stessa non sarà attiva. Le route che si basano sull'interfaccia verranno scaricate dalla tabella di routing e il traffico non verrà indirizzato a tale interfaccia. Di conseguenza, l'interfaccia non avvierà alcuna chiamata.

La soluzione per contrastare questa possibilità è consentire lo stato **up/up (spoofing)** per le interfacce dialer. Qualsiasi interfaccia può essere configurata come interfaccia dialer. Ad esempio, un'interfaccia seriale o asincrona può essere trasformata in una dialer aggiungendo il comando **dialer in-band** o **dialer dtr** alla configurazione dell'interfaccia. Queste linee non sono necessarie per le interfacce che per loro natura sono interfacce dialer (BRI e PRI). L'output di un'interfaccia show sarà simile al seguente:

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

In altre parole, l'interfaccia "finge" di essere **su/su** in modo che i percorsi associati rimangano in vigore e i pacchetti possano essere indirizzati all'interfaccia.

In alcune circostanze l'interfaccia della connessione telefonica non può essere **attiva/attiva (spoofing)**. L'output **show interface** può visualizzare l'interfaccia disattivata a livello amministrativo:

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

Disattivazione amministrativa significa semplicemente che l'interfaccia è stata configurata con il comando **shutdown**. Questo è lo stato predefinito di tutte le interfacce del router quando il router viene avviato per la prima volta. Per risolvere questo problema, usare il comando di configurazione dell'interfaccia **no shutdown**.

L'interfaccia può anche apparire in modalità standby:

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

Questo stato indica che l'interfaccia è stata configurata come backup per un'altra interfaccia. Quando una connessione richiede ridondanza in caso di errore, è possibile impostare un'interfaccia di connessione come backup. A tale scopo, aggiungere i comandi seguenti all'interfaccia della connessione primaria:

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

Dopo aver configurato il comando **backup interface**, l'interfaccia utilizzata come backup viene messa in modalità standby finché l'interfaccia primaria non raggiunge lo stato **down/down**. A questo punto, l'interfaccia di connessione configurata come backup passerà allo stato **attivo/attivo (spoofing)** in attesa di un evento di composizione.

Route statiche e route statiche mobili

Il modo più sicuro per indirizzare i pacchetti a un'interfaccia dialer è con il routing statico. Queste route vengono immesse manualmente nella configurazione del router o del server di accesso con il comando:

maschera prefisso ***route ip*** ***{****address* ***|*** *interface****}*** ***[****distanza****]***

prefisso : Prefisso della route IP per la destinazione.

maschera: Maschera di prefisso per la destinazione.

Indirizzo : Indirizzo IP dell'hop successivo che può essere utilizzato per raggiungere la rete di destinazione.

interfaccia: Interfaccia di rete da utilizzare per il traffico in uscita.

distanza : (Facoltativo) Distanza amministrativa. Questo argomento viene utilizzato nelle route statiche mobili.

Le route statiche vengono utilizzate nelle situazioni in cui il collegamento di composizione è l'unica connessione al sito remoto. Una route statica ha un valore di distanza amministrativa pari a uno (1), che la rende preferibile rispetto alle route dinamiche alla stessa destinazione.

D'altra parte, le route statiche mobili, ovvero le route statiche con una distanza amministrativa predefinita, vengono in genere utilizzate in scenari di backup DDR. In questi scenari, un protocollo di routing dinamico, ad esempio RIP o EIGRP, instrada i pacchetti attraverso il collegamento primario.

Èpreferibile un percorso statico normale (distanza amministrativa = 1) rispetto all'EIGRP (distanza amministrativa = 90) o al RIP (distanza amministrativa = 120). Il percorso statico determina il routing dei pacchetti sulla linea di composizione, anche se il router primario è attivo e in grado di passare il traffico. Tuttavia, se il percorso statico è configurato con una distanza amministrativa superiore a quella di uno dei protocolli di routing dinamico in uso sul router, il percorso statico mobile verrà utilizzato solo in assenza di un percorso "migliore", ovvero uno con una distanza amministrativa inferiore.

Se il DDR di backup viene richiamato con il comando **backup interface**, la situazione è leggermente diversa. Poiché l'interfaccia della connessione telefonica rimane in modalità standby mentre la connessione primaria è **attiva**, è possibile configurare una route statica o una route statica mobile. L'interfaccia di connessione non tenterà di stabilire una connessione fino a quando l'interfaccia primaria non **si spegne o non si spegne**.

Per una determinata connessione, il numero di route statiche (o statiche mobili) necessarie è una funzione dell'indirizzamento sulle interfacce dialer. Nei casi in cui le due interfacce dialer (una su ciascuno dei due router) condividono una rete o una subnet comune, in genere è necessaria una sola route statica. Punta alla LAN remota usando l'indirizzo dell'interfaccia di connessione del router remoto come indirizzo dell'hop successivo.

Esempi

Esempio 1: Dial è l'unica connessione che utilizza interfacce numerate. È sufficiente un percorso.

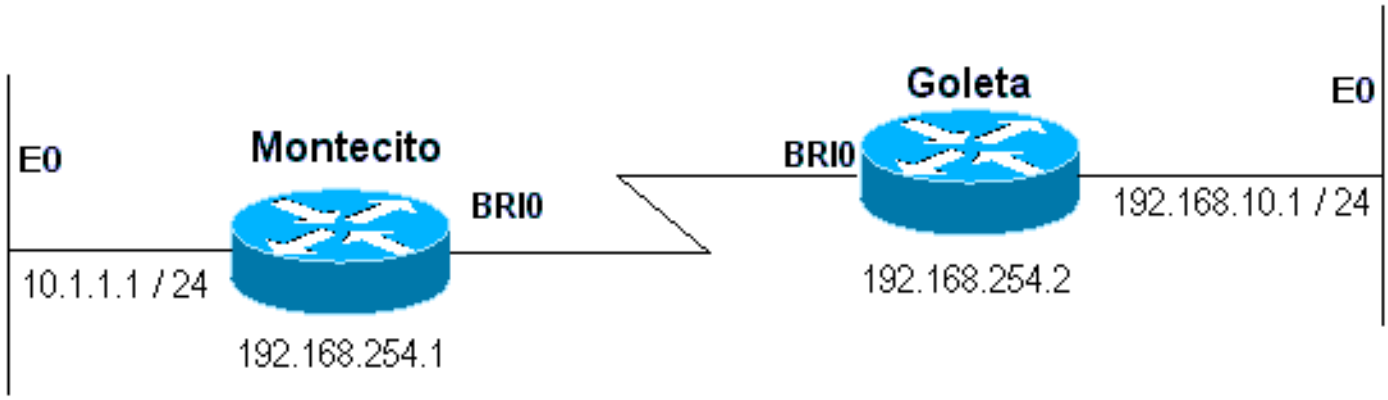

Figura 16-4: Componi tramite interfacce numerate

```
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
```

Esempio 2: Dial è l'unica connessione che utilizza interfacce senza numero. È possibile configurare questa opzione con una sola route, ma è in genere possibile configurare due route: un percorso host all'interfaccia LAN sul router remoto e un percorso alla LAN remota tramite l'interfaccia LAN remota. Questa operazione viene eseguita per evitare problemi di mappatura da layer 3 a layer 2, che possono causare errori di incapsulamento.

Questo metodo viene utilizzato anche se le interfacce dialer sui due dispositivi sono numerate, ma non si trovano sulla stessa rete o subnet.

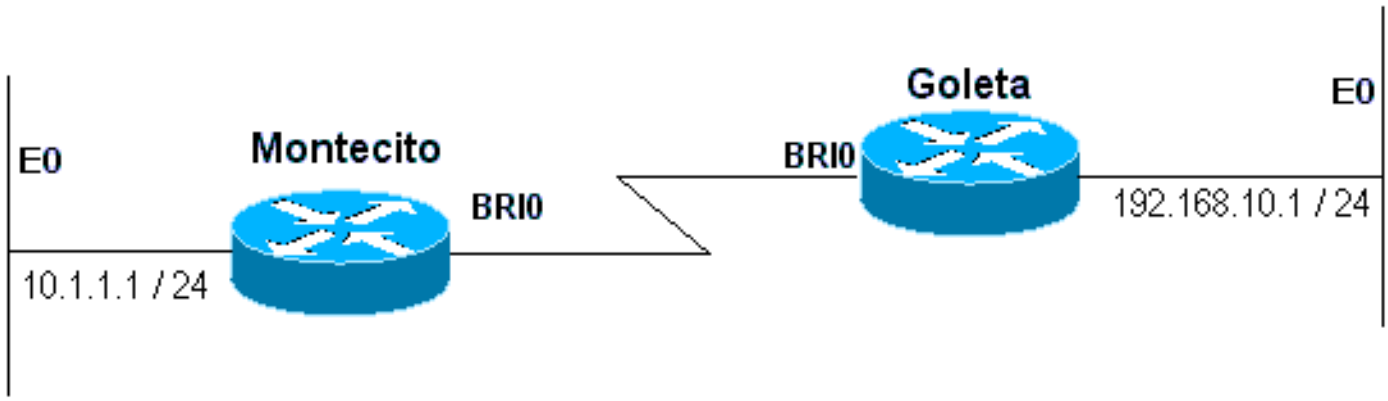

Figura 16-5: Componi utilizzando interfacce senza numero

```
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
```

Esempio 3: La composizione è una connessione di backup che utilizza interfacce numerate. È necessaria una route statica mobile.

