

Multichassis Multichassis Multilink PPP (MMP) (Teil 2)

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Beispiele](#)

[AS5200 in einem Stack \(mit Wählern\)](#)

[Verwenden eines Offload-Servers](#)

[Server mit physischen Schnittstellen auslagern](#)

[Async-, Serial- und andere Nicht-Dialer-Schnittstellen](#)

[Wählen von einem Multichassis aus](#)

[Wählen mit mehreren Chassis](#)

[Konfiguration und Einschränkungen](#)

[Konfiguration von Schnittstellenkonfigurationen pro Protokoll](#)

[Konfiguration globaler Protokollkonfigurationen](#)

[Fehlerbehebung](#)

[Sicherstellen, dass SGBP ordnungsgemäß läuft](#)

[Debuggen von PPP Multilink](#)

[Debuggen von VPN/L2F](#)

[Zugehörige Informationen](#)

[Einführung](#)

In diesem Dokument wird auch weiterhin die Unterstützung von Multilink PPP (MP) in einer Stack- oder Multichassis-Umgebung (manchmal auch als MMP bezeichnet, für *Multichassis Multilink PPP*) auf den Access Server-Plattformen von Cisco Systems beschrieben.

Dieses Dokument ist Teil 2 eines zweiteiligen Dokuments. Weitere Informationen finden Sie [im ersten Teil dieses Dokuments](#).

[Voraussetzungen](#)

Die Voraussetzungen für dieses Dokument sind in [Teil 1 dieses Dokuments](#) festgelegt.

[Beispiele](#)

[AS5200 in einem Stack \(mit Wählern\)](#)

Wenn Dialer auf den physischen Schnittstellen konfiguriert werden, muss die virtuelle

Vorlagenschnittstelle überhaupt nicht angegeben werden. Die virtuelle Zugriffsschnittstelle fungiert als passive Schnittstelle, die zwischen der Dialer-Schnittstelle und den der Dialer-Schnittstelle zugeordneten physischen Schnittstellen unterlegt ist.

Kurz gesagt, Sie müssen nur den Stapelgruppennamen, das allgemeine Kennwort und die Stapelgruppenelemente für alle Stapelelemente definieren. Es ist keine virtuelle Vorlagenschnittstelle definiert, wie im folgenden Beispiel gezeigt:

```
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 .....
  encaps 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
```

Das folgende Beispiel stammt von einem E1-Controller:

```
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
```

Nachdem die Paketschnittstelle erstellt wurde, wird sie mit nur den PPP-Befehlen der Dialer-Schnittstelle geklont. Spätere prognostizierte PPP-Verbindungen werden auch mit den PPP-Befehlen der Dialer-Schnittstelle geklont. Abbildung 3 zeigt, wie sich die Dialer-Schnittstelle auf der Paketschnittstelle befindet. Vergleichen Sie diese Informationen mit [Abbildung 2](#), in der keine Dialer-Schnittstelle vorhanden ist.

