Tecnologia Dialup: Tecniche di risoluzione dei problemi

Sommario

Introduzione

Dialup è semplicemente l'applicazione della rete telefonica pubblica commutata (PSTN) che trasporta i dati per conto dell'utente finale. Si tratta di un dispositivo CPE (Customer Premise Equipment) che invia all'interruttore telefonico un numero di telefono al quale indirizzare una connessione. Cisco AS3600, AS5200, AS5300 e AS5800 sono tutti esempi di router che possono eseguire un PRI insieme a banchi di modem digitali. L'AS2511, d'altra parte, è un esempio di router che comunica con modem esterni.

Prerequisiti

Requisiti

I lettori di questo documento devono essere a conoscenza di quanto segue:

Il mercato dei vettori è cresciuto in modo significativo e ora il mercato richiede densità di modem più elevate. La risposta a questa esigenza è una maggiore interazione con le apparecchiature della compagnia telefonica e lo sviluppo del modem digitale. Si tratta di un modem in grado di accedere direttamente alla rete PSTN. Di conseguenza, ora sono stati sviluppati modem CPE più veloci che sfruttano la chiarezza del segnale di cui godono i modem digitali. Il fatto che i modem digitali che si connettono alla PSTN tramite PRI o BRI possano trasmettere dati a più di 53k utilizzando lo standard di comunicazione V.90, dimostra il successo di questa idea.

I primi server di accesso sono stati Cisco2509 e Cisco2511. Lo switch AS2509 è in grado di supportare 8 connessioni in ingresso tramite modem esterni, mentre lo switch AS2511 ne supporta 16. Lo switch AS5200 è stato introdotto con 2 PRI e può supportare 48 utenti tramite modem digitali, rappresentando un importante passo avanti nella tecnologia. La densità dei modem è aumentata costantemente con l'AS5300 che supporta 4 e quindi 8 PRI. Infine, l'AS5800 è stato introdotto per soddisfare le esigenze delle installazioni di classe carrier che devono gestire decine di T1 in ingresso e centinaia di connessioni utente.

Un paio di tecnologie obsolete vengono menzionate in una discussione storica sulla tecnologia dialer. 56Kflex è un vecchio standard modem (precedente alla V.90) da 56k proposto da Rockwell. Cisco supporta la versione 1.1 dello standard 56Kflex sui modem interni, ma consiglia di migrare i modem CPE a V.90 il prima possibile. Un'altra tecnologia obsoleta è l'AS5100, una joint venture tra Cisco e un produttore di modem. L'AS5100 è stato creato per aumentare la densità del modem mediante l'uso di schede modem quadruple. Comprendeva un gruppo di AS2511 costruiti come schede inserite in un backplane condiviso da schede modem quadruple e una doppia scheda T1.

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.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Risoluzione dei problemi relativi alle chiamate in arrivo

La risoluzione dei problemi relativi a una chiamata in arrivo inizia dal basso e prosegue verso l'alto. Il ragionamento generale prevede quanto segue:

1. Vediamo arrivare la chiamata? (La risposta *affermativa* avanza alla domanda successiva)
2. Il destinatario risponde alla chiamata?
3. La chiamata è completata?
4. I dati passano attraverso il collegamento?
5. La sessione è stabilita? (PPP o terminale)

Per le connessioni modem, una chiamata dati ha lo stesso aspetto di una sessione terminale in arrivo fino alla fine in cui la chiamata dati passa a negoziare il protocollo PPP.

Per le chiamate in arrivo che coinvolgono modem digitali, verificare innanzitutto che l'ISDN o il server CAS sottostante riceva la chiamata. Se si utilizza un modem esterno, le sezioni ISDN e CAS possono essere ignorate.

Risoluzione dei problemi relativi alle chiamate ISDN in arrivo

Utilizzare il comando **debug isdn q931**. Di seguito è riportato un esempio di output restituito da una connessione riuscita:

```
Router# debug isdn q931
RX <- SETUP pd = 8 callref = 0x06
 Bearer Capability i = 0x8890
 Channel ID i = 0x89
 Calling Party Number i = 0x0083, `5551234'
TX -> CONNECT pd = 8 callref = 0x86
RX <- CONNECT_ACK pd = 8 callref = 0x06
```

Il messaggio di installazione indica che è in corso l'avvio di una connessione da parte dell'estremità remota. I numeri di riferimento delle chiamate vengono gestiti in coppia. In questo caso, il numero di riferimento della chiamata per il lato in ingresso della connessione è 0x06 e il numero di riferimento della chiamata del lato in uscita della connessione è 0x86. La funzionalità di connessione (spesso indicata come bearercap) indica al router il tipo di chiamata in arrivo. In questo caso, la connessione è di tipo 0x8890. Quel valore indica "ISDN Speed 64 Kb/s". Se il bearercap fosse stato 0x8090A2, avrebbe indicato "Speech/voice call u-law".

Se non è stato ricevuto alcun messaggio di installazione, è necessario verificare il numero corretto chiamandolo manualmente, se è stato effettuato il provisioning vocale. Verificare inoltre lo stato dell'interfaccia ISDN (consultare il documento sull'uso del comando **show isdn status** per la risoluzione dei problemi BRI). Se tutti questi elementi vengono estratti, verificare che il mittente della chiamata stia effettuando la chiamata corretta. A tale scopo, contattare la compagnia telefonica. Il mittente della chiamata può tracciare la chiamata per vedere dove viene inviata. Se la connessione è a lunga distanza, provare un vettore di lunga distanza diverso utilizzando un codice di distanza 1010.

Se la chiamata in arrivo è una chiamata asincrona del modem, assicurarsi che la linea sia predisposta per consentire le chiamate vocali.

Nota: le chiamate asincrone al modem BRI sono una funzionalità di 3600 router che eseguono 12.0(3)T o versioni successive. Richiede una recente revisione hardware del modulo di rete dell'interfaccia BRI. I moduli WIC non supportano le chiamate asincrone tramite modem.

Se la chiamata è arrivata ma non è stata completata, cercare un codice causa (vedere la Tabella 17-10). Il completamento viene indicato dal comando connect-ack.

Se si tratta di una chiamata asincrona, passare alla sezione "Risoluzione dei problemi relativi alla chiamata in ingresso del modem".

A questo punto la chiamata ISDN è connessa, ma non è stato rilevato alcun dato che attraversi il collegamento. Utilizzare il comando **debug ppp negotiation** per verificare se sulla linea passa traffico PPP. Se il traffico non viene visualizzato, è possibile che la velocità non corrisponda. Per verificare questa condizione, utilizzare il comando **show running-config in modalità di esecuzione privilegiata** per visualizzare la configurazione del router. Controllare le voci del comando di configurazione dell'interfaccia **mappa dialer** nel router locale e remoto. Queste voci dovrebbero

essere simili alle seguenti:

```
dialer map ip 131.108.2.5 speed 56 name C4000
```

Per i profili dialer, è necessario definire una classe mappa per impostare la velocità. Per impostazione predefinita, le interfacce ISDN tentano di utilizzare velocità di comunicazione 64K su ciascun canale.

Per informazioni dettagliate sulla configurazione delle mappe di composizione e dei profili, consultare la *guida alla configurazione delle soluzioni di composizione Cisco IOS*, la *guida di riferimento ai comandi delle soluzioni di composizione* e la *guida alla configurazione rapida delle soluzioni di composizione*.

Se si ricevono pacchetti PPP validi, il collegamento è attivo e funzionante. In questa fase, passare alla sezione "Risoluzione dei problemi relativi al protocollo PPP".

Risoluzione dei problemi relativi alle chiamate CAS in arrivo

Per risolvere i problemi di connettività del gruppo CAS ai modem, utilizzare i comandi **debug modem**, **debug modem csm** e **debug cas**.

Nota: il comando **debug cas** è apparso per la prima volta nella versione 12.0(7)T per AS5200 e AS5300. Le versioni precedenti di IOS usano il servizio di configurazione a livello di sistema interno insieme al comando exec **modem-mgmt debug rbs**. Il debug di queste informazioni su un AS5800 richiede la connessione alla scheda trunk stessa.

Determinare innanzitutto se l'interruttore della compagnia telefonica è stato disconnesso per segnalare la chiamata in arrivo. In caso contrario, verificare il numero chiamato. A tale scopo, collegare un telefono alla linea telefonica del dispositivo di origine e chiamare il numero. Se la chiamata viene effettuata correttamente, il problema è nel CPE di origine. Se la chiamata non viene ancora visualizzata sul server CAS, controllare il T1 (capitolo 15).In questo caso, usare il comando **debug serial interfaces**.

Di seguito viene mostrata una buona connessione con **debug modem CSM**:

```
Router# debug modem csm
CSM_MODEM_ALLOCATE: slot 1 and port 0 is allocated.
MODEM_REPORT(0001): DEV_INCALL at slot 1 and port 0
CSM_PROC_IDLE: CSM_EVENT_ISDN_CALL at slot 1, port 0
CSM_RING_INDICATION_PROC: RI is on
CSM_RING_INDICATION_PROC: RI is off
CSM_PROC_IC1_RING: CSM_EVENT_MODEM_OFFHOOK at slot 1, port 0
MODEM_REPORT(0001): DEV_CONNECTED at slot 1 and port 0
CSM_PROC_IC2_WAIT_FOR_CARRIER: CSM_EVENT_ISDN_CONNECTED at slot 1, port 0
```

In questo esempio, la chiamata è stata indirizzata a un modem. Se la chiamata è stata indirizzata a un modem, passare alla sezione "Risoluzione dei problemi relativi alla chiamata in ingresso del modem", più avanti.

Risoluzione dei problemi relativi alle chiamate al modem in arrivo

Per la risoluzione dei problemi relativi alle chiamate modem in arrivo, utilizzare i comandi di debug seguenti:

- **debug modem**
- **debug modem csm** (per modem digitali integrati)

Utilizzare i seguenti comandi di debug in combinazione per indicare la nuova chiamata in arrivo:

- **debug isdn q931**
- **debug cas**

Supponendo che la chiamata raggiunga il modem, questo deve rispondere.

Suggerimenti per il debug di modem esterni

Per facilitare il debug su un modem esterno collegato a una linea TTY, aumentare il volume degli altoparlanti. Questo aiuta a rendere alcuni problemi più evidenti.

Quando il modem di origine effettua una chiamata, il modem ricevente suona? In caso contrario, verificare il numero e provare a effettuare una chiamata manuale dal sito remoto. Provare a utilizzare anche un normale telefono sul lato di ricezione. Sostituire i cavi e l'hardware secondo necessità.

Ritiro chiamata modem asincrono

Se un modem esterno non risponde, controllare il cablaggio tra il modem e il server di accesso o il router. Verificare che il modem sia collegato alla porta TTY o ausiliaria sul router con un cavo RJ-45 e un adattatore DB-25 MMOD. Cisco consiglia e supporta questa configurazione dei cavi per le porte RJ-45. Questi connettori sono in genere etichettati come: *Modem.*

I cavi RJ-45 sono disponibili in alcuni modelli: diritto, rotolamento e crossover. È possibile determinare il tipo di cablaggio tenendo le due estremità di un cavo RJ-45 fianco a fianco. Vedrete otto strisce colorate, o spille, a ciascuna estremità.