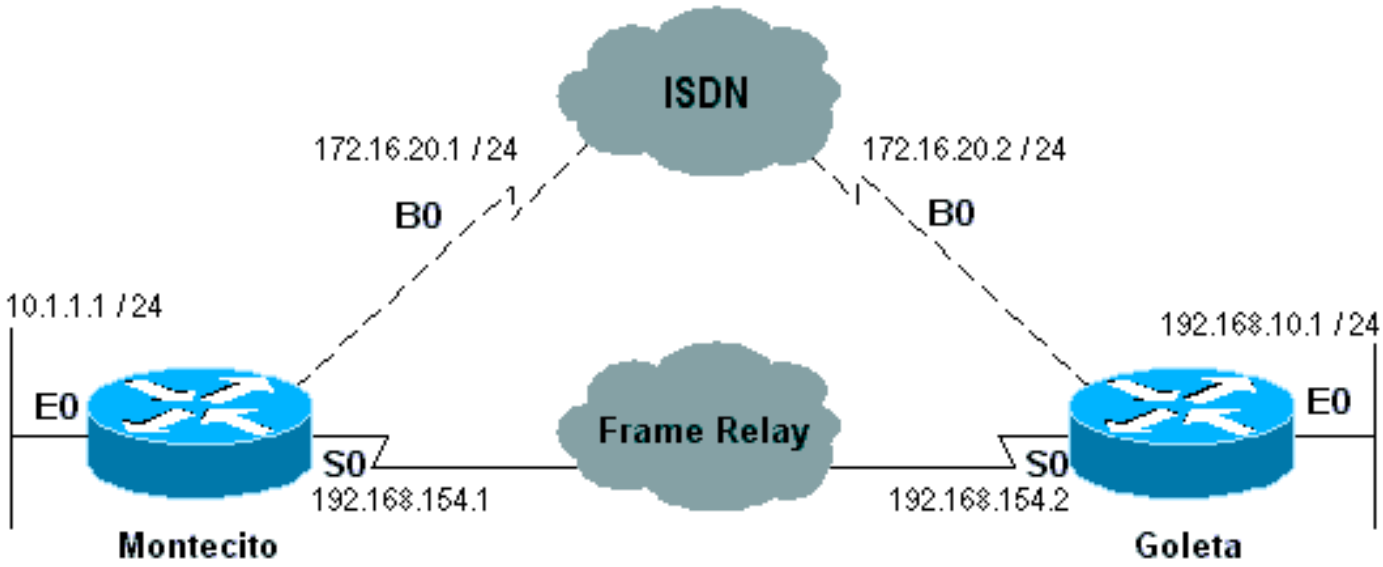

Figura 16-6: Backup tramite interfacce numerate

```
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
```

Esempio 4: La composizione è una connessione di backup che utilizza interfacce senza numero. Come nell'esempio 2, questo metodo viene utilizzato anche se le interfacce di connessione sui due dispositivi sono numerate, ma non si trovano sulla stessa rete o subnet.

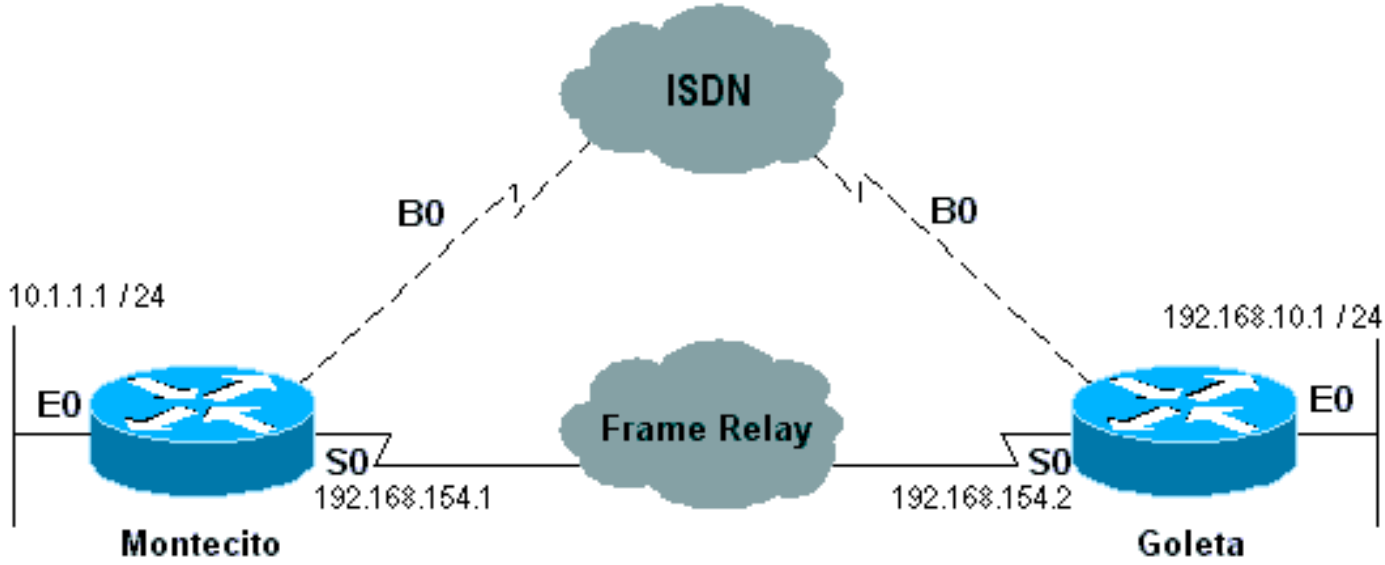

Figura 16-7: Backup con interfacce senza numero

```
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
```

Mappe dialer

Il DDR basato su mappa dialer (legacy) è potente e completo, ma le sue limitazioni influiscono sulla scalabilità e sull'estendibilità. Il DDR basato su mappa dialer si basa su un binding statico tra la specifica della chiamata per destinazione e la configurazione dell'interfaccia fisica.

Tuttavia, anche il DDR basato su mappa dialer ha molti punti di forza. Supporta Frame Relay, CLNS ISO, LAPB, snapshot routing e tutti i protocolli di routing supportati sui router Cisco. Per impostazione predefinita, il DDR basato su mappa dialer supporta la commutazione veloce.

Quando si configura un'interfaccia per le chiamate in uscita, è necessario configurare una mappa dialer per ogni destinazione remota e per ogni diverso numero chiamato nella destinazione remota. Ad esempio, se si desidera una connessione Multilink PPP per la connessione da un BRI ISDN a un'altra interfaccia ISDN BRI con un numero di directory locale diverso per ciascuno dei relativi canali B, è necessaria una mappa dialer per ciascuno dei numeri remoti:

```
!
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
!
```

L'ordine in cui vengono configurate le mappe dialer può essere importante. Se due o più comandi della mappa dialer fanno riferimento allo stesso indirizzo remoto, il router o il server di accesso li proverà uno dopo l'altro, in ordine, fino a quando non stabilisce una connessione

Nota: IOS può creare dinamicamente mappe dialer su un router che riceve una chiamata. La mappa dialer è basata sul nome utente autenticato e sull'indirizzo IP negoziato del chiamante. Le mappe dialer dinamiche possono essere visualizzate solo nell'output del comando **show dialer map**. Non è possibile visualizzarli nella configurazione corrente del router o del server di accesso.

Sintassi dei comandi

Utilizzare il seguente formato del comando di configurazione dell'interfaccia **dialer map** per:

- configurare un'interfaccia seriale o ISDN per chiamare uno o più siti, oppure
- ricevere chiamate da più siti.

