MMP (Multicassis Multilink PPP) (parte 2)

Sommario

Introduzione

Questo documento continua a descrivere il supporto per Multilink PPP (MP) in un ambiente "stack" o multicassis (talvolta chiamato MMP, per *Multicassis Multilink PPP*), sulle piattaforme access server di Cisco Systems.

Questo documento è la seconda parte di un documento composto da due parti. Per ulteriori informazioni, fare riferimento alla prima parte di questo documento.

Prerequisiti

I prerequisiti per questo documento sono illustrati nella prima parte del presente documento.

Esempi

AS5200 in uno stack (con dialer)

Quando i dialer sono configurati sulle interfacce fisiche, non è necessario specificare l'interfaccia del modello virtuale. L'interfaccia di accesso virtuale funge da interfaccia passiva ed è dotata di un collegamento diretto tra l'interfaccia della connessione e le interfacce fisiche associate a tale

interfaccia.

In breve, è sufficiente definire il nome del gruppo di stack, la password comune e i membri del gruppo di stack su tutti i membri dello stack. Non è stata definita alcuna interfaccia di modello virtuale, come illustrato nell'esempio seguente:

```
systema#config
  sgbp group stackq
  sgbp member systemb 1.1.1.2
  sgbp member systemc 1.1.1.3

  username stackq password therock

  int dialer 1
  ip unnum e0
  dialer map .....
  encap ppp
  ppp authen chap
  dialer-group 1
  ppp multilink

  controller T1 0
  framing esf
  linecode b8zs
  pri-group timeslots 1-24

  interface Serial0:23
  no ip address
  encapsulation ppp
  dialer in-band
  dialer rotary 1
  dialer-group 1
```

L'esempio seguente proviene da un controller E1:

```
controller E1 0
  framing crc4
  linecode  hdb3
  pri-group timeslots 1-31
  interface Serial0:15
  no ip address
  encapsulation ppp
  no ip route-cache
  ppp authentication chap
  ppp multilink
```

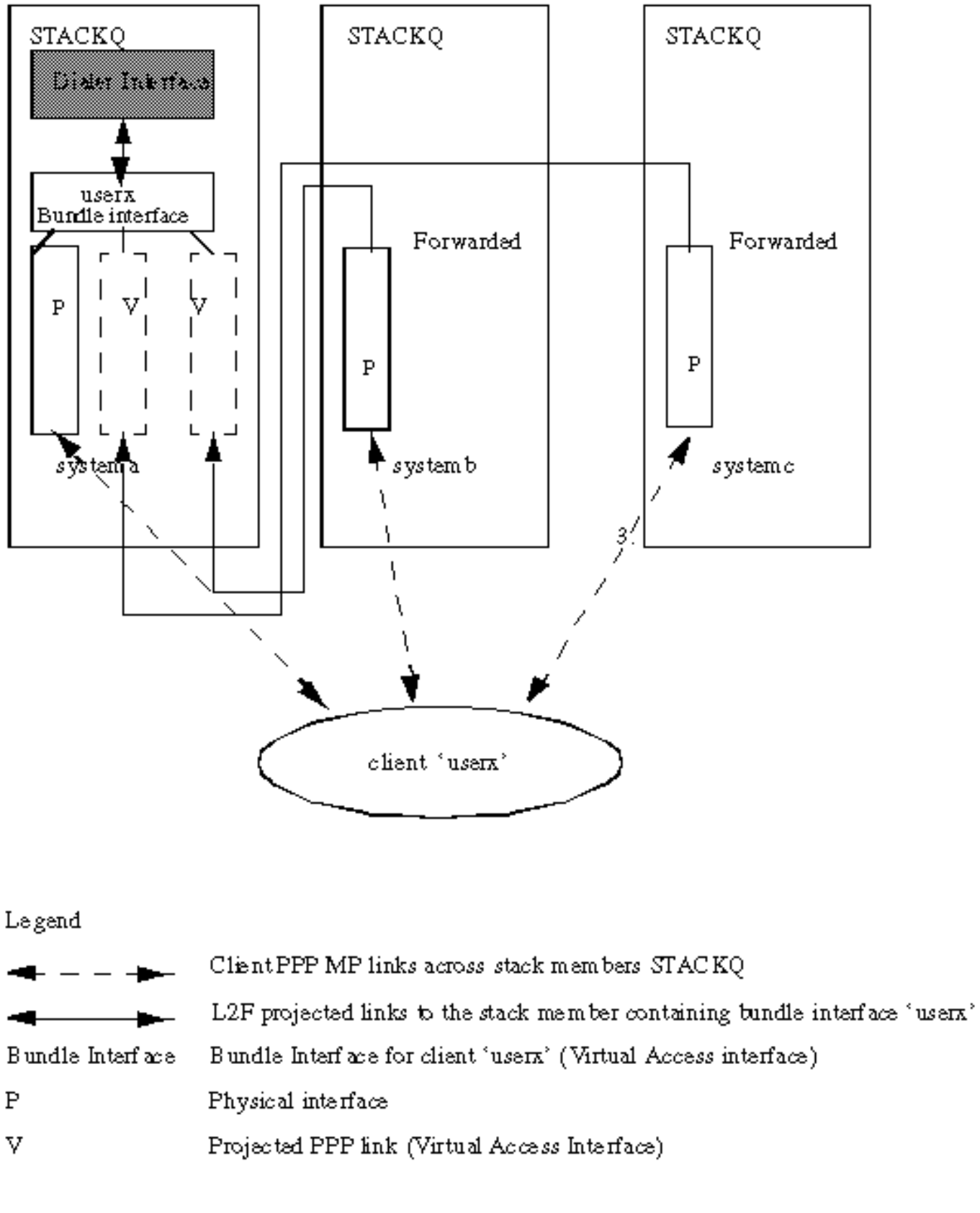
Una volta creata, l'interfaccia del bundle viene duplicata solo con i comandi PPP dell'interfaccia del dialer. I collegamenti PPP proiettati successivamente vengono duplicati anche con i comandi PPP dall'interfaccia del dialer. Nella figura 3 viene mostrata la posizione dell'interfaccia di connessione remota sopra l'interfaccia del pacchetto. Confrontare questa figura con la Figura 2, in cui non è presente un'interfaccia dialer.