- Se l'ordine dei pin colorati è lo stesso a ciascuna estremità, il cavo è diritto.
- Se l'ordine dei colori viene invertito a ciascuna estremità, il cavo viene arrotolato.
- Il cavo è un cavo crossover se i colori indicano quanto segue:

Cavo crossover da RJ45 a RJ45:

```
RJ45                    RJ45
          5 ------------------ 2
          2 ------------------ 5
          4 ------------------ 1
          1 ------------------ 4
```

Per verificare che la segnalazione sia corretta, utilizzare il comando **show line** descritto nel capitolo 16.

A parte i problemi di cablaggio, è necessario inizializzare un modem esterno per la risposta automatica. Controllare il modem remoto per verificare se è impostato sulla risposta automatica. Di solito, una spia si accende quando è impostata la risposta automatica. Impostare il modem remoto sulla risposta automatica se non è già impostato. Per informazioni sulla verifica e la modifica delle impostazioni del modem, consultare la documentazione del modem. Utilizzare un telnet inverso per inizializzare il modem (fare riferimento al capitolo 16).

Ritiro digitale (integrato) delle chiamate modem

Su un modem esterno è chiaro se la chiamata è in fase di risposta, ma i modem interni richiedono una chiamata manuale al numero ricevente. Attendere il segnale di risposta (ABT). Se non si sente un segnale ABT, controllare la configurazione per i seguenti due elementi:

1. Verificare che il comando **isdn incoming-voice modem** sia presente in tutte le interfacce ISDN che gestiscono le connessioni modem in ingresso.
2. Nella configurazione della linea TTY del modem, assicurarsi che il comando **modem inout** esista.

Inoltre, è possibile che il modulo CSM (Call Switching Module) non abbia allocato un modem interno per gestire la chiamata in arrivo. È possibile che il modem o i pool di risorse siano configurati per un numero insufficiente di connessioni in ingresso. Il server di accesso potrebbe anche avere esaurito i modem. Verificare la disponibilità dei modem e modificare in modo appropriato le impostazioni del pool di modem o del gestore del pool di risorse. Se è stato allocato un modem e la configurazione mostra **il modem in uscita**, raccogliere i debug e contattare Cisco per assistenza.

Training sul modem

Se il modem ricevente genera DSR, il training è riuscito. I guasti del training possono indicare un problema di circuito o l'incompatibilità del modem.

Per arrivare alla fine di un singolo problema del modem, andare al prompt AT sul modem di origine mentre è collegato alla linea POTS di interesse. Se si effettua una chiamata a un modem digitale in un server di accesso Cisco, prepararsi a registrare un file .wav della musica di allenamento o della DIL (Digital Disability Learning Sequence). DIL è lo spartito musicale (sequenza PCM) che il modem analogico V.90 di origine indica al modem digitale ricevente di riprodurre. La sequenza consente al modem analogico di rilevare qualsiasi danno digitale nel circuito; ad esempio più conversioni D/A, una legge/u-law, bit rubati o pad digitali. Se il DIL non viene visualizzato, i modem non hanno negoziato V.90 in V.8/V.8bis (ovvero, un problema di compatibilità del modem). Se si sente il DIL e si esegue un nuovo addestramento nel V.34, il modem analogico decide (sulla base della riproduzione DIL) che il V.90 non è realizzabile.

La musica è rumorosa? In tal caso, pulire il circuito.

Il cliente si arrende rapidamente, senza eseguire il training V.34? Per esempio, forse non sa cosa fare quando sente il V.8bis. In tal caso, provare a disabilitare V.8bis (da cui K56Flex) sul server (se accettabile). È necessario ottenere un nuovo firmware client o sostituire il modem client. In alternativa, l'estremità di composizione può inserire cinque virgole alla fine della stringa di composizione. Ciò ritarda l'ascolto del modem chiamante e causerà il timeout del segnale V.8bis dal server ricevente senza influire sul modem client. Cinque virgole nella stringa di composizione sono una linea guida generale e potrebbe essere necessario regolare per tenere conto delle condizioni locali.

Definizione della sessione

A questo punto della sequenza, i modem sono collegati e addestrati. Ora è il momento di scoprire se il traffico attraversa in modo corretto.

Se la linea che riceve la chiamata è configurata con **autoselect ppp** e l'interfaccia asincrona è configurata con **modalità asincrona interattiva**, utilizzare il comando **debug modem** per verificare il processo di selezione automatica. Quando il traffico arriva attraverso il collegamento asincrono, il

server di accesso esamina il traffico per determinare se è basato su caratteri o su pacchetti. A seconda delle impostazioni, il server di accesso avvierà una sessione PPP o eseguirà una sessione sulla linea.

Una normale sequenza di selezione automatica con pacchetti LCP PPP in entrata:

```
*Mar  1 21:34:56.958: TTY1: DSR came up
*Mar  1 21:34:56.962: tty1: Modem: IDLE->READY
*Mar  1 21:34:56.970: TTY1: EXEC creation
*Mar  1 21:34:56.978: TTY1: set timer type 10, 30 seconds
*Mar  1 21:34:59.722: TTY1: Autoselect(2) sample 7E
 !--- The inbound traffic is displayed in hexadecimal format. This is based on the !--- bits
coming in over the line, regardless of whether the bits are ASCII !--- characters or elements of
a packet. The bits represented in this example are !--- correct for a LCP packet. Anything
different would be either a malformed packet !--- or character traffic. *Mar 1 21:34:59.726:
TTY1: Autoselect(2) sample 7EFF *Mar 1 21:34:59.730: TTY1: Autoselect(2) sample 7EFF7D *Mar 1
21:34:59.730: TTY1: Autoselect(2) sample 7EFF7D23 *Mar 1 21:34:59.734: TTY1 Autoselect cmd: ppp
negotiate !--- Having determined that the inbound traffic is actually an LCP packet, the access
!--- server triggers the PPP negotiation process. *Mar 1 21:34:59.746: TTY1: EXEC creation *Mar
1 21:34:59.746: TTY1: create timer type 1, 600 seconds *Mar 1 21:34:59.794: TTY1: destroy timer
type 1 (OK) *Mar 1 21:34:59.794: TTY1: destroy timer type 0 *Mar 1 21:35:01.798: %LINK-3-UPDOWN:
Interface Async1, changed state to up !--- The async interface changes state to up, and the PPP
negotiation (not shown) !--- commences.
```

Se la chiamata è una sessione PPP e la **modalità asincrona dedicata** è configurata sull'interfaccia asincrona, utilizzare il comando **debug ppp negotiation** per verificare se dall'estremità remota provengono pacchetti di richieste di configurazione. I debug mostrano questi valori come CONFREQ. Se si osservano sia pacchetti PPP in entrata che in uscita, passare a "Risoluzione dei problemi relativi al protocollo PPP". In caso contrario, connettersi dall'estremità che ha originato la chiamata con una sessione in modalità carattere (o "exec"), ovvero una sessione non PPP.

Nota: se l'estremità ricevente visualizza un **modem asincrono dedicato** sotto l'interfaccia asincrona, un dial-in exec mostra solo ciò che sembra essere un garbage ASCII casuale. Per consentire una sessione terminale e continuare a disporre della funzionalità PPP, utilizzare il comando di configurazione dell'interfaccia asincrona in **modalità asincrona interattiva**. Nella configurazione della riga associata, utilizzare il comando **autoselect ppp**.

Il modem non può inviare o ricevere dati

Se i modem si connettono a una sessione terminale e non vengono rilevati dati, verificare le possibili cause e le azioni consigliate seguenti:

- **Impostazione velocità modem non bloccata**Usare il comando **show line** exec sul server o sul router di accesso. L'output per la porta ausiliaria deve indicare le velocità Tx e Rx attualmente configurate.Per una spiegazione dell'output del comando **show line**, vedere la sezione "Uso dei comandi di debug" nel capitolo 15.Se la linea non è configurata alla velocità corretta, utilizzare il comando di configurazione della linea **speed** per impostare la velocità della linea sul server di accesso o sulla linea del router. Impostare il valore sulla velocità più elevata in comune tra il modem e la porta del server di accesso o del router. Per impostare la velocità in baud del terminale, usare il comando di configurazione **speed** line. Questo comando imposta le velocità di trasmissione (al terminale) e di ricezione (dal terminale).Sintassi:**speed** *bps*Descrizione sintassi:*bps*: velocità in baud in bit al secondo (bps). Il valore predefinito è 9600 bps.L'esempio seguente imposta le linee 1 e 2 su un server di accesso Cisco 2509 a 115200 bps:

```
line 1 2
speed 115200
```

Nota: se per qualche motivo non è possibile utilizzare il controllo del flusso, limitare la velocità della linea a 9600 bps. Le velocità più elevate possono causare la perdita di dati.Utilizzare nuovamente il comando **show line** exec e verificare che la velocità della linea sia impostata sul valore desiderato.Quando si è certi che il server di accesso o la linea del router sia configurata per la velocità desiderata, avviare una sessione Telnet inversa verso il modem tramite tale linea. Per ulteriori informazioni, vedere la sezione "Creazione di una sessione Telnet inversa su un modem" nel capitolo 16.Utilizzare una stringa di comando del modem che includa il comando "blocca velocità DTE" per il modem in uso. Per la sintassi esatta dei comandi di configurazione, consultare la documentazione del modem.**Nota:** il comando lock DTE speed, noto anche come *port rate adjust* o *buffered mode*, è spesso correlato al modo in cui il modem gestisce la correzione degli errori. Questo comando varia notevolmente da un modem all'altro.Il blocco della velocità del modem garantisce che il modem comunichi sempre con il server di accesso Cisco o con il router alla velocità configurata sulla porta ausiliaria Cisco. Se non si utilizza questo comando, il modem ripristina la velocità del collegamento dati (la linea telefonica) anziché comunicare alla velocità configurata sul server di accesso.