Tutte le opzioni sono visualizzate in questa prima forma del comando. Per eliminare una determinata voce della mappa dialer, utilizzare una forma **no** di questo comando.

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

Utilizzare il seguente formato del comando **dialer map** per:

- configurare un'interfaccia seriale o ISDN per effettuare una chiamata a più siti;
- per autenticare le chiamate da più siti.
  `dialer map protocol next-hop-address [name hostname] [spc] [speed 56 | 64] [broadcast] [dial-string[:isdn-subaddress]]`

Per configurare un'interfaccia seriale o un'interfaccia ISDN per il supporto del bridging, usare il formato seguente del comando **dialer map**.

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

Utilizzare la forma seguente del comando **dialer map** per configurare un'interfaccia asincrona a cui effettuare una chiamata:

- un singolo sito che richiede uno script di sistema o al quale non è assegnato uno script modem, oppure
- più siti su una singola linea, su più linee o su un gruppo rotante dialer.
  ```
  dialer map protocol next-hop-address [name hostname] [broadcast]
  [modem-script modem-regexp] [system-script system-regexp] [dial-string]
  ```

Descrizione della sintassi

- *protocol* **-** Parole chiave del protocollo. Utilizzare una delle seguenti opzioni: **appletalk, bridge, clns, decnet, ip, ipx, novell, snapshot, vines o xns.**
- *next-hop-address*: indirizzo di protocollo usato per confrontare gli indirizzi a cui sono destinati i pacchetti. Questo argomento non viene utilizzato con la parola chiave **bridge** protocol.
- **name** - (Facoltativo) Indica il sistema remoto con cui comunica il router locale o il server di accesso. Utilizzato per autenticare il sistema remoto sulle chiamate in ingresso.
- *hostname* - (Facoltativo) Nome o ID della periferica remota (generalmente il nome host) con distinzione tra maiuscole e minuscole. Per i router con interfacce ISDN, il campo *hostname* (nome host) può contenere il numero fornito dall'ID della linea chiamante (nei casi in cui è disponibile l'identificazione della linea chiamante, nota anche come *CLI*, *ID chiamante* e *identificazione numerica automatica* (ANI)).
- **spc** - (Facoltativo) Specifica una connessione semipermanente tra l'apparecchiatura del cliente e la sostituzione. Viene utilizzato solo in Germania per i circuiti tra un ISDN BRI e uno switch ISDN 1TR6 e in Australia per i circuiti tra un ISDN PRI e uno switch TS-014.
- **velocità 56 | 64** - (Facoltativo) Parola chiave e valore che indicano la velocità della linea da utilizzare espressa in kilobit al secondo. Utilizzato solo per ISDN. La velocità predefinita è 64 kbps.
- **broadcast** - (Facoltativo) Indica che le trasmissioni devono essere inoltrate a questo indirizzo di protocollo.
- **script modem** - (Facoltativo) Indica lo script modem da utilizzare per la connessione (per le interfacce asincrone).
- *modem-regexp* - (Facoltativo) Espressione regolare a cui verrà associato uno script modem (per interfacce asincrone).
- **script-sistema** - (Facoltativo) Indica lo script di sistema da utilizzare per la connessione (per interfacce asincrone).
- *system-regexp* - (Facoltativo) Espressione regolare a cui verrà associato uno script di sistema (per interfacce asincrone).
- *dial-string[:isdn-subaddress]* (Facoltativo) Numero di telefono inviato al dispositivo di composizione dopo il riconoscimento dei pacchetti con un indirizzo hop successivo specificato corrispondente all'elenco degli accessi definito (e il numero di sottoindirizzo facoltativo usato per le connessioni ISDN multipunto). La stringa di composizione e il sottoindirizzo ISDN, se utilizzati, devono essere l'ultimo elemento della riga di comando.

Profili dialer

Nota: in questa sezione il termine "interfaccia dialer" si riferisce all'interfaccia configurata; non a un'interfaccia fisica sul router o sul server di accesso.

L'implementazione dei profili dialer di DDR, introdotta in IOS versione 11.2, si basa su una separazione tra la configurazione dell'interfaccia logica e quella fisica. I profili dialer consentono inoltre di associare dinamicamente le configurazioni logiche e fisiche per singola chiamata.

La metodologia dei profili dialer è utile quando si desidera eseguire le operazioni seguenti:

- condividere un'interfaccia (ISDN, seriale asincrono o seriale sincrono) per effettuare o ricevere chiamate
- modificare qualsiasi configurazione per singolo utente (ad eccezione dell'incapsulamento nella prima fase dei profili dialer)
- bridge per molte destinazioni
- evitare problemi di divisione degli orizzonti

I profili dialer consentono di separare la configurazione delle interfacce fisiche dalla configurazione logica necessaria per una chiamata e di associare dinamicamente le configurazioni logica e fisica per singola chiamata.

Un *profilo dialer* è costituito dai seguenti elementi:

- Configurazione di un'interfaccia dialer (entità logica), incluse una o più stringhe di composizione (ognuna delle quali viene utilizzata per raggiungere una sottorete di destinazione)
- Classe *dialer map* che definisce tutte le caratteristiche per qualsiasi chiamata alla stringa di composizione specificata
- Pool di *dialer* ordinato di interfacce fisiche da utilizzare per l'interfaccia dialer

Tutte le chiamate da o verso la stessa sottorete di destinazione utilizzano lo stesso profilo dialer.

La configurazione dell'interfaccia Dialer include tutte le impostazioni necessarie per raggiungere una sottorete di destinazione specifica (e tutte le reti raggiunte attraverso di essa). È possibile specificare più stringhe di composizione per la stessa interfaccia dialer. ogni stringa di composizione può essere associata a una diversa classe della mappa dialer. La classe-mappa dialer definisce tutte le caratteristiche per qualsiasi chiamata alla stringa di composizione specificata. Ad esempio, la classe map di una destinazione può specificare una velocità ISDN di 56 kbps. La classe map di una destinazione diversa può specificare una velocità ISDN di 64 kbps.

Ogni interfaccia dialer utilizza un pool di dialer, ovvero un pool di interfacce fisiche ordinate in base alla priorità assegnata a ciascuna interfaccia fisica. Un'interfaccia fisica può appartenere a più pool di dialer, in cui il conflitto viene risolto per priorità. Le interfacce ISDN BRI e PRI possono impostare un limite al numero minimo e massimo di canali B riservati da qualsiasi pool di dialer. Un canale riservato da un pool di dialer rimane inattivo finché il traffico non viene indirizzato al pool.

Quando si utilizzano i profili dialer per configurare il DDR, un'interfaccia fisica non dispone di impostazioni di configurazione ad eccezione dell'incapsulamento e dei pool di dialer a cui appartiene l'interfaccia.

Nota: il paragrafo precedente presenta un'eccezione. I comandi validi prima del completamento

dell'autenticazione devono essere configurati sull'interfaccia fisica (o BRI o PRI) e non sul profilo Dialer. I profili dialer non copiano i comandi di autenticazione PPP (o i comandi LCP) sull'interfaccia fisica.

La Figura 16-8 mostra una tipica applicazione dei profili dialer. Il router A dispone dell'interfaccia dialer 1 per il routing delle chiamate su richiesta con la sottorete 1.1.1.0 e dell'interfaccia dialer 2 per il routing delle chiamate su richiesta con la sottorete 2.2.2.0. L'indirizzo IP per l'interfaccia dialer 1 è il suo indirizzo come nodo nella rete 1.1.1.0. Allo stesso tempo, tale indirizzo IP funge da indirizzo IP delle interfacce fisiche usate dall'interfaccia dialer 1. Analogamente, l'indirizzo IP per l'interfaccia dialer 2 è il suo indirizzo come nodo nella rete 2.2.2.0.