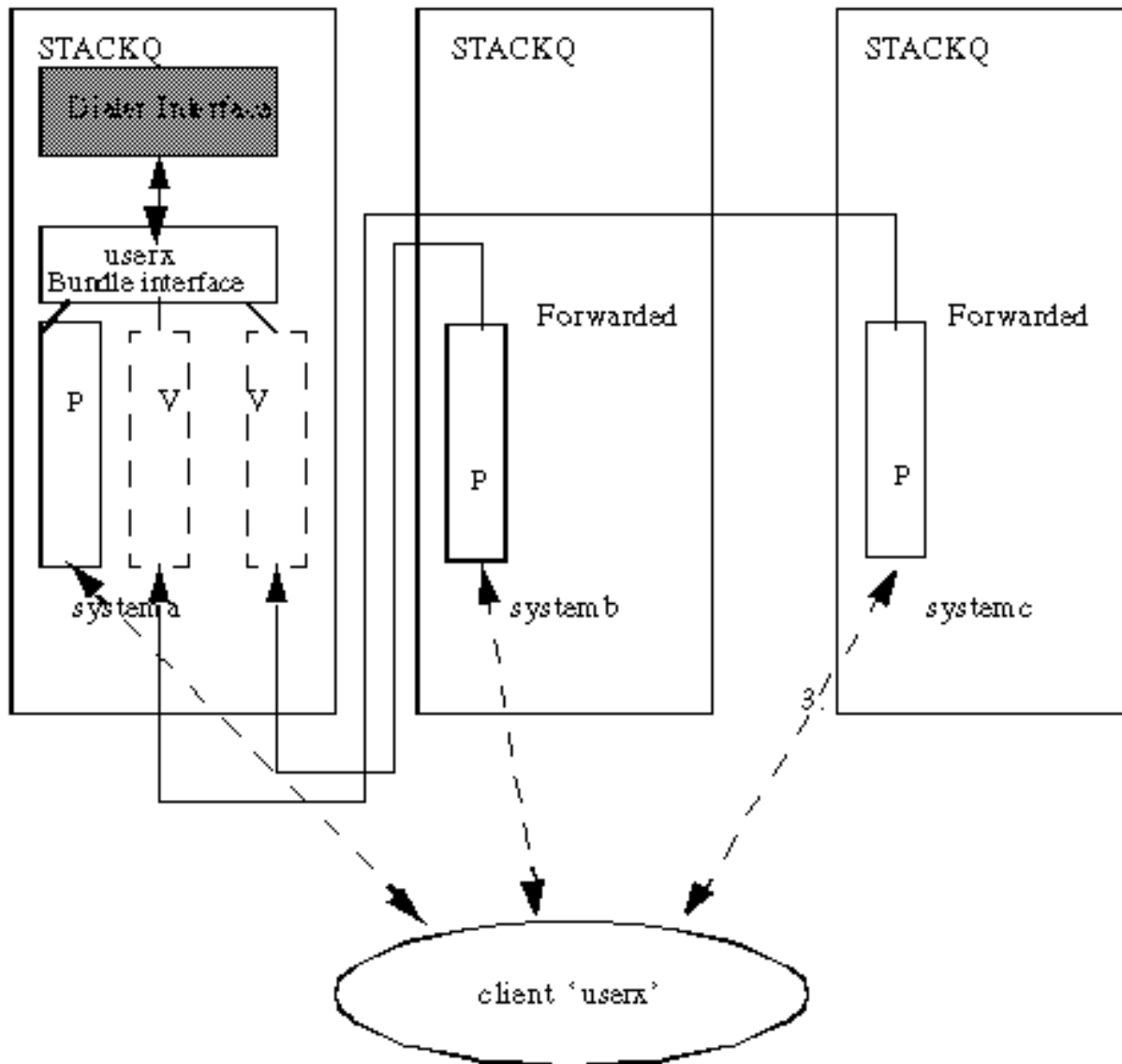
PRIs und BRIs sind standardmäßig Dialer-Schnittstellen. Eine PRI, die ohne expliziten Dialer konfiguriert wurde (über den **Dialer**-Befehl), ist immer noch eine Dialer-Schnittstelle auf Serial0:23, wie im folgenden Beispiel gezeigt:

```

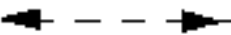

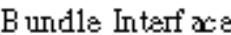


interface Serial0:23
 ip unnum e0
 dialer map .....
 encaps ppp
 ppp authen chap
 dialer-group 1
 dialer rot 1
 ppp multilink

```

Abbildung 3: Eine Stack Group-Stackq, bestehend aus **systema**, **systemb** und **systemc**. **systema**'s link ist auf der dialer interface konfiguriert.



Legend

-  Client PPP MP links across stack members STACKQ
-  L2F projected links to the stack member containing bundle interface 'userx'
-  Bundle Interface for client 'userx' (Virtual Access interface)
-  Physical interface
-  Projected PPP link (Virtual Access Interface)