I PRI e i BRI sono interfacce dialer per impostazione predefinita; un PRI configurato senza un dialer esplicito (tramite il comando **dialer rotary**) è ancora un'interfaccia dialer su Serial0:23, come mostrato nell'esempio seguente:

```
interface Serial0:23
  ip unnum e0
```

```
dialer map .....
encap ppp
ppp authen chap
dialer-group 1
dialer rot 1
ppp multilink
```

Figura 3: Stack Group-stackq costituito da **systema**, **systemb** e **systemc**. il collegamento di **system** è configurato sull'interfaccia dialer.



Utilizzo di un server offload

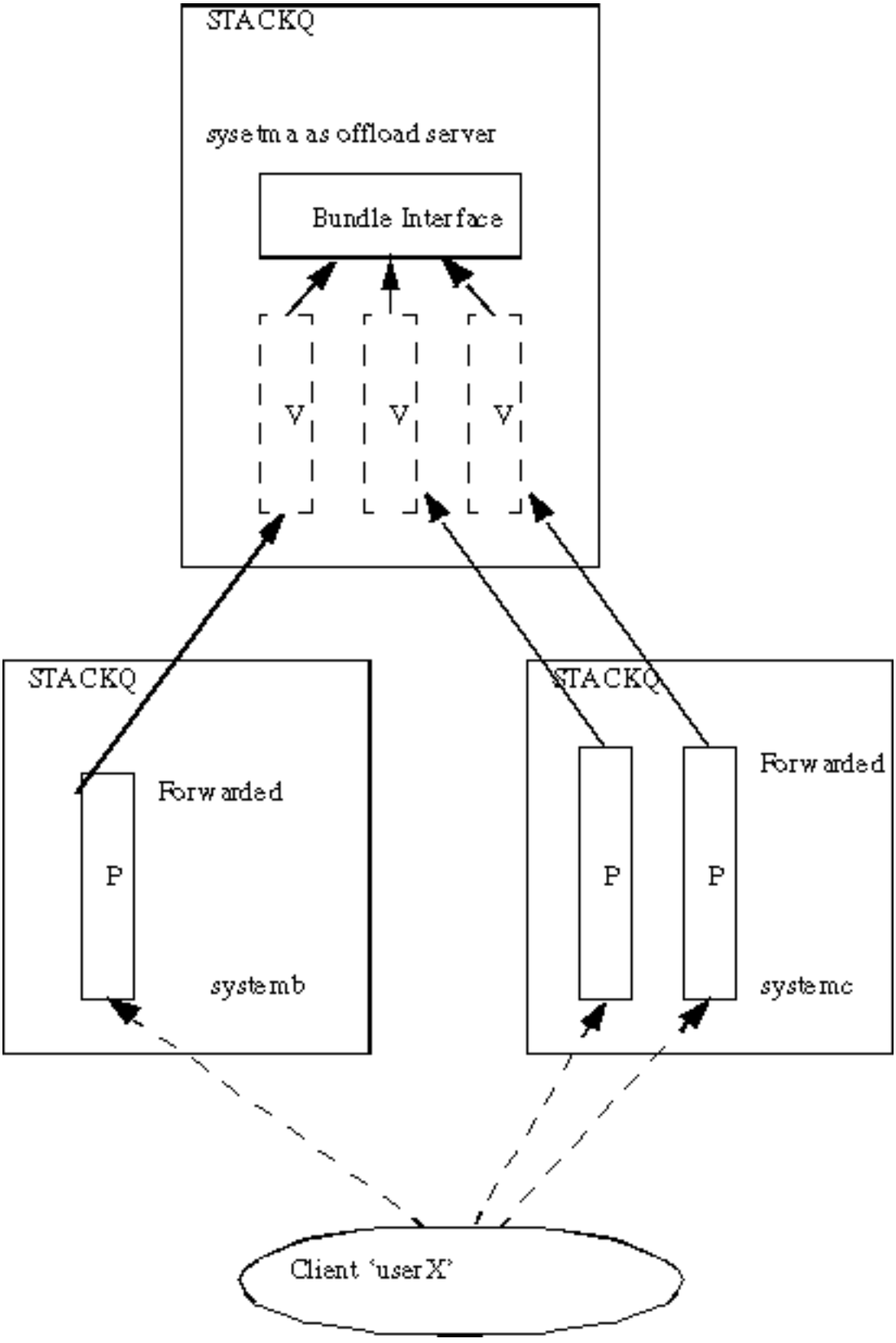
`system` è designato come server offload (utilizzando il comando **sgbp seed-bid**). Tutti gli altri membri dello stack devono essere definiti con il comando **sgbp seed-bid predefinito** (o, se non si definisce **il** comando **sgbp seed-bid**, viene utilizzato per impostazione predefinita).

```
systema#config
  multilink virtual-template 1
  sgbp group stackq
  sgbp member systemb 1.1.1.2
  sgbp member systemc 1.1.1.3
  sgbp seed-bid offload
  username stackq password therock

  interface virtual-template 1
  ip unnumbered e0
  :

  ppp authen chap
  ppp multilink
```

Figura 4: **system** come server offload.



Server offload con interfacce fisiche

Se il server offload designato dispone anche di interfacce fisiche (ad esempio, PRI) che desiderano servire lo stesso telco hunt group degli altri membri dello stack, è possibile configurarlo in modo tale da combinare le configurazioni mostrate nelle sezioni di questo documento intitolate AS5200 in uno stack (con dialer) e Uso di un server offload.

Un collegamento PPP proiettato scaricato e le relative interfacce di bundle si basano su modelli virtuali per un'origine di configurazione. Una connessione che ha il *primo collegamento* arriva a un