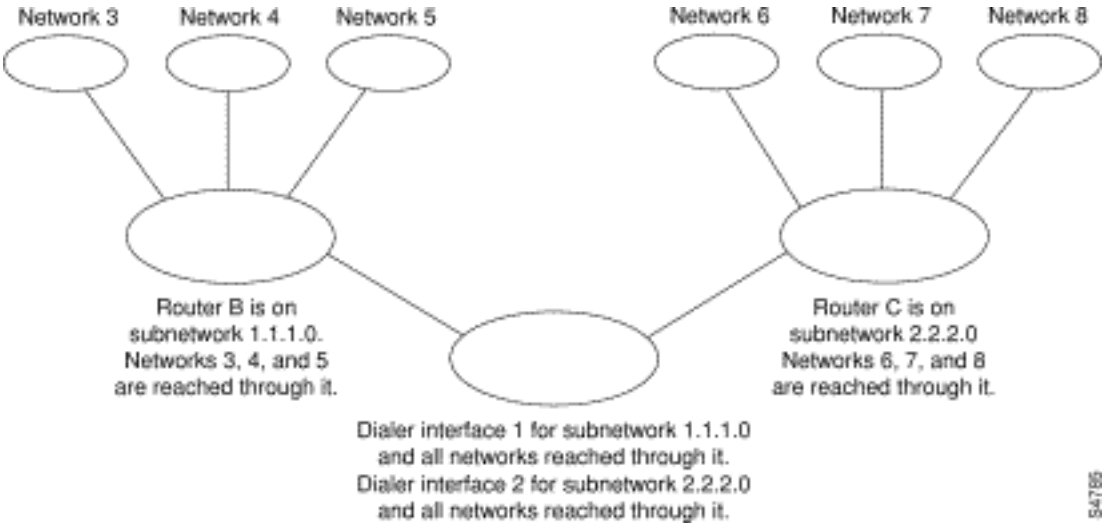

Figura 16-8: Applicazione tipica dei profili dialer

Un'interfaccia dialer utilizza un solo pool di dialer. Un'interfaccia fisica, tuttavia, può essere membro di uno o più pool di dialer e un pool di dialer può avere più interfacce fisiche come membri.

La Figura 16-9 illustra le relazioni tra i concetti di interfaccia dialer, pool dialer e interfacce fisiche. L'interfaccia dialer 0 utilizza il pool di dialer 2. L'interfaccia fisica BRI 1 appartiene al pool di dialer 2 e ha una priorità specifica nel pool. Anche l'interfaccia fisica BRI 2 appartiene al pool di dialer 2. Poiché il conflitto viene risolto sulla base dei livelli di priorità delle interfacce fisiche nel pool, a BRI 1 e BRI 2 devono essere assegnate priorità diverse nel pool. Forse a BRI 1 è assegnata la priorità 100 e a BRI 2 la priorità 50 nel pool dialer 2 (una priorità di 50 è più alta di una priorità di 100). BRI 2 ha una priorità più alta nel pool e i suoi inviti saranno posizionati per primi.

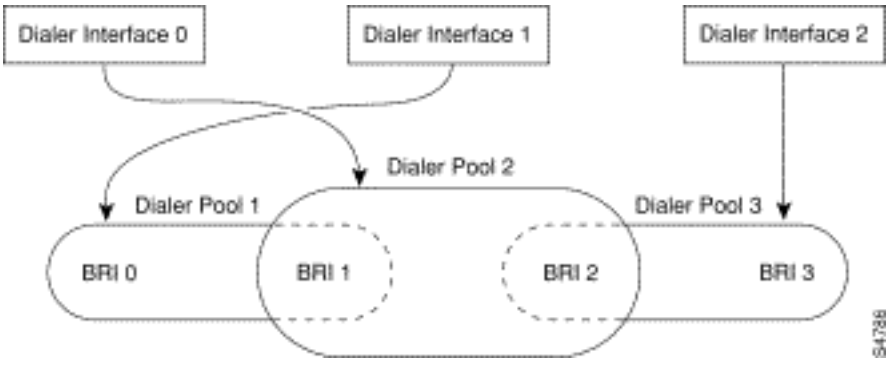

Figura 16-9: Relazioni tra interfacce dialer, pool di dialer e interfacce fisiche

[Passaggi di configurazione del profilo Dialer]

Comando	Scopo
interface dialer number	Creare un'interfaccia Dialer.
maschera indirizzo **ip**	Specificare l'indirizzo IP e la maschera dell'interfaccia Dialer come nodo nella rete di destinazione da chiamare.
encapsulation ppp	Specificare l'incapsulamento PPP.
dialer nome-remoto *nomeutente*	Specificare il nome di autenticazione CHAP del router remoto.
dialer string *dial-string* **class** *class-name*	Specificare la destinazione remota da chiamare e la classe mappa che definisce le caratteristiche per le chiamate a questa destinazione.
dialer *poolnumber*	Specificare il pool di composizione da utilizzare per le chiamate a questa destinazione.
dialer-group *group-number*	Assegnare l'interfaccia Dialer a un gruppo dialer.
dialer-list *dialer-group* **protocol** *nome-protocollo* **{allow | nega | list** *access-list-number***}**	Specificare un elenco degli accessi in base al numero di elenco o al protocollo e al numero di elenco per definire i pacchetti "interessanti" che possono attivare una chiamata.

Operazioni PPP

Il protocollo PPP (Point-to-Point Protocol) è di gran lunga il protocollo di trasporto a livello di collegamento più comune, avendo completamente usurpato SLIP come protocollo di scelta per le connessioni seriali sincrone e asincrone (e in molti casi non-dial). Il protocollo PPP è stato originariamente definito nel 1989 dalla RFC 1134, che da allora è diventato obsoleto a causa di una serie di RFC che culminano (a partire da questa scrittura) nella RFC 1661. Sono inoltre disponibili numerose RFC che definiscono gli elementi del protocollo, ad esempio RFC 1990 (PPP Multilink Protocol), RFC 2125 (PPP Bandwidth Allocation Protocol) e molti altri. Un repository online di RFC è disponibile all'indirizzo:

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

La migliore definizione di PPP è forse la RFC1661, che afferma:

Il protocollo PPP (Point-to-Point) costituisce un metodo standard per il trasporto di datagrammi multiprotocollo su collegamenti point-to-point. Il PPP è costituito da tre componenti principali:

1. Metodo per l'incapsulamento dei datagrammi multi-protocollo.
2. Un LCP (Link Control Protocol) per la creazione, la configurazione e la verifica della connessione dati.
3. Famiglia di NCP (Network Control Protocol) per stabilire e configurare diversi protocolli a

livello di rete.

Fasi della negoziazione PPP

La negoziazione PPP è costituita da tre fasi: Protocollo LCP (Link Control Protocol), autenticazione e protocollo NCP (Network Control Protocol). Ciascuna parte procede in ordine, una volta stabilita la connessione asincrona o ISDN.

LCP

Il protocollo PPP non segue un modello client/server. Tutte le connessioni sono peer-to-peer. Pertanto, quando sono presenti un chiamante e un ricevente, entrambe le estremità della connessione point-to-point devono concordare i protocolli e i parametri negoziati.

Quando la negoziazione ha inizio, ciascun peer che desidera stabilire una connessione PPP deve inviare una richiesta Configure (visualizzata nella **negoziazione PPP di debug** e di seguito indicata come CONFREQ). Le opzioni incluse in CONFREQ non sono quelle predefinite per il collegamento. Queste includono spesso Maximum Receive Unit (MRU), Async Control Character Map (ACCM), Authentication Protocol (AuthProto) e il Magic Number. Vengono inoltre visualizzati l'unità di ricezione ricostruita massima (MRRU) e il discriminatore endpoint (EndpointDisc), utilizzati per Multilink PPP.

Esistono tre possibili risposte a qualsiasi CONFREQ:

- Se il peer riconosce le opzioni e accetta i valori visualizzati in CONFREQ, è necessario emettere un messaggio di conferma della configurazione (CONFACK).
- Ènecessario inviare un messaggio Configura-Rifiuta (CONFREJ) se una delle opzioni in CONFREQ non viene riconosciuta (ad esempio, alcune opzioni specifiche del fornitore) o se i valori di una delle opzioni sono stati esplicitamente negati nella configurazione del peer.
- Se vengono riconosciute tutte le opzioni contenute in CONFREQ, è necessario inviare un messaggio di conferma (CONFNAK), ma i valori non sono accettabili per il peer.

I due peer continuano a scambiarsi richieste CONFREQ, CONFREJ e CONFNAK finché ciascuno di essi non invia una richiesta CONFACK, finché la connessione di composizione non viene interrotta o finché uno o entrambi i peer non indicano che la negoziazione non può essere completata.

Autenticazione

Dopo il completamento della negoziazione LCP e il raggiungimento di un accordo su AuthProto, il passo successivo è l'autenticazione. L'autenticazione, sebbene non obbligatoria in base a RFC161, è consigliata su tutte le connessioni remote. In alcuni casi è necessario un corretto funzionamento; I profili dialer sono un esempio calzante.