- **Controllo del flusso hardware non configurato su modem o router locale o remoto**Utilizzare il comando **show line** ***aux-line-number*** exec e cercare quanto segue nel campo Capabilities:

```
Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
```

Per ulteriori informazioni, fare riferimento a Interpretazione di Show Line Output nel Capitolo 16.Se in questo campo non si fa riferimento al controllo del flusso hardware, il controllo del flusso hardware non è abilitato sulla linea. È consigliabile il controllo del flusso hardware per l'accesso da server a modem.Per una spiegazione dell'output del comando **show line**, vedere la sezione "Uso dei comandi di debug" nel capitolo 15.Configurare il controllo del flusso hardware sulla linea utilizzando il comando flowcontrol hardware line configuration.Per impostare il metodo di controllo del flusso di dati tra il terminale o un altro dispositivo seriale e il router, usare il comando di configurazione della linea di **controllo del flusso**. Utilizzare la forma no di questo comando per disabilitare il controllo del flusso.Sintassi:**controllo flusso {none | software [lock] [in] | out] | hardware [in | out]}**Descrizione sintassi:**none**: disattiva il controllo del flusso.**software** - Imposta il controllo del flusso del software. Una parola chiave opzionale specifica la direzione: **in** fa sì che il software Cisco IOS ascolti il controllo del flusso dal dispositivo collegato, mentre **out** fa in modo che il software invii le informazioni di controllo del flusso al dispositivo collegato. Se non specificate una direzione, vengono utilizzate entrambe.**lock** - Rende impossibile disattivare il controllo del flusso dall'host remoto quando il dispositivo collegato richiede il controllo del flusso software. Questa opzione si applica alle connessioni che utilizzano il protocollo Telnet o rlogin.**hardware** - Imposta il controllo del flusso dell'hardware. Una parola chiave opzionale specifica la direzione: **in** fa sì che il software ascolti il controllo del flusso dal dispositivo collegato, mentre **out** fa in modo che il software invii le informazioni di controllo al dispositivo collegato. Se non specificate una direzione, vengono utilizzate entrambe. Per ulteriori informazioni sul controllo del flusso hardware, consultare il manuale dell'hardware fornito con il router.Esempio:L'esempio seguente imposta il controllo del flusso hardware sulla riga 7:

```
line 7
flowcontrol hardware
```

Nota: se per qualche motivo non è possibile utilizzare il controllo del flusso, limitare la velocità della linea a 9600 bps. Le velocità più elevate possono causare la perdita di dati.Dopo aver attivato il controllo del flusso hardware sul server di accesso o sulla linea del router, avviare una sessione Telnet inversa verso il modem tramite tale linea. Per ulteriori informazioni,

vedere la sezione "Creazione di una sessione Telnet inversa su un modem" nel capitolo 16.Utilizzare una stringa di comando del modem che includa il comando **RTS/CTS Flow** per il modem in uso. Questo comando garantisce che il modem utilizzi lo stesso metodo di controllo del flusso (ovvero, controllo del flusso hardware) del server di accesso o del router Cisco. Per la sintassi esatta dei comandi di configurazione, consultare la documentazione del modem.

- **Comandi mappa dialer non configurati correttamente**Utilizzare il comando **show running-config in modalità di** esecuzione **privilegiata** per visualizzare la configurazione del router. Controllare le voci del comando **dialer map** per verificare se la parola chiave **broadcast** è specificata.Se la parola chiave è mancante, aggiungerla alla configurazione.Sintassi:**dialer map** ***protocol next-hop-address*** **[name** ***hostname*****] [broadcast] [***dial-string***]**Descrizione sintassi:*protocol* - Protocollo soggetto a mapping. Le opzioni includono IP, IPX, bridge e snapshot.*next-hop-address*: l'indirizzo di protocollo dell'interfaccia asincrona del sito opposto.**name** ***hostname*****: parametro obbligatorio utilizzato nell'autenticazione PPP.** È il nome del sito remoto per il quale viene creata la mappa dialer. Il nome fa distinzione tra maiuscole e minuscole e deve corrispondere al nome host del router remoto.**broadcast** - Parola chiave facoltativa che consente di trasmettere i pacchetti (ad esempio, gli aggiornamenti IP RIP o IPX RIP/SAP) che vengono inoltrati alla destinazione remota. Nelle configurazioni di esempio con routing statico, non si desidera aggiornare il routing e la parola chiave **broadcast** viene omessa.*dial-string* - Numero di telefono del sito remoto. È necessario includere tutti i codici di accesso (ad esempio, 9 per uscire da un ufficio, i codici di composizione internazionali, gli indicativi di località).Verificare che i comandi della **mappa dialer** specifichino gli indirizzi dell'hop successivo corretti.Se l'indirizzo dell'hop successivo non è corretto, modificarlo utilizzando il comando **dialer map**.Verificare che tutte le altre opzioni dei comandi della mappa dialer siano specificate correttamente per il protocollo in uso.Per informazioni dettagliate sulla configurazione delle mappe dialer, consultare la *guida alla configurazione di Cisco IOS Wide-Area Networking* e la *guida di riferimento dei comandi di Wide-Area Networking*.
- **Problema con la connessione del modem**Accertarsi che il modem sia in funzione e che sia collegato in modo sicuro alla porta corretta. Determinare se un altro modem funziona quando collegato alla stessa porta.

Il debug di una sessione di esecuzione in ingresso è in genere suddiviso in alcune categorie principali:

- Il client remoto non riceve alcun prompt exec
- Nella Sessione Di Accesso Remoto Viene Visualizzato "Garbage"
- Sessione di accesso remoto aperta nella sessione esistente
- Il Modem Di Ricezione Connessione Remota Non Si Disconnette Correttamente

Il client remoto non riceve alcun prompt exec

- **La selezione automatica è abilitata nella riga**Tentare di accedere alla modalità di esecuzione premendo Invio.
- **La riga è configurata con il comando no exec**Utilizzare il comando **show line** exec per visualizzare lo stato della riga appropriata.Controllare il campo Capabilities per vedere se dice "exec soppressed". In questo caso, il comando di configurazione della riga **no exec** è abilitato.Configurare il comando **exec** line configuration sulla riga per consentire l'avvio delle sessioni di esecuzione. Questo comando non dispone di argomenti o parole chiave.L'esempio seguente attiva l'exec sulla riga 7:

```
line 7
```

```
exec
```

- **Il controllo del flusso non è abilitato.oIl controllo del flusso è abilitato solo su un dispositivo (DTE o DCE).oIl controllo del flusso non è configurato correttamente.**Utilizzare il comando **show line** *aux-line-number* exec e cercare quanto segue nel campo Capabilities:

```
Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
```

Per ulteriori informazioni, fare riferimento a Interpretazione di Show Line Output nel Capitolo 16.Se in questo campo non si fa riferimento al controllo del flusso hardware, il controllo del flusso hardware non è abilitato sulla linea. È consigliabile il controllo del flusso hardware per l'accesso da server a modem.Per una spiegazione dell'output del comando show line, vedere la sezione "Uso dei comandi di debug" nel capitolo 15.Configurare il controllo del flusso hardware sulla linea utilizzando il comando di configurazione della linea **hardware flowcontrol**. L'esempio seguente imposta il controllo del flusso hardware sulla riga 7:

```
line 7
flowcontrol hardware
```

Nota: se per qualche motivo non è possibile utilizzare il controllo del flusso, limitare la velocità della linea a 9600 bps. Le velocità più elevate possono causare la perdita di dati.Dopo aver attivato il controllo del flusso hardware sul server di accesso o sulla linea del router, avviare una sessione Telnet inversa verso il modem tramite tale linea. Per ulteriori informazioni, vedere la sezione "Creazione di una sessione Telnet inversa su un modem" nel capitolo 16.Utilizzare una stringa di comando del modem che includa il comando RTS/CTS Flow per il modem in uso. Questo comando garantisce che il modem utilizzi lo stesso metodo di controllo del flusso (ovvero, controllo del flusso hardware) del server di accesso o del router Cisco. Per la sintassi esatta dei comandi di configurazione, consultare la documentazione del modem.

- **Impostazione velocità modem non bloccata**Usare il comando **show line** exec sul server o sul router di accesso. L'output per la porta ausiliaria deve indicare le velocità Tx e Rx attualmente configurate.Per una spiegazione dell'output del comando show line, vedere la sezione "Uso dei comandi di debug" nel capitolo 15.Se la linea non è configurata alla velocità corretta, utilizzare il comando di configurazione della linea di velocità per impostare la velocità della linea sul server di accesso o sulla linea del router. Impostare il valore sulla velocità più elevata in comune tra il modem e la porta del server di accesso o del router. Per impostare la velocità in baud del terminale, usare il comando di configurazione speed line. Questo comando imposta le velocità di trasmissione (al terminale) e di ricezione (dal terminale).Sintassi:**speed** *bps*Descrizione sintassi:*bps*: velocità in baud in bit al secondo (bps). Il valore predefinito è 9600 bps.Esempio:L'esempio seguente imposta le linee 1 e 2 su un server di accesso Cisco 2509 a 115200 bps:

```
line 1 2
speed 115200
```

Nota: se per qualche motivo non è possibile utilizzare il controllo del flusso, limitare la velocità della linea a 9600 bps. Le velocità più elevate possono causare la perdita di dati.Utilizzare nuovamente il comando **show line** exec e verificare che la velocità della linea sia impostata sul valore desiderato.Quando si è certi che il server di accesso o la linea del router sia configurata per la velocità desiderata, avviare una sessione Telnet inversa verso il modem tramite tale linea. Per ulteriori informazioni, vedere la sezione "Creazione di una sessione Telnet inversa su un modem" nel capitolo 16.Utilizzare una stringa di comando del modem che includa il comando **lock** DTE speed per il modem in uso. Per la sintassi esatta dei comandi di configurazione, consultare la documentazione del modem.**Nota:** il comando **lock** DTE speed, noto anche come regolazione della velocità della porta o modalità buffered, è spesso correlato al modo in cui il modem gestisce la correzione degli errori. Questo comando

varia notevolmente da un modem all'altro.Il blocco della velocità del modem garantisce che il modem comunichi sempre con il server di accesso Cisco o con il router alla velocità configurata sulla porta ausiliaria Cisco. Se non si utilizza questo comando, il modem torna alla velocità del collegamento dati (la linea telefonica) anziché alla velocità configurata sul server di accesso.

Nelle sessioni di accesso remoto viene visualizzato "Garbage"

- **Impostazione velocità modem non bloccata**Usare il comando **show line** exec sul server o sul router di accesso. L'output per la porta ausiliaria deve indicare le velocità Tx e Rx attualmente configurate.Per una spiegazione dell'output del comando **show line**, vedere la sezione "Uso dei comandi di debug" nel capitolo 15.Se la linea non è configurata alla velocità corretta, utilizzare il comando di configurazione della linea **speed** per impostare la velocità della linea sul server di accesso o sulla linea del router. Impostare il valore sulla velocità più elevata in comune tra il modem e la porta del server di accesso o del router.Per impostare la velocità in baud del terminale, usare il comando di configurazione **speed** line. Questo comando imposta le velocità di trasmissione (al terminale) e di ricezione (dal terminale).Sintassi:**velocità** ***bps***Descrizione sintassi:Velocità in baud in bit al secondo (bps). Il valore predefinito è 9600 bps.Esempio:L'esempio seguente imposta le linee 1 e 2 su un server di accesso Cisco 2509 a 115200 bps:linea 1 2speed 115200**Nota:** se per qualche motivo non è possibile utilizzare il controllo del flusso, limitare la velocità della linea a 9600 bps. Le velocità più elevate possono causare la perdita di dati.Utilizzare nuovamente il comando **show line** exec e verificare che la velocità della linea sia impostata sul valore desiderato.Quando si è certi che il server di accesso o la linea del router sia configurata per la velocità desiderata, avviare una sessione Telnet inversa verso il modem tramite tale linea. Per ulteriori informazioni, vedere la sezione "Creazione di una sessione Telnet inversa su un modem" nel capitolo 16.Utilizzare una stringa di comando del modem che includa il comando **lock** DTE speed per il modem in uso. Per la sintassi esatta dei comandi di configurazione, consultare la documentazione del modem.**Nota:** il comando **lock** DTE speed, noto anche come *port rate adjust* o *buffered mode*, è spesso correlato al modo in cui il modem gestisce la correzione degli errori. Questo comando varia notevolmente da un modem all'altro.Il blocco della velocità del modem garantisce che il modem comunichi sempre con il server di accesso Cisco o con il router alla velocità configurata sulla porta ausiliaria Cisco. Se non si utilizza questo comando, il modem torna alla velocità del collegamento dati (la linea telefonica) anziché alla velocità configurata sul server di accesso.