dispositivo fisico collegato a un'interfaccia dialer, e l'origine della configurazione per l'interfaccia bundle e tutti i successivi collegamenti PPP proiettati è la configurazione dell'interfaccia dialer. Pertanto, queste variazioni coesistono, a seconda del membro dello stack da cui proviene il primo collegamento.

Questa configurazione non è consigliata a causa della complessità delle configurazioni richieste sulle interfacce della connessione telefonica e del modello virtuale.

Interfacce asincrone, seriali e altre interfacce non dialer

Sebbene sia possibile configurare dispositivi seriali e asincroni come interfacce dialer (in questo caso viene ripristinato AS5200 in uno stack (con dialer), come mostrato nella sezione in questione del presente documento), è possibile scegliere di supportare MP multicassis senza alcuna configurazione dialer per interfacce asincrone, seriali e altre interfacce non dialer. L'origine di tutte le configurazioni viene quindi definita nell'interfaccia del modello virtuale, come illustrato di seguito.

```
#config
  multilink virtual-template 1
  sgbp group stackq
  sgbp member systemb 1.1.1.2
  sgbp member systemc 1.1.1.3
  username stackq password therock
  interface virtual-template 1
  ip unnumbered e0
  :
  ppp authen chap
  ppp multilink

  int async 1
  encap ppp
  ppp multilink
  ppp authen chap
  :

  line 1
  login
  autoselect ppp
  autoselect during-login
  speed 38400
  flow hardware
```

Chiamata in uscita da un multicassis

Al momento, la configurazione multi-chassis **non supporta le chiamate in uscita**, perché il protocollo L2F (Layer 2 Forwarding) non supporta le chiamate in uscita.