I due tipi principali di autenticazione in PPP sono il protocollo PAP (Password Authentication Protocol) e il protocollo CHAP (Challenge Handshake Authentication Protocol), definiti da RFC1334 e aggiornati da RFC1994.

Il protocollo PAP è il più semplice tra i due, ma offre un livello di protezione inferiore perché la password in testo normale viene inviata tramite la connessione di composizione. La protezione CHAP è maggiore in quanto la password in testo normale non viene mai inviata attraverso la

connessione di composizione.

Il PAP può essere necessario in uno dei seguenti ambienti:

- Ampia base installata di applicazioni client che non supportano la protezione CHAP
- Incompatibilità tra le implementazioni di CHAP di diversi fornitori

Quando si parla di autenticazione, è utile utilizzare i termini "richiedente" e "autenticatore" per distinguere i ruoli svolti dai dispositivi a entrambe le estremità della connessione, anche se entrambi i peer possono agire in entrambi i ruoli. "Richiedente" descrive il dispositivo che richiede l'accesso alla rete e fornisce le informazioni di autenticazione; l'autenticatore verifica la validità delle informazioni di autenticazione e consente o non consente la connessione. È comune per entrambi i peer agire in entrambi i ruoli quando viene stabilita una connessione DDR tra router.

PAP

Il PAP è abbastanza semplice. Dopo il completamento della negoziazione LCP, il richiedente invia ripetutamente la combinazione nome utente/password tramite il collegamento finché l'autenticatore non risponde con una conferma o finché il collegamento non viene interrotto. L'autenticatore può disconnettere il collegamento se determina che la combinazione nome utente/password non è valida.

CHAP

La protezione CHAP è un po' più complicata. L'autenticatore invia una richiesta di verifica al richiedente, che risponde con un valore. Questo valore viene calcolato utilizzando una funzione "hash unidirezionale" per eseguire l'hashing della richiesta di verifica e della password CHAP. Il valore risultante viene inviato all'autenticatore insieme al nome host CHAP del richiedente (che può essere diverso dal nome host effettivo) in un messaggio di *risposta*.

L'autenticatore legge il nome host nel messaggio di risposta, cerca la password prevista per il nome host e quindi calcola il valore previsto che il richiedente invierà nella sua risposta eseguendo la stessa funzione hash eseguita dal richiedente. Se i valori risultanti corrispondono, l'autenticazione ha esito positivo. In caso di errore, la connessione verrà interrotta.

AAA

Per eseguire il protocollo PAP o CHAP, è possibile usare un servizio di autenticazione, autorizzazione e accounting (AAA), ad esempio TACACS+ o RADIUS.

NCP

Dopo l'autenticazione, inizia la fase NCP. Come in LCP, i pari si scambiano i CONFREQ, i CONFREJ, i CONFNAK e i CONFACK. Tuttavia, in questa fase della negoziazione, gli elementi che vengono negoziati hanno a che fare con protocolli di livello superiore (IP, IPX, Bridging, CDP, ecc.). È possibile negoziare uno o più protocolli. Poiché è il protocollo più utilizzato e altri protocolli operano in modo molto simile, il protocollo IPCP (Internet Protocol Control Protocol), definito nella RFC132, è l'argomento al centro di questa discussione. Altre RFC pertinenti includono, a titolo esemplificativo:

- RFC 1552 (protocollo di controllo IPX)

- RFC 1378 (AppleTalk Control Protocol)
- RFC 1638 (Bridging Control Protocol)
- RFC 1762 (protocollo di controllo DECnet)
- RFC 1763 (protocollo di controllo Vines)

Inoltre, il protocollo Cisco Discovery Protocol Control Protocol (CDPCP) può essere negoziato durante il protocollo NCP, anche se questa procedura non è comune. I tecnici Cisco TAC consigliano solitamente di configurare il comando no cdp enable su qualsiasi interfaccia della connessione per evitare che i pacchetti CDP continuino a ricevere chiamate per un periodo di tempo indefinito.

L'elemento chiave negoziato in IPCP è l'indirizzo di ciascun peer. Ognuno dei pari si trova in uno dei due stati possibili; o ha un indirizzo IP o no. Se il peer dispone già di un indirizzo, invierà tale indirizzo in una richiesta CONFREQ all'altro peer. Se l'indirizzo è accettabile per l'altro peer, verrà restituito CONFACK. Se l'indirizzo non è accettabile, la risposta sarà un CONFNAK contenente un indirizzo che il peer utilizzerà.

Se il peer non dispone di un indirizzo, invierà un messaggio CONFREQ con l'indirizzo 0.0.0.0. In questo modo, l'altro peer assegnerà un indirizzo, tramite l'invio di un messaggio CONFREQ con l'indirizzo corretto.

Altre opzioni possono essere negoziate in IPCP. Vengono comunemente visualizzati gli indirizzi primario e secondario per il server dei nomi di dominio e il server dei nomi NetBIOS, come descritto in Informational RFC1877. Anche il protocollo IP Compression Protocol (RFC1332) è comune.

Metodologie PPP alternative

Le metodologie PPP alternative includono PPP multilink, PPP multicassis e profili virtuali.

Multilink PPP

Il protocollo MLP (Multilink Point-to-Point Protocol) fornisce funzionalità di bilanciamento del carico su più collegamenti WAN. Allo stesso tempo, offre interoperabilità tra più fornitori, frammentazione dei pacchetti, sequenziamento corretto e calcolo del carico sia sul traffico in entrata che in uscita. L'implementazione Cisco di Multilink PPP supporta le specifiche di frammentazione e sequenza di pacchetti della RFC 1717.

Il protocollo Multilink PPP consente di frammentare i pacchetti. Questi frammenti possono essere inviati contemporaneamente a più collegamenti point-to-point allo stesso indirizzo remoto. I collegamenti multipli vengono visualizzati in risposta a una soglia di carico dialer definita dall'utente. Il carico può essere calcolato sul traffico in entrata, in uscita o su entrambi, in base al traffico tra i siti specifici. MLP fornisce larghezza di banda su richiesta e riduce la latenza di trasmissione sui collegamenti WAN.

Multilink PPP funziona sui seguenti tipi di interfaccia (singola o multipla) configurati per supportare sia i gruppi a rotazione su chiamata su richiesta che l'incapsulamento PPP:

- interfacce seriali asincrone
- BRI
- PRI

Configurazione

Per configurare Multilink PPP su interfacce asincrone, configurare le interfacce asincrone in modo che supportino l'incapsulamento DDR e PPP. È quindi possibile configurare un'interfaccia Dialer per supportare l'incapsulamento PPP, la larghezza di banda su richiesta e Multilink PPP. A un certo punto, tuttavia, l'aggiunta di altre interfacce asincrone non migliora le prestazioni. Con le dimensioni MTU predefinite, Multilink PPP deve supportare tre interfacce asincrone con modem V.34. Tuttavia, i pacchetti potrebbero essere scartati occasionalmente se l'MTU è piccola o se si verificano grandi burst di brevi frame.

Per abilitare Multilink PPP su una singola interfaccia ISDN BRI o PRI, non è necessario definire un gruppo rotante dialer separatamente, in quanto le interfacce ISDN sono gruppi rotanti dialer per impostazione predefinita. Se non si utilizzano le procedure di autenticazione PPP, il servizio telefonico deve passare le informazioni sull'ID chiamante.

Ènecessario un numero di soglia di carico. Per un esempio di configurazione del protocollo Multilink PPP su una singola interfaccia ISDN BRI, vedere di seguito l'*esempio del protocollo Multilink PPP su una singola interfaccia ISDN*.

Se è stato configurato Multilink PPP e si desidera che un pacchetto di connessione multipla sia connesso a tempo indeterminato, usare il comando **dialer idle-timeout** per impostare un timer di inattività molto alto. Il comando **dialer-load threshold 1** non mantiene un fascio di *n* collegamenti multipli connessi a tempo indeterminato e il comando **dialer-load threshold 2** non mantiene un fascio di due collegamenti multipli connessi a tempo indeterminato.

Per abilitare Multilink PPP su più interfacce ISDN BRI o PRI, è necessario configurare un'interfaccia rotante Dialer e configurarla per Multilink PPP. È quindi possibile configurare i BRI separatamente e aggiungerli ciascuno allo stesso gruppo rotante. Vedere di seguito *l'esempio di Multilink PPP su più interfacce ISDN*.