Sintomo: La sessione di connessione remota viene aperta in una sessione già esistente avviata da un altro utente. In altre parole, invece di ottenere un prompt di accesso, un utente che accede al portale vede una sessione stabilita da un altro utente (che può essere un prompt dei comandi UNIX, una sessione dell'editor di testo e così via).

Sessione di accesso remoto aperta nella sessione esistente

- **Modem configurato per DCD sempre in alto**Il modem deve essere riconfigurato in modo da avere DCD alto solo su CD. A tale scopo, in genere viene utilizzata la stringa di comando del modem **&C1**, ma per informazioni sulla sintassi esatta del modem, vedere la documentazione del modem.Potrebbe essere necessario configurare la linea 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** e riconfigurare la riga del server di accesso con il comando **exec** line configuration

- **Il controllo del modem non è abilitato sul server o sul router di accesso**Usare il comando **show line** exec sul server o sul router di accesso. L'output per la porta ausiliaria deve essere visualizzato **in out** 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 show**, vedere la sezione "Uso dei comandi di debug" nel capitolo 15.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.**Nota:** accertarsi di utilizzare il comando **modem inout** invece del comando **modem dialin** quando la connettività del modem è in questione. Quest'ultimo comando consente alla riga di accettare solo chiamate in ingresso. Le chiamate in uscita verranno rifiutate, rendendo impossibile stabilire una sessione Telnet con il modem per configurarla. Se si desidera attivare il comando **modem dialin**, eseguire questa operazione solo dopo aver verificato il corretto funzionamento del modem.
- **Cablaggio non corretto**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 etichettati come: Modem.I cavi RJ-45 sono di due tipi: rettilineo e laminato. Se si tengono le due estremità di un cavo RJ-45 una accanto all'altra, si vedranno otto strisce colorate, o spine, a ciascuna estremità. Se l'ordine dei pin colorati è lo stesso a ciascuna estremità, il cavo è diritto. Se l'ordine dei colori viene invertito a ciascuna estremità, il cavo viene arrotolato.Il cavo piatto (CAB-500RJ) è di serie con i modelli Cisco 2500/CS500.Per verificare la correttezza del cablaggio, usare il comando **show line** exec. Vedere la spiegazione dell'output del comando **show line** nella sezione "Uso dei comandi di debug" in questo capitolo 15.

Il Modem Di Ricezione Connessione Remota Non Si Disconnette Correttamente

- **Il modem non rileva DTR**Immettere la stringa di comando **Hangup DTR modem**. Questo comando indica al modem di eliminare il vettore quando il segnale DTR non viene più ricevuto.Su un modem compatibile Hayes, la stringa **&D3** viene comunemente utilizzata per configurare **DTR Hangup** sul modem. Per la sintassi esatta di questo comando, consultare la documentazione del modem in uso.
- **Il controllo del modem non è abilitato sul router o sul server di accesso**Usare il comando **show line** exec sul server o sul router di accesso. L'output per la porta ausiliaria deve essere visualizzato **in out** 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 show, vedere la sezione "Uso dei comandi di debug" nel capitolo 15.Configurare la linea per il controllo del modem utilizzando il comando modem inout line configuration. Il controllo del modem è ora abilitato sul server di accesso.**Nota:** accertarsi di utilizzare il comando **modem inout** invece del comando **modem dialin** quando la connettività del modem è in questione. Quest'ultimo comando consente alla riga di accettare solo chiamate in ingresso. Le chiamate in uscita verranno rifiutate, rendendo impossibile stabilire una sessione Telnet con il modem per configurarla. Se si desidera attivare il comando **modem dialin**, eseguire questa

operazione solo dopo aver verificato il corretto funzionamento del modem.

Risoluzione dei problemi relativi alle chiamate in uscita

Mentre l'approccio per la risoluzione dei problemi delle chiamate in arrivo inizia in basso, la risoluzione dei problemi di una connessione in uscita inizia in alto. Il ragionamento generale prevede quanto segue:

1. Il routing DDR (Dial on Demand Routing) avvia una chiamata? (La risposta affermativa avanza alla domanda successiva)
2. Se si tratta di un modem asincrono, gli script di chat eseguono i comandi previsti?
3. La chiamata arriva alla rete PSTN?
4. L'estremità remota risponde alla chiamata?
5. La chiamata è completata?
6. I dati passano attraverso il collegamento?
7. La sessione è stabilita? (PPP o terminale)

Verifica del funzionamento di Dialer

Per verificare se il dialer sta tentando di effettuare una chiamata alla destinazione remota, utilizzare il comando **debug dialer events**. È possibile ottenere informazioni più dettagliate dal **pacchetto debug dialer**, ma il comando **debug dialer packet** richiede molte risorse e non deve essere usato su un sistema occupato con più interfacce dialer in funzione.

La riga seguente dell'output degli eventi dialer di debug per un pacchetto IP elenca il nome dell'interfaccia DDR e gli indirizzi di origine e di destinazione del pacchetto:

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

Se il traffico non avvia un tentativo di composizione, la causa più comune è una configurazione errata (una delle definizioni di traffico interessanti, lo stato dell'interfaccia della connessione o il routing).

Il traffico non avvia un tentativo di composizione

- **Definizioni di "traffico interessante" mancanti o errate**Utilizzando il comando **show running-config**, verificare che l'interfaccia sia configurata con un **gruppo dialer** e che sia presente un **elenco** di **dialer a** livello globale configurato con un numero corrispondente.Verificare che il comando **dialer-list** sia configurato per autorizzare un intero protocollo o il traffico che corrisponde a un elenco degli accessiVerificare che l'elenco degli accessi dichiari interessanti i pacchetti che attraversano il collegamento. Un test utile è l'uso del comando exec privilegiato **debug ip packet [list number]** usando il numero dell'elenco degli accessi pertinente. Quindi, provare a eseguire il ping sul collegamento, o inviare il traffico, attraverso di esso. Se i filtri del traffico interessati sono stati definiti correttamente, i pacchetti verranno visualizzati nell'output di debug. Se non è presente alcun output di debug da questo test, l'elenco degli accessi non corrisponde ai pacchetti.
- **Stato interfaccia**Per verificare che l'interfaccia sia nello stato "up/up (spoofing)", usare il comando **show interfaces [*interface name*]**.Interfaccia in modalità "standby"Un'altra interfaccia

(primaria) sul router è stata configurata per usare l'interfaccia di connessione remota come interfaccia di backup. Inoltre, l'interfaccia primaria non si trova in uno stato di "down/down", che è necessario per far uscire l'interfaccia della connessione telefonica dalla modalità standby. Inoltre, è necessario configurare un *ritardo di backup* sull'interfaccia primaria, altrimenti il comando **backup interface** non verrà mai applicato.Per verificare che l'interfaccia della connessione telefonica passi da "standby" a "up/up (spoofing)", in genere è necessario estrarre il cavo dall'interfaccia primaria. Spegnendo l'interfaccia primaria con il comando di configurazione **shutdown** non si metterà l'interfaccia primaria in "down/down", ma in modo amministrativo, e non così.Inoltre, se la connessione primaria è tramite Frame Relay, la configurazione Frame Relay deve essere eseguita su un'interfaccia seriale point-to-point e la società telefonica deve passare il bit "Active". Questa pratica è nota anche come "LMI end-to-end".Interfaccia "disattivata a livello amministrativo"L'interfaccia della connessione remota è stata configurata con il comando **shutdown**. Questo è anche lo stato predefinito di qualsiasi interfaccia quando un router Cisco viene avviato per la prima volta. Per rimuovere questo ostacolo, usare il comando di configurazione interfaccia **no shutdown**.

- **Routing non corretto**Eseguire il comando exec **show ip route [*a.b.c.d*]**, dove *a.b.c.d* è l'indirizzo dell'interfaccia di connessione del router remoto. se si usa **ip senza numero** sul router remoto, usare l'indirizzo dell'interfaccia elencata nel comando **ip senza numero**.L'output dovrebbe mostrare un percorso all'indirizzo remoto tramite l'interfaccia di connessione. Se non è disponibile alcuna route, verificare che le route statiche o mobili siano state configurate esaminando l'output del comando show running-config.Se esiste un percorso tramite un'interfaccia diversa da quella dialer, l'implicazione è che il DDR viene utilizzato come backup. Esaminare la configurazione del router per verificare che siano state configurate route statiche o statiche mobili. Il modo più sicuro per verificare il routing, in questo caso, è disabilitare la connessione primaria ed eseguire il comando **show ip route [*a.b.c.d*]** per verificare che nella tabella di routing sia stata installata la route corretta.**Nota:** se si tenta di eseguire questa operazione durante le operazioni di rete attive, potrebbe essere attivato un evento di composizione. Questo tipo di test può essere eseguito al meglio durante i cicli di manutenzione pianificati.

Effettuare la chiamata

Se il routing e i filtri del traffico interessanti sono corretti, avviare una chiamata. È possibile verificare questa condizione tramite gli **eventi di debug dialer**:

```
Async1 DDR: Dialing cause ip (s=10.0.0.1, d=10.0.0.2)
Async1 DDR: Attempting to dial 5551212
```

Se viene individuata la causa della chiamata ma non viene effettuato alcun tentativo di composizione, la causa più comune è una configurazione errata della mappa o del profilo della composizione.

Chiamata non effettuata

Di seguito sono elencati alcuni possibili problemi e le azioni suggerite:

- **Mapping dialer non configurato correttamente**Utilizzare il comando **show running-config** per verificare che l'interfaccia di composizione sia configurata con almeno un'istruzione *dialer map* che punti all'indirizzo di protocollo e al numero chiamato del sito remoto.

- **Profilo dialer non configurato correttamente**Utilizzare il comando **show running-config** per verificare che l'interfaccia dialer sia configurata con un comando **dialer pool X** e che l'interfaccia dialer sul router sia configurata con un *membro* corrispondente del *pool dialer X*. Se i profili dialer non sono configurati correttamente, è possibile che venga visualizzato un messaggio di debug del tipo:
  ```
  Dialer1: Can't place call, no dialer pool set
  ```
  Verificare che sia configurata una **stringa di connessione**.