Di conseguenza, non è possibile per il server di offload (quando un percorso viene falsificato, viene usato un profilo dialer e così via) avviare una chiamata sul membro dello stack front-end nello stesso gruppo di stack. Tutte le route falsificate devono essere installate sui membri dello stack front-end, in quanto sono quelle con le connessioni di composizione fisiche (ad esempio PRI).

Di seguito sono riportate alcune soluzioni alternative.

- Quando si esegue il comando **sgbp ppp-forward** sul membro dello stack front-end, tutte le

chiamate PPP e PPP multilink vengono inoltrate automaticamente al vincitore dell'offerta Stack Group Bidding Protocol (SGBP), ad esempio un server offload.Ènecessario affidarsi alla connessione remota del Network Access Server (NAS) e lasciare che la convergenza del routing IP (solo per IP) faccia il suo corso. Ad esempio, per comporre 1.1.1.1, inserire questo indirizzo nell'istruzione della mappa di composizione sul NAS e inserire un percorso statico sul NAS, come indicato di seguito:

```
ip route 1.1.1.1 255.255.255.255 serial0:23
int serial0:23
ip address 3.3.3.3 255.0.0.0
dialer map ip 1.1.1.1 howard 7771234
```

Quando la composizione si connette al peer remoto, viene stabilita la connessione PPP tra il peer remoto e il server offload. Il membro dello stack front-end è stato completamente ignorato. Il protocollo PPP sul server di offload installa quindi una route host al peer—1.1.1.1. A questo punto, il protocollo di routing IP converge dalla route host al server di offload perché la metrica di routing gravita la route in tale posizione.**Nota:** la convergenza del ciclo determina una latenza.

- Se il comando **sgbp ppp-forward** non è definito sul membro dello stack front-end, solo le chiamate PPP multilink vengono inoltrate automaticamente al vincitore dell'offerta SGBP, ad esempio un server offload. In questo modo, un dialer tra il membro dello stack front-end e un peer remoto si estende sulla connessione PPP tra il front-end e il peer remoto, come se il NAS non facesse parte di uno stack group.**Nota:** ciò accade se la connessione è in modalità PPP diritta (e non PPP multilink).

Connessione a uno chassis multicast

Se il routing IP (ad esempio EIGRP (Enhanced Interior Gateway Routing Protocol) e OSPF (Open Shortest Path First) vengono scambiati tra il client e il membro dello stack che alla fine si aggiudica l'offerta (ad esempio il server offload), procedere come segue:

Impedisci installazione di un percorso connesso sul lato client

Configurare il client 1.1.1.2, dove 1.1.1.2 è l'indirizzo del server NAS (il server di inoltro del frame trasparente), come mostrato di seguito.

```
int bri0

dialer map 1.1.1.2 ....
```

Se, ad esempio, è in esecuzione il protocollo EIGRP tra il client e il server offload, la tabella di routing nel server offload indica che per ottenere la versione 1.1.1.2 la route deve passare attraverso l'interfaccia di accesso virtuale. Infatti il protocollo IPCP (IP Control Protocol) PPP sul lato client installa una route connessa 1.1.1.2 all'interfaccia BRI. EIGRP quindi annuncia questa route al server offload tramite la sessione PPP (su L2F). Il protocollo EIGRP sul server offload indica quindi che per ottenere la versione 1.1.1.2, deve essere indirizzato al client. Il percorso del client 1.1.1.1 è l'interfaccia di accesso virtuale.

A questo punto, il pacchetto è destinato al client 1.1.1.1. Il routing IP invia il pacchetto all'interfaccia di accesso virtuale. L'interfaccia di accesso virtuale incapsula il protocollo IP/User Data Protocol (UDP)/L2F/PPP e invia il pacchetto al NAS L2F—1.1.1.2. A questo punto, tutto è

normale. Quindi, invece di inviare il pacchetto attraverso (ad esempio) l'interfaccia Ethernet, il routing IP lo invia nuovamente tramite l'interfaccia di accesso virtuale. Questo perché la tabella di routing indica che per raggiungere il NAS, deve passare attraverso il client. In questo modo viene creato un loop di routing e vengono disabilitati efficacemente gli input e gli output sul tunnel L2F.