Esempio di Multilink PPP su un'interfaccia ISDN

Nell'esempio seguente viene attivato Multilink PPP sull'interfaccia BRI 0. Quando viene configurato un BRI, non è necessaria alcuna configurazione del gruppo rotante dialer (per impostazione predefinita, l'interfaccia ISDN è un gruppo rotante).

```
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
```

Esempio di Multilink PPP su più interfacce ISDN

Nell'esempio seguente vengono configurati più BRI ISDN in modo che appartengano allo stesso gruppo di rotazione dialer per Multilink PPP. Utilizzare il comando **dialer rotary-group** per assegnare ciascun BRI ISDN al gruppo rotante del dialer che deve corrispondere al numero dell'interfaccia Dialer (in questo caso, il numero 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
```

Multicassis Multilink PPP

Multilink PPP consente di dividere e ricombinare i pacchetti in un singolo sistema terminale su una pipe logica (detta anche *bundle*) formata da più collegamenti. Multilink PPP fornisce larghezza di banda su richiesta e riduce la latenza di trasmissione sui collegamenti WAN.

Il protocollo MMP (Multicassis Multilink PPP), d'altra parte, offre la funzionalità aggiuntiva che consente ai collegamenti di terminare su più router con indirizzi remoti diversi. Il protocollo MMP può inoltre gestire sia il traffico analogico che quello digitale.

Questa funzionalità è destinata a situazioni in cui vi sono pool di utenti remoti, in cui un singolo server di accesso non è in grado di fornire un numero sufficiente di porte di accesso remoto. MMP consente alle aziende di fornire un unico numero di accesso remoto ai propri utenti e di applicare la stessa soluzione alle chiamate analogiche e digitali. Questa funzione consente, ad esempio, ai provider di servizi Internet di allocare un singolo numero a rotazione ISDN a più PRI ISDN su più router.

Per una descrizione completa dei comandi MMP a cui si fa riferimento nel presente documento, consultare la *guida di riferimento dei comandi di Cisco Dial Solutions*. Per individuare la documentazione di altri comandi illustrati in questo capitolo, utilizzare l'indice principale di riferimento dei comandi oppure eseguire una ricerca in linea.

Il protocollo MMP è supportato sulle piattaforme Cisco serie 7500, 4500 e 2500 e sulle interfacce sincrona seriale, asincrona seriale, ISDN BRI, ISDN PRI e Dialer.

Il protocollo MMP non richiede la riconfigurazione degli switch della compagnia telefonica.

Configurazione

I router o i server di accesso sono configurati per appartenere a gruppi di peer, denominati *gruppi di stack*. Tutti i membri del gruppo di stack sono peer; i gruppi di stack non hanno bisogno di un router lead permanente. Qualsiasi membro dello stack può rispondere alle chiamate provenienti da un singolo numero di accesso, che in genere è un gruppo di risposta PRI ISDN. Le chiamate

possono arrivare da dispositivi degli utenti remoti, come router, modem, schede di terminale ISDN o schede PC.

Una volta stabilita una connessione con un membro di un *gruppo di stack*, tale membro è il proprietario della chiamata. Se una seconda chiamata arriva dallo stesso client e un router diverso risponde alla chiamata, il router stabilisce un tunnel e inoltra tutti i pacchetti appartenenti alla chiamata al router proprietario della chiamata. Il processo di creazione di un tunnel e di inoltro delle chiamate al router proprietario della chiamata è talvolta denominato *proiezione del collegamento PPP al dispositivo master della chiamata*.

Se è disponibile un router più potente, è possibile configurarlo come membro del gruppo di stack e gli altri membri del gruppo possono stabilire dei tunnel e inoltrare tutte le chiamate al gruppo. In questo caso, gli altri membri dello stack stanno solo rispondendo alle chiamate e inoltrando il traffico al più potente router *di offload*.

Nota: le linee WAN ad alta latenza tra i membri dello stack group possono rendere inefficiente il funzionamento dello stack group.

Le operazioni di gestione delle chiamate MMP, licitazione e inoltro di livello 2 nel gruppo di stack procedono come segue. È anche mostrata nella Figura 16-10.

1. Quando la prima chiamata arriva allo stack group, il router A risponde.
2. Nell'offerta, il router A vince perché ha già la chiamata. Il router A diventa il *dispositivo master* della *chiamata* per quella sessione con il dispositivo remoto. Il router A può anche essere chiamato l'*host dell'interfaccia del bundle master*.
3. Quando il dispositivo remoto che ha avviato la chiamata richiede una larghezza di banda maggiore, esegue una seconda chiamata Multilink PPP al gruppo.
4. Quando arriva la seconda chiamata, il router D risponde e informa il gruppo dello stack. Il router A ha vinto la gara perché sta già gestendo la sessione con il dispositivo remoto.
5. Il router D crea un tunnel per il router A e inoltra i dati PPP non elaborati al router A.
6. Il router A ricompone i pacchetti e ne crea una nuova sequenza.
7. Se il router D riceve più chiamate e anche queste appartengono al router A, il tunnel tra A e D si ingrandisce per gestire il traffico aggiunto. Il router D non stabilisce un tunnel aggiuntivo per A.
8. Se arrivano e ricevono risposta più chiamate da un altro router, quest'ultimo stabilisce anche un tunnel verso A e inoltra i dati PPP non elaborati.
9. I dati riassemblati vengono trasmessi alla rete aziendale come se fossero tutti collegati fisicamente.

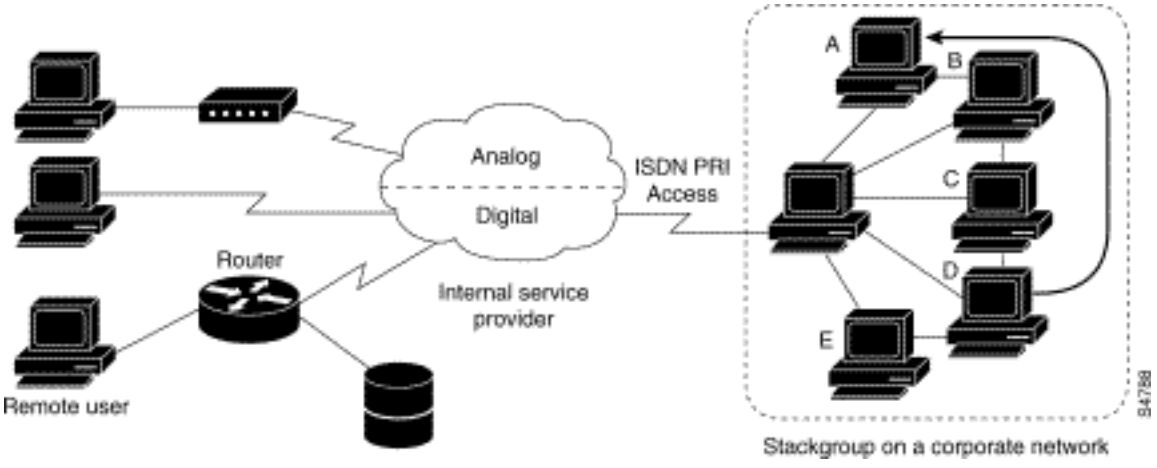

Figura 16-10: Tipico scenario PPP Multilink Multilink

A differenza della figura precedente, la Figura 16-11 presenta un router di offload. I server di accesso che appartengono a un gruppo di stack rispondono alle chiamate, stabiliscono i tunnel e inoltrano le chiamate a un router Cisco 4700 che vince la licitazione e che è il dispositivo master di tutte le chiamate. Cisco 4700 ricompone e riordina tutti i pacchetti in arrivo attraverso il gruppo di stack.

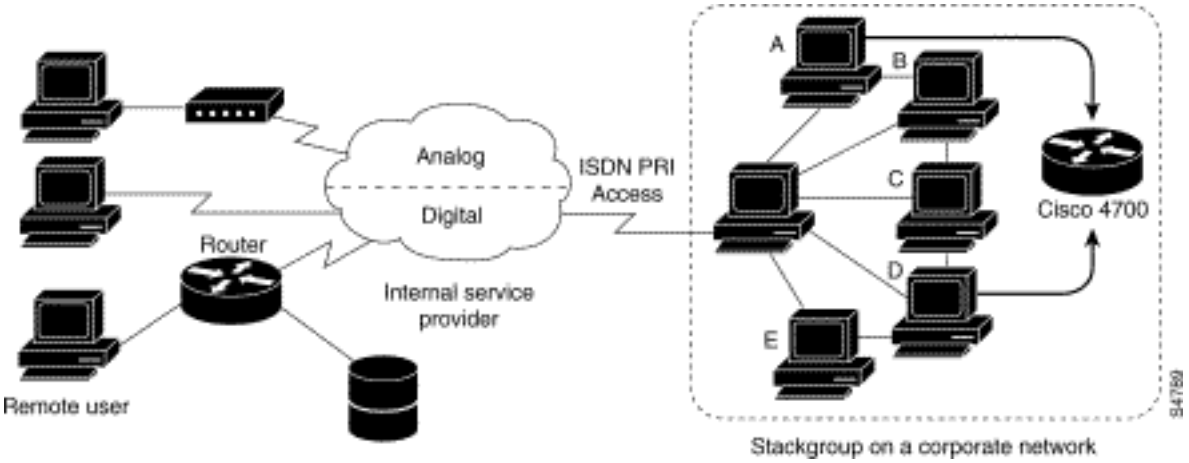

Figura 16-11: Multicassis Multilink PPP con un router offload come membro del gruppo di stack

Nota: è possibile creare gruppi di stack usando diverse piattaforme di server di accesso, switching e router. Tuttavia, i server di accesso universale come Cisco AS5200 non devono essere combinati con ISDN. Questa operazione deve essere eseguita solo con server di accesso come la piattaforma 4x00. Poiché le chiamate dall'ufficio centrale vengono assegnate in modo arbitrario, questa combinazione potrebbe causare la consegna di una chiamata analogica a un server di accesso solo digitale, che non sarebbe in grado di gestire la chiamata.

Il supporto MMP su un gruppo di router richiede che ogni router sia configurato per supportare quanto segue:

- Multilink PPP
- Protocollo SGBP (Stack Group Bind Protocol)
- Modello virtuale utilizzato per la clonazione della configurazione dell'interfaccia per il supporto di MMP

Profili virtuali

Profili virtuali è un'applicazione PPP (Point-to-Point Protocol) univoca in grado di creare e configurare dinamicamente un'interfaccia di accesso virtuale quando viene ricevuta una chiamata in ingresso e di disattivarla dinamicamente al termine della chiamata. I profili virtuali funzionano con PPP semplice e con MLP (Multilink PPP).

Le informazioni di configurazione per un'interfaccia di accesso virtuale per i profili virtuali possono provenire da un'interfaccia di modello virtuale, da una configurazione specifica dell'utente memorizzata in un server di autenticazione, autorizzazione e accounting (AAA) o da entrambi.

La configurazione AAA specifica dell'utente utilizzata dai profili virtuali è la configurazione dell'*interfaccia* e viene scaricata durante le negoziazioni LCP. Anche un'altra funzionalità, denominata Configurazione per utente, utilizza le informazioni di configurazione ottenute da un

server AAA. Tuttavia, la configurazione per utente utilizza la configurazione di *rete* (ad esempio elenchi di accesso e filtri di route) scaricata durante le negoziazioni NCP.

La configurazione dell'interfaccia di accesso virtuale tramite i profili virtuali, le interfacce dei modelli virtuali e le configurazioni AAA sono regolate da due regole:

- Ogni applicazione di accesso virtuale può disporre al massimo di un modello da cui duplicare. Tuttavia, può avere più configurazioni AAA da cui duplicare (profili virtuali, informazioni AAA e configurazione AAA per utente, che a sua volta potrebbe includere la configurazione per più protocolli).
- Quando i profili virtuali sono configurati da un modello virtuale, il relativo modello ha la priorità più alta di qualsiasi altro modello virtuale.

Vedere la sezione "Interoperabilità con altre funzionalità di composizione Cisco" più avanti per una descrizione delle possibili sequenze di configurazione che dipendono dalla presenza o assenza di MLP o di un'altra funzionalità di accesso virtuale che duplica un'interfaccia di modello virtuale.