Chiamate in uscita asincrone - Verifica operazione script di chat

Se la chiamata in uscita è una chiamata modem, è necessario eseguire uno script di chat affinché la chiamata possa continuare. Per DDR basati su mappa dialer, lo script di chat viene richiamato dal parametro script modem in un comando mappa dialer. Se il DDR è basato sul profilo dialer, ciò avviene mediante **lo script di** comando **dialer**, configurato sulla riga TTY. Entrambi gli utenti si basano su uno script di chat esistente nella configurazione globale del router, ad esempio:

```
chat-script callout AT OK atdt\T TIMEOUT 60 CONNECT \c
```

In entrambi i casi, il comando per visualizzare l'attività dello script di chat è **debug chat**. Se la stringa di composizione, ovvero il numero di telefono, utilizzata nel comando **dialer map** o **dialer string** è 5551212, l'output del comando debug sarà simile al seguente:

```
CHAT1: Attempting async line dialer script

CHAT1: Dialing using Modem script: callout & System script: none
CHAT1: process started
CHAT1: Asserting DTR
CHAT1: Chat script callout started
CHAT1: Sending string: AT
CHAT1: Expecting string: OK
CHAT1: Completed match for expect: OK
CHAT1: Sending string: atdt5551212
CHAT1: Expecting string: CONNECT
CHAT1: Completed match for expect: CONNECT
CHAT1: Chat script callout finished, status = Success
```

I problemi relativi allo script di chat possono essere suddivisi in tre categorie:

- Errore di configurazione
- Errore del modem
- Errore di connessione

Errore dello script di chat

Questo elenco mostra i possibili output dei programmi di chat di debug e le azioni consigliate:

- **nessuno script di chat corrispondente trovato per [number]**Non è stato configurato uno script di chat. Aggiungetene uno.
- **Dialout dello script di chat completato, stato = Timeout della connessione; l'host remoto non risponde**Il modem non risponde allo script di chat. Verificare la comunicazione con il modem (fare riferimento alla Tabella 16-2 nel Capitolo 16).
- **Timeout previsto: CONNETTI***Possibilità 1*: Il modem locale non effettua la chiamata. Verificare

che il modem possa effettuare una chiamata eseguendo una connessione Telnet inversa al modem e avviando manualmente una composizione.*Possibilità 2*: Il modem remoto non risponde. Per verificarlo, comporre il modem remoto con un normale telefono POTS.*Possibilità 3*: Il numero composto non è corretto. Verificare il numero componendolo manualmente. Se necessario, correggere la configurazione.*Possibilità 4*: L'addestramento del modem richiede troppo tempo o il valore di TIMEOUT è troppo basso. Se il modem locale è esterno, alzare il volume degli altoparlanti e ascoltare i segnali acustici. Se il training viene interrotto bruscamente, provare ad aumentare il valore di TIMEOUT nel comando **chat-script**. Se il valore di TIMEOUT è già pari a 60 secondi o superiore, vedere la sezione Formazione modem.

Chiamate ISDN in uscita

In caso di primo sospetto di errore ISDN, sia su BRI che PRI, controllare sempre l'output del comando **show isdn status**. È importante notare che il livello 1 deve essere Attivo e il livello 2 deve essere nello stato *MULTIPLE_FRAME_DEFINED*. Vedere la sezione "Interpreting Show ISDN Status Output" nel Capitolo 16 per informazioni sulla lettura di questo output, nonché per le misure correttive.

Per le chiamate ISDN in uscita, **gli eventi debug isdn q931** e **debug isdn** sono gli strumenti migliori da utilizzare. Fortunatamente, il debug delle chiamate in uscita è molto simile al debug delle chiamate in arrivo. Una normale chiamata riuscita potrebbe avere il seguente aspetto:

```
*Mar 20 21:07:45.025: ISDN BR0: Event: Call to 5553759 at 64 Kb/s
*Mar 20 21:07:45.033: ISDN BR0: TX ->  SETUP pd = 8  callref = 0x2C
*Mar 20 21:07:45.037:         Bearer Capability i = 0x8890
*Mar 20 21:07:45.041:         Channel ID i = 0x83
*Mar 20 21:07:45.041:         Keypad Facility i = 0x35353533373539
*Mar 20 21:07:45.141: ISDN BR0: RX <-  CALL_PROC pd = 8  callref = 0xAC
*Mar 20 21:07:45.145:         Channel ID i = 0x89
*Mar 20 21:07:45.157: ISDN BR0: received HOST_PROCEEDING
        Channel ID i = 0x0101
*Mar 20 21:07:45.161:   -------------------
        Channel ID i = 0x89
*Mar 20 21:07:45.313: ISDN BR0: RX <-  CONNECT pd = 8  callref = 0xAC
*Mar 20 21:07:45.325: ISDN BR0: received HOST_CONNECT
 !--- The CONNECT message is the key indicator of success. If a CONNECT is not received, !---
you may see a DISCONNECT or a RELEASE_COMP (release complete) message followed by !--- a cause
code (see below) *Mar 20 22:11:03.212: ISDN BR0: RX <- RELEASE_COMP pd = 8 callref = 0x8F *Mar
20 22:11:03.216: Cause i = 0x8295 - Call rejected
```

Il valore della causa indica due cose.

- Il secondo byte del valore a 4 o 6 byte indica da dove nel percorso della chiamata end-to-end è stato ricevuto DISCONNECT o RELEASE_COMP. In questo modo è possibile localizzare il problema.
- Il terzo e il quarto byte indicano la causa effettiva dell'errore. Vedere le tabelle seguenti per il significato dei diversi valori.

Nota: la seguente immagine indica in genere un errore di protocollo superiore:

```
Cause i = 0x8090 - Normal call clearing
```

Un errore di autenticazione PPP è in genere dovuto a un errore. Attivare la **negoziazione ppp di**

debug e l'**autenticazione ppp di debug** prima di presupporre che l'errore di connessione sia necessariamente un problema ISDN

Campi Codice Causa

La Tabella 17-9 elenca i campi del codice causa ISDN che vengono visualizzati nel seguente formato all'interno dei comandi di debug:

```
i=0x y1 y2 z1 z2 [a1 a2]
```

Campi Cause Code ISDN

Campo	Descrizione valore
0x	I valori che seguono sono in formato esadecimale.
a1	8 - Codifica standard ITU-T.
s2	0—Utente 1—Rete privata che serve l'utente locale 2—Rete pubblica che serve l'utente locale 3—Rete di transito 4—Rete pubblica che serve l'utente remoto 5—Rete privata che serve l'utente remoto 7—Rete internazionale A—Rete oltre il punto di internetworking
z1	Classe (il numero esadecimale più significativo) del valore della causa. Fare riferimento alla tabella seguente per informazioni dettagliate sui valori possibili.
z2	Valore (il numero esadecimale meno significativo) del valore della causa. Fare riferimento alla tabella seguente per informazioni dettagliate sui valori possibili.
a1	(Facoltativo) Campo diagnostico che è sempre 8.
A2	(Facoltativo) Campo di diagnostica che corrisponde a uno dei valori seguenti: 0 - Sconosciuto 1 - Permanente 2 - Transitorio

Valori causa ISDN

Nella tabella seguente vengono descritti alcuni dei valori più comuni relativi alla causa dell'elemento informazioni causa, ovvero il terzo e il quarto byte del codice causa. Per informazioni più complete sui codici e i valori ISDN, vedere Informazioni sui codici causa di **disconnessione isdn di debug q931**.

Valore esadecimale	Causa	Spiegazione
81	Numero	Il numero ISDN è stato inviato allo

	non allocato (non assegnato)	switch nel formato corretto; tuttavia, il numero non è assegnato ad alcuna apparecchiatura di destinazione.
90	Cancellazione di chiamata normale	Si è verificata la normale cancellazione delle chiamate.
91	Utente occupato	Il sistema chiamato riconosce la richiesta di connessione ma non è in grado di accettare la chiamata perché tutti i canali B sono in uso.
92	Nessun utente che risponde	Impossibile completare la connessione. La destinazione non risponde alla chiamata.
93	Nessuna risposta dall'utente (avviso utente)	La destinazione risponde alla richiesta di connessione ma non la completa entro il tempo prescritto. Il problema si verifica all'estremità remota della connessione.
95	Chiamata rifiutata	La destinazione è in grado di accettare la chiamata, ma l'ha rifiutata per motivi sconosciuti.
9°C	Formato numero non valido	Impossibile stabilire la connessione. L'indirizzo di destinazione è stato presentato in un formato non riconoscibile oppure l'indirizzo di destinazione è incompleto.
9 SEPTIES	Normale, non specificato	Segnala l'occorrenza di un evento normale quando non si applica alcuna causa standard. Non è richiesta alcuna azione.
A2	Nessun circuito/ canale disponibile	Impossibile stabilire la connessione. Nessun canale appropriato disponibile per la chiamata.
A6	Rete non funzionante	Impossibile raggiungere la destinazione. La rete non funziona correttamente e la condizione potrebbe durare per un periodo di tempo prolungato. Un tentativo di riconnessione immediata non riuscirà.

CA	Circuito/canale richiesto non disponibile	L'apparecchiatura remota non è in grado di fornire il canale richiesto per un motivo sconosciuto. Questo potrebbe essere un problema temporaneo.
B2	Facilità richiesta non sottoscritta	L'apparecchiatura remota supporta il servizio supplementare richiesto solo in abbonamento. Questo è spesso un riferimento al servizio a lunga distanza.
B9	Supporto non autorizzato	L'utente ha richiesto una funzionalità di connessione fornita dalla rete, ma non è autorizzato a utilizzarla. Potrebbe trattarsi di un problema di sottoscrizione.
D8	Destinazione incompatibile	Indica un tentativo di connessione ad apparecchiature non ISDN. Ad esempio, a una linea analogica.
E0	Elemento di informazioni obbligatorio mancante	L'apparecchiatura ricevente ha ricevuto un messaggio che non include uno degli elementi di informazione obbligatori. Ciò è in genere dovuto a un errore del canale D. Se l'errore si verifica in modo sistematico, segnalarlo al provider di servizi ISDN.
E4	Contenuto dell'elemento di informazione non valido	L'apparecchiatura remota ha ricevuto un messaggio che include informazioni non valide nell'elemento di informazione. Ciò è in genere dovuto a un errore del canale D.

Chiamate in uscita CAS

Per le chiamate in uscita tramite CAS T1 o E1 e i modem digitali integrati, gran parte della risoluzione dei problemi è simile ad altre operazioni di risoluzione dei problemi DDR. Lo stesso vale anche per le chiamate modem integrate in uscita su una linea PRI. Le funzionalità univoche di una chiamata di questo tipo richiedono un debug speciale in caso di errore della chiamata.

Come per altre situazioni DDR, è necessario verificare che sia richiesto un tentativo di chiamata. A tale scopo, utilizzare **gli eventi di debug dialer**. Per ulteriori informazioni, fare riferimento al documento sulla verifica del funzionamento di Dialer.