Per evitare questo problema, non consentire a IPCP di installare una route connessa sul lato client.

Nota: ciò si verifica solo quando tra il client e Cisco Home Gateway è in esecuzione un protocollo di routing IP.

La configurazione del client è la seguente:

```
int bri0

no peer neighbor-route
```

Mappe dialer sul client

Quando il client effettua una chiamata a un ambiente multicassis, definire sempre i dialer per ogni potenziale vincitore del bundle multilink. Ad esempio, se lo stack a più chassis contiene quattro server offload, dovrebbero essere definite quattro mappe dialer sul lato client.

Ad esempio:

```
client 1.1.1.1

int bri0

dialer map 1.1.1.3 ...
```

In questo esempio, 1.1.1.3 è solo un server offload.

Un pacchetto destinato alla versione 1.1.1.2 viene indirizzato all'BRI e il dialer compone la destinazione perché esiste una corrispondenza nella mappa del dialer. Il server offload 1.1.1.4 vince effettivamente l'offerta e la sessione PPP viene proiettata in tale posizione. Il protocollo EIGRP viene scambiato tra il client e il server offload. La tabella di routing IP sul client è compilata con una route 1.1.1.4 (server offload) a BRI0. Ora, sul client, un pacchetto destinato a 1.1.1.4 viene instradato a BRI0. Il dialer, tuttavia, non può comporre il numero perché non esiste una corrispondenza di dialer.

Nota: definire sempre mappe dialer per tutti i potenziali vincitori di offerte SGBP sui client ogni volta che l'accesso ai server offload è un requisito dei client.

Configurazione e limitazioni

- L'immagine j-image aziendale è necessaria per MP multicassis.
- Èpossibile definire un solo gruppo di stack per ciascun server di accesso.
- I collegamenti WAN ad alta latenza tra i membri dello stack, che causano ritardi nel riassemblaggio del pannello di gestione, possono causare l'inefficienza del pannello di

gestione multicassis.
- Le interfacce sono supportate per dispositivi PRI, [M]BRI, seriali e asincroni.
- Dialout non supportato.

Configurazione delle configurazioni dell'interfaccia per protocollo

Per motivi pratici, non configurare un indirizzo di protocollo specifico nel modello virtuale.

```
interface virtual-template 1

ip address 1.1.1.2 255.0.0.0

:
```

L'interfaccia del modello virtuale funge da modello da cui viene duplicato dinamicamente qualsiasi numero di interfacce di accesso virtuale. Non specificare un indirizzo specifico del protocollo per interfaccia per l'interfaccia del modello virtuale. Poiché un indirizzo IP deve essere univoco per ogni interfaccia di rete, è errato specificare un indirizzo IP univoco nell'interfaccia del modello virtuale. Eseguire invece le operazioni seguenti:

```
interface virtual-template 1

ip unnum e0

:
```

Configurazione delle configurazioni del protocollo globale

Un client che chiama un singolo router di accesso e si aspetta che il server di accesso abbia un indirizzo globale univoco (ad esempio DECnet) ora in realtà chiama il gruppo di stack multicassis multilink composto da diversi server di accesso. In questo tipo di situazione, terminare il gruppo di stack in modo deterministico su un singolo server di accesso. A tale scopo, eseguire il comando **sgbp seed-bid offload** sul server di accesso designato (o specificare l'offerta più alta).

Risoluzione dei problemi

In caso di problemi, è innanzitutto necessario tornare a un singolo membro dello stack e disabilitare tutti gli altri membri. Verificare quindi le connessioni PPP multilink e seguire la normale autenticazione CHAP (Challenge Handshake Authentication Protocol) e la configurazione dell'interfaccia per rilevare eventuali errori di configurazione e così via. Una volta verificato il corretto funzionamento, abilitare gli altri membri dello stack, quindi procedere come segue:

1. Accertarsi che SGBP sia attivo e in esecuzione.
2. Debug del collegamento multiplo PPP.
3. Eseguire il debug di VPN e L2F.