Questa funzionalità viene eseguita su tutte le piattaforme Cisco IOS che supportano MLP.

Per una descrizione completa dei comandi menzionati in questa sezione, consultare il capitolo "Virtual Profiles Commands" della *guida di riferimento dei comandi di Dial Solutions* nella documentazione di Cisco IOS. Per individuare la documentazione relativa ad altri comandi illustrati in questo capitolo, è possibile utilizzare l'indice principale di riferimento dei comandi oppure eseguire ricerche in linea.

Premesse

In questa sezione vengono presentate informazioni di base sui profili virtuali per comprendere meglio l'applicazione prima di iniziare a configurarla.

Restrizioni

Èconsigliabile utilizzare indirizzi non numerati nelle interfacce dei modelli virtuali per evitare la creazione di indirizzi di rete duplicati nelle interfacce di accesso virtuale.

Prerequisiti

L'uso di informazioni di configurazione dell'interfaccia AAA specifiche dell'utente con i profili virtuali richiede che il router sia configurato per il server AAA e che il server AAA abbia coppie AV di configurazione dell'interfaccia specifica dell'utente. Le coppie AV rilevanti (su un server RADIUS) iniziano come segue:

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

Le informazioni che seguono il segno di uguale (=) possono essere qualsiasi comando di configurazione dell'interfaccia Cisco IOS. Ad esempio, la riga potrebbe essere la seguente:

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

L'utilizzo di un'interfaccia di modello virtuale con i profili virtuali richiede la definizione di un

modello virtuale specifico per i profili virtuali.

Interoperabilità con altre funzionalità di composizione Cisco

I profili virtuali interagiscono con Cisco DDR, Multilink PPP (MLP) e dialer come ISDN.

Configurazione DDR delle interfacce fisiche

I profili virtuali interagiscono completamente con le interfacce fisiche nei seguenti stati di configurazione DDR quando non sono configurate altre applicazioni di interfaccia di accesso virtuale:

- I profili dialer sono configurati per l'interfaccia. Al posto della configurazione dei profili virtuali viene utilizzato il profilo dialer.
- DDR non configurato sull'interfaccia. I profili virtuali sostituiscono la configurazione corrente.
- DDR legacy configurato sull'interfaccia. I profili virtuali sostituiscono la configurazione corrente.

Nota: se si usa un'interfaccia di connessione (compreso qualsiasi dialer ISDN), la relativa configurazione viene usata sull'interfaccia fisica anziché sulla configurazione dei profili virtuali.

Effetto Multilink PPP sulla configurazione dell'interfaccia di accesso virtuale

Come mostrato nella tabella 16-8, la configurazione esatta di un'interfaccia di accesso virtuale dipende dai tre fattori seguenti:

- Indica se i profili virtuali sono configurati dal modello virtuale, da AAA, da entrambi o da nessuno dei due. Questi stati sono indicati rispettivamente come "VP VT only", "VP AAA only", "VP VT e VP AAA" e "No VP at all" nella tabella.
- La presenza o l'assenza di un'interfaccia dialer.
- La presenza o l'assenza di MLP. L'etichetta di colonna "MLP" è un componente aggiuntivo per qualsiasi funzionalità di accesso virtuale che supporti MLP e cloni da un'interfaccia di modello virtuale.

Nella Tabella 16-8, "Multilink VT" significa che viene duplicata un'interfaccia di modello virtuale *se* ne è stata definita una per MLP o una funzione di accesso virtuale che utilizza MLP.

Tabella 16-8: Sequenza di duplicazione della configurazione dei profili virtuali

Configurazione profili virtuali	MLP senza dialer	Dialer MLP	MLP No Dialer	Nessun dialer MLP
Solo VP VT	VP VT	VP VT	VP VT	VP VT
Solo VP AAA	(Multilink VT) VP AAA	(Multilink VT) VP AAA	VP AAA	VP AAA
VP VT e VP AAA	VP VT VP	VP VT VP	VP VT VP AAA	VP VT VP AAA

	AAA	AAA		
Nessun VP	(Multilink VT)	Dialer	Nessuna interfaccia di accesso virtuale creata.	Nessuna interfaccia di accesso virtuale creata.

L'ordine degli elementi in qualsiasi cella della tabella è importante. Se VP VT è visualizzato sopra VP AAA, significa che prima il modello virtuale dei profili virtuali viene clonato sull'interfaccia, quindi viene applicata la configurazione dell'interfaccia AAA per l'utente. La configurazione dell'interfaccia AAA specifica dell'utente aggiunge elementi alla configurazione e ignora eventuali comandi di configurazione dell'interfaccia fisica o del modello virtuale in conflitto.

Interoperabilità con altre funzionalità che utilizzano modelli virtuali

I profili virtuali inoltre interagiscono con le applicazioni di accesso virtuale che duplicano un'interfaccia di modello virtuale. Ogni applicazione di accesso virtuale può avere al massimo un modello da cui duplicare, ma può duplicare più configurazioni AAA.

L'interazione tra i profili virtuali e altre applicazioni di modelli virtuali è la seguente:

- Se i profili virtuali sono abilitati e per essi è definito un modello virtuale, viene utilizzato il modello virtuale Profili virtuali.
- Se i profili virtuali sono configurati solo da AAA (non è definito alcun modello virtuale per i profili virtuali), è possibile duplicare il modello virtuale di un'altra applicazione di accesso virtuale (ad esempio VPDN) sull'interfaccia di accesso virtuale.
- Un eventuale modello virtuale viene duplicato su un'interfaccia di accesso virtuale prima della configurazione dei profili virtuali AAA o della configurazione AAA per utente. La configurazione AAA per utente, se utilizzata, viene applicata per ultima.

Terminologia

In questo capitolo vengono utilizzati i seguenti termini nuovi o non comuni:

Coppia AV: Un parametro di configurazione su un server AAA; parte della configurazione utente che il server AAA invia al router in risposta alle richieste di autorizzazione specifiche dell'utente. Il router interpreta ciascuna coppia AV come un comando di configurazione del router Cisco IOS e applica le coppie AV in ordine. In questo capitolo, il termine coppia AV si riferisce a un parametro di configurazione interfaccia su un server RADIUS.

Una coppia AV di configurazione interfaccia per profili virtuali può assumere una forma simile alla seguente:

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

clonazione: Creazione e configurazione di un'interfaccia di accesso virtuale tramite l'applicazione di comandi di configurazione da un modello virtuale specifico. Il modello virtuale è l'origine delle informazioni utente generiche e delle informazioni dipendenti dal router. Il risultato della clonazione è un'interfaccia di accesso virtuale configurata con tutti i comandi nel modello.

virtual access interface (interfaccia di accesso virtuale): Istanza di un'interfaccia virtuale univoca creata in modo dinamico ed esistente temporaneamente. Le interfacce di accesso virtuale possono essere create e configurate in modo diverso da applicazioni diverse, ad esempio profili virtuali e reti di accesso remoto private virtuali.

interfaccia modello virtuale: Configurazione generica dell'interfaccia per determinati utenti o per un determinato scopo, più informazioni dipendenti dal router. Questa operazione viene effettuata sotto forma di elenco di comandi dell'interfaccia Cisco IOS da applicare all'interfaccia virtuale secondo necessità.

profilo virtuale: Istanza di un'interfaccia di accesso virtuale univoca creata in modo dinamico quando determinati utenti effettuano una chiamata e che viene disattivata in modo dinamico quando la chiamata viene interrotta. Il profilo virtuale di un utente specifico può essere configurato tramite un'interfaccia di modello virtuale, una configurazione di interfaccia specifica dell'utente memorizzata su un server AAA oppure tramite un'interfaccia di modello virtuale e una configurazione di interfaccia specifica dell'utente da AAA.

La configurazione di un'interfaccia di accesso virtuale inizia con un'eventuale interfaccia del modello virtuale, seguita dall'applicazione della configurazione specifica dell'utente per la sessione di connessione remota dell'utente specifico (se disponibile).

Esempio annotato di negoziazione PPP

Nell'esempio, il comando ping attiva un collegamento ISDN tra i router *Montecito* e *Goleta*. Si noti che, sebbene in questo esempio non sia presente l'indicatore orario, è in genere consigliabile utilizzare il comando di configurazione globale **timestamp debug datetime msec**.

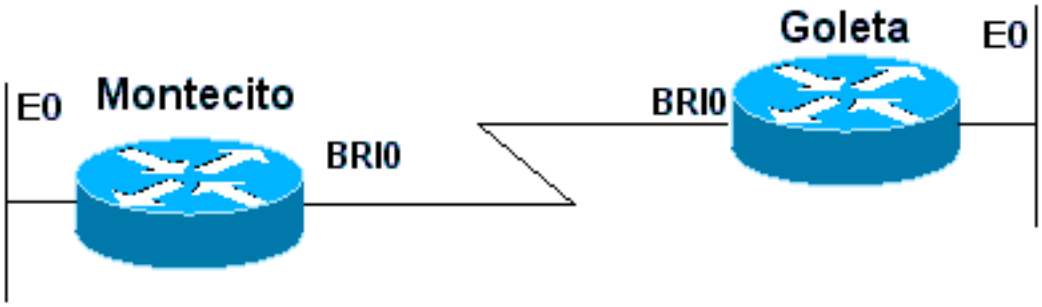

Figura 16-12: Router-ISDN-Router

Questi debug sono presi da *Montecito*; tuttavia, il debug su *Goleta* sembrerebbe più o meno lo stesso.

Nota: i debug potrebbero essere visualizzati in un formato diverso. Questo output è il formato di output del debug PPP precedente, prima delle modifiche introdotte in IOS versione 11.2(8). Vedere il Capitolo 17 per un esempio di debug PPP nelle versioni più recenti di IOS.