Prima di poter effettuare una chiamata, è necessario allocare un modem per la chiamata. Per visualizzare questo processo e la chiamata successiva, utilizzare i comandi di debug seguenti:

- **debug modem**
- **debug modem csm**
- **debug cas**

Nota: il comando **debug cas** è apparso per la prima volta in IOS versione 12.0(7)T per AS5200 e AS5300. Le versioni precedenti di IOS usano un **servizio interno di** comandi di configurazione a livello di sistema insieme al comando exec **modem-mgmt debug rbs**:

Attivazione dei debug

```
router#conf t

Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#service internal
router(config)#^Z

router#modem-mgmt csm ?
  debug-rbs     enable rbs debugging
  no-debug-rbs  disable rbs debugging

router#modem-mgmt csm debug-rbs
router#
neat msg at slot 0: debug-rbs is on
neat msg at slot 0: special debug-rbs is on
```

Disattivazione dei debug

```
router#
router#modem-mgmt csm no-debug-rbs
neat msg at slot 0: debug-rbs is off
```

Nota: per eseguire il debug di queste informazioni su un AS5800 è necessario connettersi alla scheda trunk. Di seguito è riportato un esempio di una normale chiamata in uscita su un server CAS T1 con provisioning e configurazione per FXS-Ground-Start:

```
Mica Modem(1/0): Rcvd Dial String(5551111) [Modem receives digits from chat script]
CSM_PROC_IDLE: CSM_EVENT_MODEM_OFFHOOK at slot 1, port 0
CSM_RX_CAS_EVENT_FROM_NEAT:(A003):  EVENT_CHANNEL_LOCK at slot 1 and port 0
CSM_PROC_OC4_DIALING: CSM_EVENT_DSX0_BCHAN_ASSIGNED at slot 1, port 0
Mica Modem(1/0): Configure(0x1)
Mica Modem(1/0): Configure(0x2)
Mica Modem(1/0): Configure(0x5)
Mica Modem(1/0): Call Setup
neat msg at slot 0: (0/2): Tx RING_GROUND
Mica Modem(1/0): State Transition to Call Setup
neat msg at slot 0: (0/2): Rx TIP_GROUND_NORING [Telco switch goes OFFHOOK]
CSM_RX_CAS_EVENT_FROM_NEAT:(A003):  EVENT_START_TX_TONE at slot 1 and port 0
CSM_PROC_OC5_WAIT_FOR_CARRIER: CSM_EVENT_DSX0_START_TX_TONE at slot 1, port 0
neat msg at slot 0: (0/2): Tx LOOP_CLOSURE [Now the router goes OFFHOOK]
Mica Modem(1/0): Rcvd Tone detected(2)
Mica Modem(1/0): Generate digits:called_party_num=5551111 len=8
Mica Modem(1/0): Rcvd Digits Generated
CSM_PROC_OC5_WAIT_FOR_CARRIER: CSM_EVENT_ADDR_INFO_COLLECTED at slot 1, port 0
CSM_RX_CAS_EVENT_FROM_NEAT:(A003):  EVENT_CHANNEL_CONNECTED at slot 1 and port 0
CSM_PROC_OC5_WAIT_FOR_CARRIER: CSM_EVENT_DSX0_CONNECTED at slot 1, port 0
Mica Modem(1/0): Link Initiate
Mica Modem(1/0): State Transition to Connect
Mica Modem(1/0): State Transition to Link
```

```
Mica Modem(1/0): State Transition to Trainup
Mica Modem(1/0): State Transition to EC Negotiating
Mica Modem(1/0): State Transition to Steady State
Mica Modem(1/0): State Transition to Steady State Speedshifting
Mica Modem(1/0): State Transition to Steady State
```

I debug per T1 ed E1 con altri tipi di segnalazione sono simili.

Raggiungere questo punto del debug indica che i modem chiamanti e rispondenti sono stati addestrati e connessi e che i protocolli di livello superiore possono iniziare a negoziare. Se un modem è allocato correttamente per la chiamata in uscita ma la connessione non riesce a raggiungere tale punto, è necessario esaminare il T1. Fare riferimento al Capitolo 15 per informazioni sulla risoluzione dei problemi di T1.

Risoluzione dei problemi relativi a PPP

La risoluzione dei problemi relativi alla parte PPP di una connessione inizia quando si è certi che la connessione remota, ISDN o asincrona, è stata stabilita correttamente.

Èimportante comprendere l'aspetto di una sequenza PPP di debug riuscita prima di risolvere i problemi relativi alla negoziazione PPP. In questo modo, il confronto tra una sessione di debug PPP difettosa e una sequenza PPP di debug completata correttamente consente di risparmiare tempo e fatica.

Di seguito è riportato un esempio di sequenza PPP riuscita. Per una descrizione dettagliata dei campi di output, vedere Dettagli negoziazione LCP PPP.

```
Montecito#
Mar 13 10:57:13.415: %LINK-3-UPDOWN: Interface Async1, changed state to up
Mar 13 10:57:15.415: As1 LCP: O CONFREQ [ACKrcvd] id 2 len 25
Mar 13 10:57:15.415: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:15.415: As1 LCP:    AuthProto CHAP (0x0305C22305)
Mar 13 10:57:15.415: As1 LCP:    MagicNumber 0x1084F0A2 (0x05061084F0A2)
Mar 13 10:57:15.415: As1 LCP:    PFC (0x0702)
Mar 13 10:57:15.415: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:15.543: As1 LCP: I CONFACK [REQsent] id 2 len 25
Mar 13 10:57:15.543: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:15.543: As1 LCP:    AuthProto CHAP (0x0305C22305)
Mar 13 10:57:15.543: As1 LCP:    MagicNumber 0x1084F0A2 (0x05061084F0A2)
Mar 13 10:57:15.543: As1 LCP:    PFC (0x0702)
Mar 13 10:57:15.547: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:16.919: As1 LCP: I CONFREQ [ACKrcvd] id 4 len 23
Mar 13 10:57:16.919: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:16.919: As1 LCP:    MagicNumber 0x001327B0 (0x0506001327B0)
Mar 13 10:57:16.919: As1 LCP:    PFC (0x0702)
Mar 13 10:57:16.919: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:16.919: As1 LCP:    Callback 6  (0x0D0306)
Mar 13 10:57:16.919: As1 LCP: O CONFREJ [ACKrcvd] id 4 len 7
Mar 13 10:57:16.919: As1 LCP:    Callback 6  (0x0D0306)
Mar 13 10:57:17.047: As1 LCP: I CONFREQ [ACKrcvd] id 5 len 20
Mar 13 10:57:17.047: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:17.047: As1 LCP:    MagicNumber 0x001327B0 (0x0506001327B0)
Mar 13 10:57:17.047: As1 LCP:    PFC (0x0702)
Mar 13 10:57:17.047: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:17.047: As1 LCP: O CONFACK [ACKrcvd] id 5 len 20
Mar 13 10:57:17.047: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:17.047: As1 LCP:    MagicNumber 0x001327B0 (0x0506001327B0)
Mar 13 10:57:17.047: As1 LCP:    PFC (0x0702)
```

```
Mar 13 10:57:17.047: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:17.047: As1 LCP: State is Open
Mar 13 10:57:17.047: As1 PPP: Phase is AUTHENTICATING, by this end
Mar 13 10:57:17.047: As1 CHAP: O CHALLENGE id 1 len 28 from "Montecito"
Mar 13 10:57:17.191: As1 CHAP: I RESPONSE id 1 len 30 from "Goleta"
Mar 13 10:57:17.191: As1 CHAP: O SUCCESS id 1 len 4
Mar 13 10:57:17.191: As1 PPP: Phase is UP
Mar 13 10:57:17.191: As1 IPCP: O CONFREQ [Closed] id 1 len 10
Mar 13 10:57:17.191: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:17.303: As1 IPCP: I CONFREQ [REQsent] id 1 len 40
Mar 13 10:57:17.303: As1 IPCP:    CompressType VJ 15 slots CompressSlotID
 (0x0206002D0F01)
Mar 13 10:57:17.303: As1 IPCP:    Address 0.0.0.0 (0x030600000000)
Mar 13 10:57:17.303: As1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Mar 13 10:57:17.303: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:17.303: As1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Mar 13 10:57:17.303: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:17.303: As1 IPCP: O CONFREJ [REQsent] id 1 len 22
Mar 13 10:57:17.303: As1 IPCP:    CompressType VJ 15 slots CompressSlotID
 (0x0206002D0F01)
Mar 13 10:57:17.303: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:17.303: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:17.319: As1 CCP: I CONFREQ [Not negotiated] id 1 len 15
Mar 13 10:57:17.319: As1 CCP:    MS-PPC supported bits 0x00000001 (0x120600000001)
Mar 13 10:57:17.319: As1 CCP:    Stacker history 1 check mode EXTENDED (0x1105000104)
Mar 13 10:57:17.319: As1 LCP: O PROTREJ [Open] id 3 len 21 protocol CCP
Mar 13 10:57:17.319: As1 LCP:  (0x80FD0101000F12060000000111050001)
Mar 13 10:57:17.319: As1 LCP:  (0x04)
Mar 13 10:57:17.319: As1 IPCP: I CONFACK [REQsent] id 1 len 10
Mar 13 10:57:17.319: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:18.191: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1,
 changed state to up
Mar 13 10:57:19.191: As1 IPCP: TIMEout: State ACKrcvd
Mar 13 10:57:19.191: As1 IPCP: O CONFREQ [ACKrcvd] id 2 len 10
Mar 13 10:57:19.191: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:19.315: As1 IPCP: I CONFACK [REQsent] id 2 len 10
Mar 13 10:57:19.315: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:20.307: As1 IPCP: I CONFREQ [ACKrcvd] id 2 len 34
Mar 13 10:57:20.307: As1 IPCP:    Address 0.0.0.0 (0x030600000000)
Mar 13 10:57:20.307: As1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Mar 13 10:57:20.307: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:20.307: As1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Mar 13 10:57:20.307: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:20.307: As1 IPCP: O CONFREJ [ACKrcvd] id 2 len 16
Mar 13 10:57:20.307: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:20.307: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:20.419: As1 IPCP: I CONFREQ [ACKrcvd] id 3 len 22
Mar 13 10:57:20.419: As1 IPCP:    Address 0.0.0.0 (0x030600000000)
Mar 13 10:57:20.419: As1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Mar 13 10:57:20.419: As1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Mar 13 10:57:20.419: As1 IPCP: O CONFNAK [ACKrcvd] id 3 len 22
Mar 13 10:57:20.419: As1 IPCP:    Address 10.1.1.1 (0x03060A010101)
Mar 13 10:57:20.419: As1 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
Mar 13 10:57:20.419: As1 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
Mar 13 10:57:20.543: As1 IPCP: I CONFREQ [ACKrcvd] id 4 len 22
Mar 13 10:57:20.543: As1 IPCP:    Address 10.1.1.1 (0x03060A010101)
Mar 13 10:57:20.547: As1 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
Mar 13 10:57:20.547: As1 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
Mar 13 10:57:20.547: As1 IPCP: O CONFACK [ACKrcvd] id 4 len 22
Mar 13 10:57:20.547: As1 IPCP:    Address 10.1.1.1 (0x03060A010101)
Mar 13 10:57:20.547: As1 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
Mar 13 10:57:20.547: As1 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
Mar 13 10:57:20.547: As1 IPCP: State is Open
Mar 13 10:57:20.551: As1 IPCP: Install route to 10.1.1.1
```

Nota: i debug potrebbero essere visualizzati in un formato diverso. Nell'esempio viene mostrato il nuovo formato di output del debug PPP modificato in IOS versione 11.2(8). Vedere il Capitolo 16 per un esempio di debug PPP con le versioni precedenti di IOS.