Verifica del corretto funzionamento di SGBP

Utilizzare il comando **show sgbp** per verificare che tutti gli Stati membri siano attivi. In caso contrario, verificare gli stati IDLE, AUTHOK o ACTIVE. Come accennato in precedenza, lo stato IDLE è valido per tutti i membri dello stack remoti intenzionalmente inattivi.

Se si verifica il problema descritto sopra, attivare i comandi **debug sgbp hellos** e **debug sgbp error**. L'autenticazione tra due membri dello stack, ad esempio tra `systema` e `systemb`, deve essere la seguente (in `systema`):

```
systema# debug sgdp hellos

%SGBP-7-CHALLENGE: Send Hello Challenge to systemb group stackq
%SGBP-7-CHALLENGED: Hello Challenge message from member systemb (1.1.1.2)
%SGBP-7-RESPONSE: Send Hello Response to systemb group stackq
%SGBP-7-CHALLENGE: Send Hello Challenge to systemb group stackq
%SGBP-7-RESPONDED: Hello Response message from member systemb (1.1.1.2)
%SGBP-7-AUTHOK: Send Hello Authentication OK to member systemb (1.1.1.2)
%SGBP-7-INFO: Addr = 1.1.1.2 Reference = 0xC347DF7
%SGBP-5-ARRIVING: New peer event for member systemb
```

`systema` invia una richiesta di verifica in stile CHAP e riceve una risposta da `systemb`. Analogamente, `systemb` invia una richiesta e riceve una risposta da `systema`.

Se l'autenticazione non riesce, viene visualizzato quanto segue:

```
%SGBP-7-AUTHFAILED - Member systemb failed authentication
```

Ciò significa che la password `systemb` remota per stackq non corrisponde alla password definita in `systema`.

```
%SGBP-7-NORESP -Fail to respond to systemb group stackq, may not have password
```

Ciò significa che `system` non ha un nome utente o una password definiti localmente o tramite TACACS+.

In generale, definire un segreto comune a tutti i membri dello stack per lo stack group `stackq`. È possibile definirli localmente o tramite TACACS+.

Un nome utente locale definito su ciascun membro dello stack è:

```
username stackq password blah
```

Questo segreto comune è quello di facilitare le offerte e l'arbitrato del membro dello stack SGBP.

Per informazioni sull'autenticazione dei collegamenti PPP quando un client remoto effettua una chiamata ai membri dello stack, consultare la sezione Debug PPP Multilink di questo documento.

In caso di problemi di cablaggio o routing, un errore comune è quello di avere l'indirizzo IP di origine del membro dello stack (che in realtà viene ricevuto nel messaggio hello SGBP) diverso dall'indirizzo IP definito localmente per lo stesso membro dello stack.

```
systema#debug sgbp error
%SGBP-7-DIFFERENT - systemb's addr 1.1.1.2 is different from hello's addr 3.3.4.5
```

Ciò significa che l'indirizzo IP di origine dell'hello SGBP ricevuto da `systemb` non corrisponde all'indirizzo IP configurato localmente per `systemb` (tramite il comando **sgbp member**). Per risolvere il problema, andare su `systemb` e verificare la presenza di più interfacce tramite le quali l'hello SGBP può trasmettere il messaggio.

Un'altra causa comune degli errori è:

```
%SGBP-7-MISCONF, Possible misconfigured member routerk (1.1.1.6)
```

Ciò significa che non si dispone di un `system` definito localmente, a differenza di un altro membro dello stack.

Debug del collegamento multiplo PPP

La prima cosa da verificare è se il client e il membro dello stack sono stati autenticati correttamente sul protocollo PPP.

In questo esempio viene illustrata l'autenticazione CHAP, in quanto più complessa. Ad esempio, si usa una piattaforma Cisco come client con i nomi utente locali (anche TACACS+ (Terminal Access Controller Access Control System Plus) è supportato, ma non viene mostrato qui).

Utente client x	Tutti i membri dello stack **stackq**
#**config** username stackq password blah	#**config** username userx password blah

Nessuna Interfaccia Dialer Coinvolta

Poiché sul server offload non è presente un'interfaccia di connessione, è necessario che l'*interfaccia di configurazione* delle interfacce di accesso virtuale sia configurata da un'altra *origine*. La risposta è interfacce di modelli virtuali.