```
Montecito#show debugging

  PPP:

    PPP authentication debugging is on

    PPP protocol negotiation debugging is on
```

A
Montecito#**ping 172.16.20.2**

Type escape sequence to abort.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Q
ppp: ipcp_reqci: returning CONFACK.

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

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

T
 BRI0: install route to 172.16.20.2

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

Il traffico A viene generato per avviare un tentativo di composizione.

B - La connessione è stata stabilita (i debug ISDN non sono stati utilizzati in questo esempio).

Inizio LCP:

C - *Montecito* invia richieste di configurazione LCP per AUTHTYPE e per MAGICNUMBER.

D - *Goleta* invia le sue CONFREQ. Se il valore per MAGICNUMBER è uguale al valore inviato da *Montecito*, è molto probabile che la linea venga ripetuta.

E - Ciò indica che *Montecito* ha inviato riconoscimenti ai CONFREQ di *Goleta*.

F - *Montecito* riceve CONFACK da *Goleta*.

Inizio fase di autenticazione:

G, H - *Montecito* e *Goleta* si sfidano per l'autenticazione.

J - *Goleta* risponde alla sfida.

K, L - *Goleta* supera con successo l'autenticazione.

M - Messaggio da *Goleta* a *Montecito*: autenticazione riuscita.

Inizio della negoziazione NCP:

N, P - Ogni router invia il proprio indirizzo IP configurato in un CONFREQ.

Q, R - *Montecito* invia una CONFACK al CONFREQ di *Goleta*.

S - ? e viceversa.

Il percorso T, U - A è installato da *Montecito* a *Goleta* e il protocollo sull'interfaccia cambia in "up", indicando che i negoziati NCP sono stati completati con successo.

Prima di chiamare il team TAC di Cisco Systems

Prima di chiamare il Technical Assistance Center (TAC) di Cisco Systems, leggere attentamente questo capitolo e completare le azioni suggerite per il problema del sistema.

Inoltre, fai quanto segue e documenta i risultati in modo che possiamo assisterti meglio:

Per tutti i problemi, raccogliere l'output di **show running-config** e **show version**. Verificare che il parametro **timestamp del servizio** comandi **datetime debug msec** sia presente nella configurazione.

Per i problemi DDR, raccogliere quanto segue:

- **mostra mappa dialer**
- **debug dialer**
- **negoziazione ppp di debug**
- **debug autenticazione ppp**

Se è coinvolta una connessione ISDN, raccogliere:

- **show isdn status**
- **debug isdn q931**
- **debug di eventi isdn**

Se sono coinvolti modem, raccogliere:

- mostra righe
- show line [x]
- **show modem** (se sono interessati modem integrati)
- **show modem version** (se sono interessati modem integrati)
- **debug modem**
- **debug modem csm** (se sono interessati modem integrati)
- **debug chat** (se uno scenario DDR)

Se sono coinvolti T1 o PRI, raccogliere:

- **show controller t1**

Informazioni correlate

- Guida alle soluzioni di composizione Cisco IOS
- Panoramica delle interfacce, dei controller e delle linee utilizzati per l'accesso dial
- Routing su linee modem
- Configurazione porta seriale e trunk T1/E1
- Progettazione di interreti DDR
- Scelta e preparazione della configurazione del DDR
- Configurazione di DDRtitle
- Panoramica della tecnologia PPP
- Progettazione di ISDN Internetworks
- Tipi, codici e valori degli switch ISDN
- Attivazione della linea ISDN
- Documentazione e supporto tecnico – Cisco Systems