Dettagli negoziazione LCP PPP

Timestamp	Descrizione
10:57:15.415	Richiesta di configurazione in uscita (O CONFREQ). Il server NAS invia un pacchetto di richiesta di configurazione PPP in uscita al client.
10:57:15.543	Riconoscimento configurazione in ingresso (I CONFACK). Il cliente accetta la richiesta PPP di Montecito.
10:57:16.919	Richiesta di configurazione in ingresso (CONFREQ). Il client desidera negoziare il protocollo di callback.
10:57:16.919	Rifiuto configurazione in uscita (O CONFREJ). Il NAS rifiuta l'opzione di richiamata.
10:57:17.047	Richiesta di configurazione in ingresso (CONFREQ). Il client richiede un nuovo set di opzioni. Si noti che questa volta Microsoft Callback non è richiesto.
10:57:17.047	Riconoscimento configurazione in uscita (O CONFACK). Il NAS accetta la nuova serie di opzioni.
10:57:17.047	Negoziazione LCP PPP completata. Lo stato LCP è "Aperto". Entrambe le parti hanno confermato (CONFACK) la richiesta di configurazione dell'altra parte (CONFREQ).
10:57:17,047 fino alle 10:57:17,191	Autenticazione PPP completata. Dopo la negoziazione LCP, viene avviata l'autenticazione. L'autenticazione deve essere eseguita prima del recapito di qualsiasi protocollo di rete, ad esempio IP. Entrambe le parti si autenticano con il metodo negoziato durante LCP. Montecito sta autenticando il client tramite CHAP.
10:57:20.551	Lo stato è aperto per il protocollo IPCP (IP Control Protocol). Viene negoziata e installata una route per il peer IPCP a cui viene assegnato l'indirizzo IP 1.1.1.1.

Link Control Protocol

Durante la negoziazione LCP si verificano in genere due tipi di problemi.

Il primo si verifica quando un peer effettua richieste di configurazione che l'altro peer non può o non riconosce. Sebbene si tratti di un'occorrenza frequente, può trattarsi di un problema se il

richiedente insiste sul parametro. Un esempio tipico è la negoziazione di AUTHTYPE (nota anche come "AuthProto"). Ad esempio, molti server di accesso sono configurati per accettare solo la protezione CHAP per l'autenticazione. Se il chiamante è configurato per eseguire solo l'autenticazione PAP, CONFREQ e CONFNAK verranno scambiati finché un peer o l'altro non interrompe la connessione.

```
BR0:1 LCP: I CONFREQ [ACKrcvd] id 66 len 14
BR0:1 LCP:    AuthProto PAP (0x0304C023)
BR0:1 LCP:    MagicNumber 0xBC6B9F91 (0x0506BC6B9F91)
BR0:1 LCP: O CONFNAK [ACKrcvd] id 66 len 9
BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
BR0:1 LCP: I CONFREQ [ACKrcvd] id 67 len 14
BR0:1 LCP:    AuthProto PAP (0x0304C023)
BR0:1 LCP:    MagicNumber 0xBC6B9F91 (0x0506BC6B9F91)
BR0:1 LCP: O CONFNAK [ACKrcvd] id 67 len 9
BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
BR0:1 LCP: I CONFREQ [ACKrcvd] id 68 len 14
BR0:1 LCP:    AuthProto PAP (0x0304C023)
BR0:1 LCP:    MagicNumber 0xBC6B9F91 (0x0506BC6B9F91)
BR0:1 LCP: O CONFNAK [ACKrcvd] id 68 len 9
BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
...
...
```

Il secondo tipo di problema in LCP è quando su uno o entrambi i peer vengono visualizzate solo le CONFREQ in uscita, come nell'esempio seguente. Di solito questo è il risultato di ciò che viene definito una *mancata corrispondenza di velocità* nel livello inferiore. Questa condizione può verificarsi in modalità asincrona o DDR ISDN.

```
Jun 10 19:57:59.768: As5 PPP: Phase is ESTABLISHING, Active Open
Jun 10 19:57:59.768: As5 LCP: O CONFREQ [Closed] id 64 len 25
Jun 10 19:57:59.768: As5 LCP: ACCM 0x000A0000 (0x0206000A0000)
Jun 10 19:57:59.768: As5 LCP: AuthProto CHAP (0x0305C22305)
Jun 10 19:57:59.768: As5 LCP: MagicNumber 0x5779D9D2 (0x05065779D9D2)
Jun 10 19:57:59.768: As5 LCP: PFC (0x0702)
Jun 10 19:57:59.768: As5 LCP: ACFC (0x0802)
Jun 10 19:58:01.768: As5 LCP: TIMEout: State REQsent
Jun 10 19:58:01.768: As5 LCP: O CONFREQ [REQsent] id 65 len 25
Jun 10 19:58:01.768: As5 LCP: ACCM 0x000A0000 (0x0206000A0000)
Jun 10 19:58:01.768: As5 LCP: AuthProto CHAP (0x0305C22305)
Jun 10 19:58:01.768: As5 LCP: MagicNumber 0x5779D9D2 (0x05065779D9D2)
Jun 10 19:58:01.768: As5 LCP: PFC (0x0702)
Jun 10 19:58:01.768: As5 LCP: ACFC (0x0802).
Jun 10 19:58:03.768: As5 LCP: TIMEout: State REQsent
Jun 10 19:58:03.768: As5 LCP: O CONFREQ [REQsent] id 66 len 25
Jun 10 19:58:03.768: As5 LCP: ACCM 0x000A0000 (0x0206000A0000)
Jun 10 19:58:03.768: As5 LCP: AuthProto CHAP (0x0305C22305)
Jun 10 19:58:03.768: As5 LCP: MagicNumber 0x5779D9D2 (0x05065779D9D2)
Jun 10 19:58:03.768: As5 LCP: PFC (0x0702)
Jun 10 19:58:03.768: As5 LCP: ACF.C (0x0802)
Jun 10 19:58:05.768: As5 LCP: TIMEout: State REQsent
Jun 10 19:58:05.768: As5 LCP: O CONFREQ [REQsent] id 67 len 25
!--- This repeats every two seconds until: Jun 10 19:58:19.768: As5 LCP: O CONFREQ [REQsent] id
74 len 25 Jun 10 19:58:19.768: As5 LCP: ACCM 0x000A0000 (0x0206000A0000) Jun 10 19:58:19.768:
As5 LCP: AuthProto CHAP (0x0305C22305) Jun 10 19:58:19.768: As5 LCP: MagicNumber 0x5779D9D2
(0x05065779D9D2) Jun 10 19:58:19.768: As5 LCP: PFC (0x0702) Jun 10 19:58:19.768: As5 LCP: ACFC
(0x0802) Jun 10 19:58:21.768: As5 LCP: TIMEout: State REQsent Jun 10 19:58:21.768: TTY5: Async
Int reset: Dropping DTR
```

Se la connessione è asincrona, la causa probabile è una mancata corrispondenza tra il router e il

modem. Ciò si verifica in genere quando non è stato possibile bloccare la velocità DTE del modem sulla velocità configurata della linea TTY. Il problema può essere rilevato su uno o su entrambi i peer, quindi verificare entrambi. Fare riferimento a Modem Cannot Send or Receive Data (Il modem non può inviare o ricevere dati) più indietro in questo capitolo.

Se i sintomi compaiono quando la connessione è su ISDN, è probabile che un peer si connetta a 56K, mentre l'altro a 64K. Anche se questa condizione è rara, si verifica. Il problema potrebbe essere uno o entrambi i colleghi, o forse la compagnia telefonica. Utilizzare **debug isdn q931** ed esaminare i messaggi SETUP su ciascuno dei peer. La capacità del supporto inviata da un peer deve corrispondere alla capacità del supporto visualizzata nel messaggio SETUP ricevuto sull'altro peer. Per risolvere il problema, configurare la velocità di composizione, 56K o 64K, nella **mappa dialer** dei comandi a livello di interfaccia o nella **velocità isdn** della **connessione dialer** configurata in una classe mappa.

```
*Mar 20 21:07:45.033: ISDN BR0: TX ->  SETUP pd = 8  callref = 0x2C
*Mar 20 21:07:45.037:         Bearer Capability i = 0x8890
*Mar 20 21:07:45.041:         Channel ID i = 0x83
*Mar 20 21:07:45.041:         Keypad Facility i = 0x35353533373539
```

Questa situazione può giustificare una chiamata al TAC Cisco. Raccogliere i seguenti output da entrambi i peer prima di chiamare il TAC:

- **show running-config**
- **show version**
- **debug isdn q931**
- **debug di eventi isdn**
- **negoziazione ppp di debug**

Autenticazione

L'autenticazione non riuscita è la causa più comune di un errore PPP. Nomi utente e password non configurati o non corrispondenti generano messaggi di errore nell'output del comando debug.

Nell'esempio seguente viene mostrato che il nome utente Goleta non dispone dell'autorizzazione per accedere al server NAS, che non dispone di un nome utente locale configurato per questo utente. Per risolvere il problema, usare il **comando username *name* password** password per aggiungere il nome utente "Goleta" al database AAA locale del NAS:

```
Mar 13 11:01:42.399: As2 LCP: State is Open
Mar 13 11:01:42.399: As2 PPP: Phase is AUTHENTICATING, by this end
Mar 13 11:01:42.399: As2 CHAP: O CHALLENGE id 1 len 28 from "Montecito"
Mar 13 11:01:42.539: As2 CHAP: I RESPONSE id 1 len 30 from "Goleta"
Mar 13 11:01:42.539: As2 CHAP: Unable to validate Response.  Username Goleta not found
Mar 13 11:01:42.539: As2 CHAP: O FAILURE id 1 len 26 msg is "Authentication failure"
Mar 13 11:01:42.539: As2 PPP: Phase is TERMINATING
```

L'esempio seguente mostra che il nome utente "Goleta" è configurato sul NAS. Il confronto delle password non è riuscito. Per risolvere il problema, utilizzare il **comando username *name* password** password per specificare la password di login corretta per Goleta:

```
Mar 13 11:04:06.843: As3 LCP: State is Open
Mar 13 11:04:06.843: As3 PPP: Phase is AUTHENTICATING, by this end
Mar 13 11:04:06.843: As3 CHAP: O CHALLENGE id 1 len 28 from "Montecito"
```

```
Mar 13 11:04:06.987: As3 CHAP: I RESPONSE id 1 len 30 from "Goleta"
Mar 13 11:04:06.987: As3 CHAP: O FAILURE id 1 len 25 msg is "MD/DES compare failed"
Mar 13 11:04:06.987: As3 PPP: Phase is TERMINATING
```

Per ulteriori informazioni sull'autenticazione PAP, consultare il documento sulla configurazione e la risoluzione dei problemi relativi al protocollo PAP (PPP Password Authentication Protocol).