1. Innanzitutto, verificare che il numero di modello virtuale globale multilink sia definito su ciascun membro dello stack.
   ```
   #config
   Multilink virtual-template 1
   ```

2. Se non è stata configurata alcuna interfaccia dialer per le interfacce fisiche in questione (ad esempio PRI, BRI, seriale asincrona e sincrona), è possibile definire:
   ```
   interface virtual-template 1
   ip unnumbered e0
   ppp authen chap
   ppp Multilink
   ```

   Nota: non si definisce un indirizzo IP specifico nel modello virtuale. Questo perché le interfacce di accesso virtuale previste vengono sempre clonate dall'interfaccia del modello virtuale. Se anche un successivo collegamento PPP viene proiettato su un membro dello stack con un'interfaccia di accesso virtuale già clonata e attiva, gli indirizzi IP delle due interfacce virtuali sono identici e l'IP instrada erroneamente il traffico tra di esse.

Interfacce Dialer Interessate

Quando i dialer sono configurati sulle interfacce fisiche, non è necessario specificare un'interfaccia modello virtuale, in quanto la configurazione dell'interfaccia risiede nell'interfaccia dialer. In questo

caso, l'interfaccia di accesso virtuale funge da interfaccia passiva ed è collegata tramite un collegamento tra l'interfaccia del dialer e le interfacce membro associate a tale interfaccia.

Nota: l'interfaccia dialer, Dialer 1, viene visualizzata nella sessione di connessione multipla PPP come segue:

```
systema#show ppp Multilink
Bundle userx 2 members, Master link is Virtual-Access4
Dialer interface is Dialer1
0 lost fragments, 0 reordered, 0 unassigned, 100/255 load
0 discarded,  0 lost received, sequence 40/66 rcvd/sent
members 2
Serial0:4
systemb:Virtual-Access6    (1.1.1.1)
```

LCP e NCP

Gli stati LCP su tutte le interfacce membri devono essere attivi. IPCP, ATCP e altri NCP devono essere attivi solo sull'interfaccia del bundle.

L'output del comando **show int dell'**interfaccia del bundle `Virtual-Access4` deve essere il seguente:

```
router#show int  Virtual-Access4
Virtual-Access4 is up, line protocol is up
        :
    LCP Open, Multilink Open
    Open: ipcp
           :
```

Tutte le altre interfacce membro devono avere il seguente output **show int**:

```
router# show int Serial0:4
Serial0:4 is up, line protocol is up
        :
LCP Open, Multilink Open
Closed:  ipcp
```

Debug VPN/L2F

Attiva quanto segue:

```
debug vpn event
debug vpn error
```

Quando l'interfaccia fisica accetta la chiamata in arrivo e viene inoltrata al membro dello stack di destinazione, viene visualizzato quanto segue:

```
Serial0:21 VPN Forwarding
Serial0:21 VPN vpn_forward_user userx is forwarded
```

Sul membro dello stack di destinazione, se viene visualizzato quanto segue:

```
Virtual-Access1 VPN PPP LCP not accepting rcv CONFACK
Virtual-Access1 VPN PPP LCP not accepting sent CONFACK
```

Verificare quindi la definizione dell'interfaccia del modello virtuale. In genere, l'interfaccia del modello virtuale deve corrispondere ai parametri dell'interfaccia PPP dell'interfaccia fisica che ha accettato una chiamata in ingresso.

Tenere presente la configurazione minima (utilizzando CHAP come esempio):

```
#config
multilink virtual template 4
int virtual-template 4
ip unnum e0
encap ppp
ppp authen chap
ppp Multilink
```

Èpossibile visualizzare quanto segue:

```
Virtual-Access1 VPN PPP LCP accepted sent & rcv CONFACK
```

Se viene visualizzato il messaggio precedente, il protocollo L2F ha proiettato correttamente il collegamento PPP dal membro dello stack che per primo ha effettuato la chiamata in arrivo al membro dello stack in cui risiede (o creerà, come nello scenario di offload) l'interfaccia del bundle per lo stesso client.

Errore comune: impossibile definire il nome utente per il nome dello stack comune (stackq) o password non corrispondente su tutti i membri dello stack.

Utilizzare il seguente comando:

```
debug vpdn l2f-error
```

Il messaggio seguente ha restituito:

```
L2F Tunnel authentication failed for stackq
```

In questo caso, correggere il nome utente e la password di ciascun membro dello stack.

Informazioni correlate

- Parte 1 del presente documento
- Funzioni PPP di accesso virtuale nel software Cisco IOS
- Informazioni sulla VPDN
- Supporto tecnico – Cisco Systems