Protocollo di controllo di rete

Dopo che i peer hanno completato l'autenticazione richiesta, la negoziazione passa alla fase NCP. Se entrambi i peer sono configurati correttamente, la negoziazione NCP potrebbe essere simile all'esempio seguente, che mostra un PC client che accede e negozia con un NAS:

```
solvang# show debug
Generic IP:
IP peer address activity debugging is on
PPP:
PPP protocol negotiation debugging is on

*Mar  1 21:35:04.186: As4 PPP: Phase is UP
*Mar  1 21:35:04.190: As4 IPCP: O CONFREQ [Not negotiated] id 1 len 10
*Mar  1 21:35:04.194: As4 IPCP:    Address 10.1.2.1 (0x03060A010201)
*Mar  1 21:35:04.282: As4 IPCP: I CONFREQ [REQsent] id 1 len 28
*Mar  1 21:35:04.282: As4 IPCP:    CompressType VJ 15 slots CompressSlotID
 (0x0206002D0F01)
*Mar  1 21:35:04.286: As4 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  1 21:35:04.290: As4 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  1 21:35:04.298: As4 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  1 21:35:04.306: As4 IPCP: O CONFREJ [REQsent] id 1 len 10
*Mar  1 21:35:04.310: As4 IPCP:    CompressType VJ 15 slots CompressSlotID
 (0x0206002D0F01)
*Mar  1 21:35:04.314: As4 CCP: I CONFREQ [Not negotiated] id 1 len 15
*Mar  1 21:35:04.318: As4 CCP:    MS-PPC supported bits 0x00000001 (0x120600000001)
*Mar  1 21:35:04.318: As4 CCP:    Stacker history 1 check mode EXTENDED (0x1105000104)
*Mar  1 21:35:04.322: As4 LCP: O PROTREJ [Open] id 3 len 21 protocol CCP
*Mar  1 21:35:04.326: As4 LCP:  (0x80FD0101000F12060000000111050001)
*Mar  1 21:35:04.330: As4 LCP:  (0x04)
*Mar  1 21:35:04.334: As4 IPCP: I CONFACK [REQsent] id 1 len 10
*Mar  1 21:35:04.338: As4 IPCP:    Address 10.1.2.1 (0x03060A010201)
*Mar  1 21:35:05.186: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async4,
 changed state to up
*Mar  1 21:35:07.274: As4 IPCP: I CONFREQ [ACKrcvd] id 2 len 22
*Mar  1 21:35:07.278: As4 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  1 21:35:07.282: As4 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  1 21:35:07.286: As4 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  1 21:35:07.294: As4 IPCP: O CONFNAK [ACKrcvd] id 2 len 22
*Mar  1 21:35:07.298: As4 IPCP:    Address 10.1.2.2 (0x03060A010202)
*Mar  1 21:35:07.302: As4 IPCP:    PrimaryDNS 10.2.2.3 (0x81060A020203)
*Mar  1 21:35:07.310: As4 IPCP:    SecondaryDNS 10.2.3.1 (0x83060A020301)
*Mar  1 21:35:07.426: As4 IPCP: I CONFREQ [ACKrcvd] id 3 len 22
*Mar  1 21:35:07.430: As4 IPCP:    Address 10.1.2.2 (0x03060A010202)
*Mar  1 21:35:07.434: As4 IPCP:    PrimaryDNS 10.2.2.3 (0x81060A020203)
*Mar  1 21:35:07.442: As4 IPCP:    SecondaryDNS 10.2.3.1 (0x83060A020301)
*Mar  1 21:35:07.446: ip_get_pool: As4: validate address = 10.1.2.2
*Mar  1 21:35:07.450: ip_get_pool: As4: using pool default
*Mar  1 21:35:07.450: ip_get_pool: As4: returning address = 10.1.2.2
*Mar  1 21:35:07.454: set_ip_peer_addr: As4: address = 10.1.2.2 (3) is redundant
*Mar  1 21:35:07.458: As4 IPCP: O CONFACK [ACKrcvd] id 3 len 22
*Mar  1 21:35:07.462: As4 IPCP:    Address 10.1.2.2 (0x03060A010202)
*Mar  1 21:35:07.466: As4 IPCP:    PrimaryDNS 10.2.2.3 (0x81060A020203)
*Mar  1 21:35:07.474: As4 IPCP:    SecondaryDNS 10.2.3.1 (0x83060A020301)
```

```
*Mar  1 21:35:07.478: As4 IPCP: State is Open
*Mar  1 21:35:07.490: As4 IPCP: Install route to 10.1.2.2
```

Dettagli negoziazione NCP PPP

Timestamp	Descrizione
21:35:04.190	Richiesta di configurazione in uscita (O CONFREQ). Il server NAS invia al peer un pacchetto di richiesta di configurazione PPP in uscita contenente il relativo indirizzo IP.
21:35:04.282	CONFREQ in arrivo. Il peer richiede di eseguire la compressione dell'intestazione VJ. Richiede un indirizzo IP per se stesso, nonché gli indirizzi dei server DNS primario e secondario.
21:35:04.306	Config-Reject in uscita (CONFREJ). La compressione dell'intestazione VJ è rifiutata.
21:35:04.314 fino alle 21:35:04.330	Il peer invia una richiesta per eseguire Compression Control Protocol; l'intero protocollo viene rifiutato dal server NAS tramite un messaggio PROTREJ. Il peer non deve tentare (e non tenta di rieseguire il CCP.
21:35:04.334	Il peer riconosce l'indirizzo IP del server NAS con una CONFACK.
21:35:07.274	CONFREQ in arrivo. Il peer non richiede più la compressione dell'intestazione VJ, ma richiede comunque un indirizzo IP per se stesso, nonché indirizzi dei server DNS primario e secondario.
21:35:07.294	Il server NAS invia un CONFNAK contenente l'indirizzo che il peer deve utilizzare e gli indirizzi dei server DNS primario e secondario.
21:35:07.426	Il peer invia gli indirizzi al NAS; tentativo di confermare la corretta ricezione degli indirizzi.
21:35:07.458	Il NAS riconosce gli indirizzi con un CONFACK.
21:35:07.478	Dopo aver rilasciato una CONFACK su ciascun lato della connessione, la negoziazione viene completata. Il comando **show interfaces Async4** sul NAS mostra "IPCP: Apri".
21:35:07.490	Nella tabella di routing del server NAS è installato un percorso host al peer remoto.

I peer possono negoziare contemporaneamente più di un protocollo di layer 3. Non è raro, ad esempio, vedere che IP e IPX vengono negoziati. È inoltre possibile che un protocollo riesca a negoziare, mentre l'altro no.

Risoluzione dei problemi NCP

Tutti i problemi che si verificano durante la negoziazione NCP possono in genere essere ricondotti

alle configurazioni dei peer di negoziazione. Se la negoziazione PPP non riesce durante la fase NCP, fare riferimento ai passaggi seguenti:

1. Verificare la configurazione del protocollo di interfacciaEsaminare l'output del comando exec privilegiato **show running-config**. Verificare che l'interfaccia sia configurata per supportare il protocollo da eseguire sulla connessione.
2. Verifica indirizzo interfacciaConfermare che per l'interfaccia in questione sia configurato un indirizzo. Se si utilizza il comando **ip unnumber [*interface-name*]** o **ipx ppp-client loopback [*number*]**, verificare che l'interfaccia a cui si fa riferimento sia configurata con un indirizzo.
3. Verifica disponibilità indirizzi clientSe si prevede che il server NAS invii un indirizzo IP al chiamante, assicurarsi che tale indirizzo sia disponibile. L'indirizzo IP da comunicare al chiamante può essere ottenuto tramite uno dei seguenti metodi:Configurare localmente sull'interfaccia. Controllare la configurazione dell'interfaccia per il comando **peer default ip address a.b.c.d**. In pratica, questo metodo dovrebbe essere utilizzato solo sulle interfacce che accettano connessioni da un singolo chiamante, ad esempio su un'interfaccia asincrona (*non* asincrona di gruppo).Pool di indirizzi configurato localmente sul server NAS. L'interfaccia deve avere il comando **peer default ip address pool [*nome-pool*]**. Inoltre, il pool deve essere definito a livello di sistema con il comando **ip local pool [*nome-pool*] [*primo-indirizzo*] [*ultimo-indirizzo*]**. L'intervallo di indirizzi definito nel pool deve essere sufficientemente ampio da contenere il numero massimo di chiamanti connessi contemporaneamente supportato dal server NAS.Server DHCP. L'interfaccia NAS deve essere configurata con il comando **peer default ip address dhcp**. Inoltre, il server NAS deve essere configurato in modo da puntare a un server DHCP con il comando di configurazione globale **ip dhcp-server [*address*]**.AAA Se si usa TACACS+ o RADIUS per l'autorizzazione, il server AAA può essere configurato in modo da consegnare un indirizzo IP specifico a un determinato chiamante ogni volta che questo si connette. Per ulteriori informazioni, vedere il Capitolo 16.
4. Verifica configurazione indirizzi serverPer restituire gli indirizzi configurati dei server dei nomi di dominio o dei server Windows NT in risposta alle richieste BOOTP, verificare che i comandi a livello globale **async-bootp dns-server [*address*]** e **async-bootp nbns-server [*address*]** siano configurati.**Nota:** mentre il comando **async-bootp subnet-mask [*mask*]** può essere configurato sul server NAS, la subnet mask *non* verrà negoziata tra il server NAS e un PC client dial-in PPP. A causa della natura delle connessioni point-to-point, il client utilizza automaticamente l'indirizzo IP del server NAS (appreso durante la negoziazione IPCP) come gateway predefinito. La subnet mask non è necessaria in questo ambiente point-to-point. Il PC sa che se l'indirizzo di destinazione non corrisponde all'indirizzo locale, il pacchetto deve essere inoltrato al gateway predefinito (NAS) che viene sempre raggiunto tramite il collegamento PPP.

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

- Pagina T1/E1: Risoluzione dei problemi
- Guida alle soluzioni di composizione Cisco IOS
- Monitoraggio e manutenzione dell'interfaccia T1/E1
- Risoluzione dei problemi di negoziazione PPP
- Risoluzione dei problemi dei modem
- Comandi di debug per il modem
- Risoluzione dei problemi ISDN
- Risoluzione dei problemi di T1 PRI
- Documentazione e supporto tecnico – Cisco Systems