Verwenden eines Offload-Servers

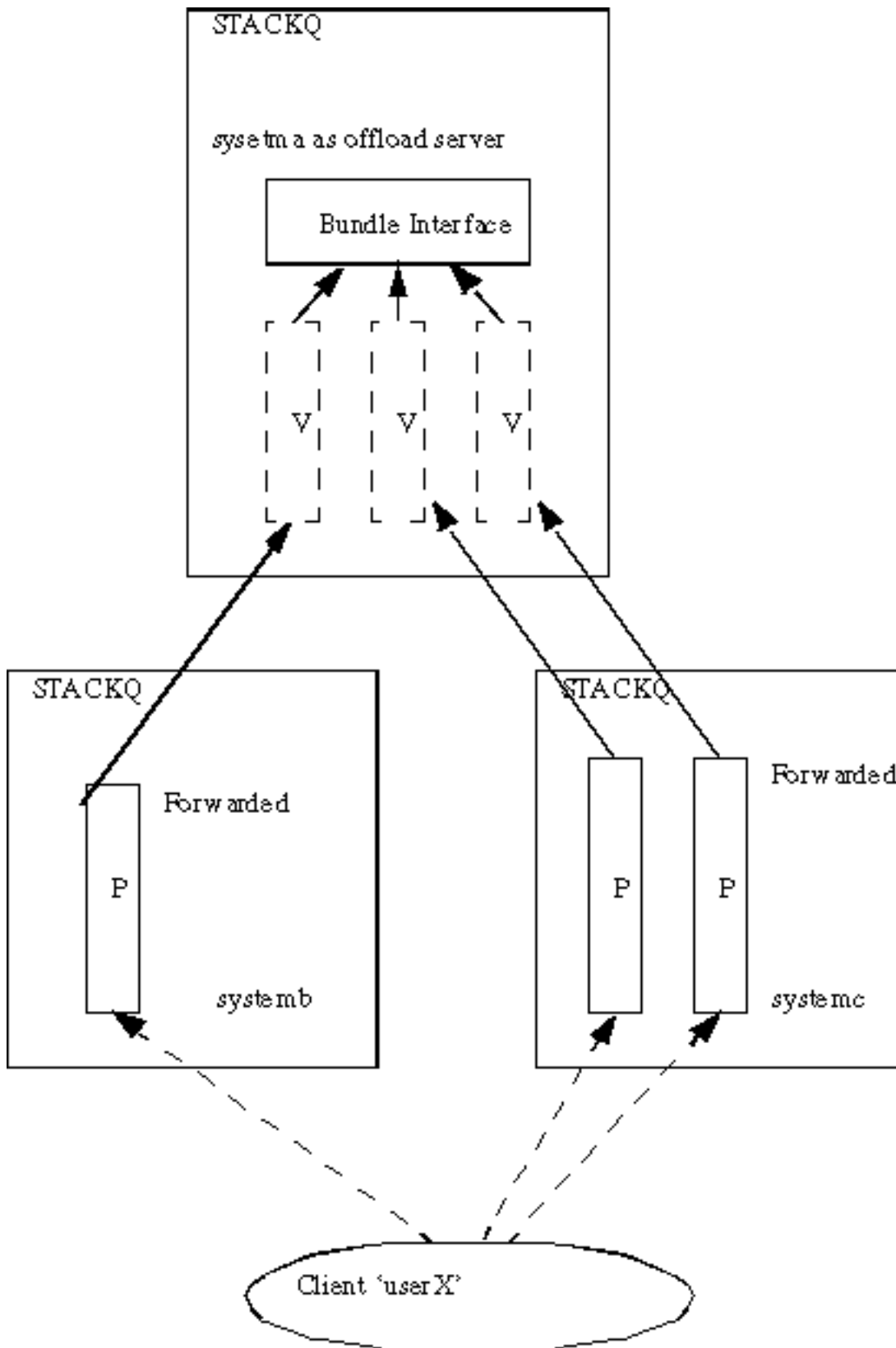
`systema` wird als Offload-Server bezeichnet (mithilfe des Befehls **`sgbp seed-bid`**). Alle anderen Stapelgruppenmitglieder müssen mit dem **Standard-Befehl `sgbp seed-bid`** definiert werden (oder, wenn Sie **den Befehl `sgbp seed-bid`** nicht definieren, wird dies standardmäßig übernommen).

```
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
```

Abbildung 4: `systema` als Offload-Server.



Server mit physischen Schnittstellen auslagern

Wenn der designierte Offload-Server auch physische Schnittstellen (z. B. PRI) hat, die dieselbe Telco-Sammelgruppe wie die anderen Stack-Mitglieder bedienen möchten, können Sie dies konfigurieren, indem Sie Konfigurationen kombinieren, die in den Abschnitten dieses Dokuments mit dem Titel [AS5200 in einem Stack \(mit Dialern\)](#) und [mit einem Offload-Server](#) angezeigt werden.

Eine entladene projizierte PPP-Verbindung und ihre Paketschnittstellen basieren auf virtuellen

Vorlagen für eine Konfigurationsquelle. Eine Verbindung mit der *ersten Verbindung* erreicht ein physisches Gerät, das mit einer Dialer-Schnittstelle verbunden ist. Die Konfigurationsquelle für die Paketschnittstelle und alle nachfolgenden prognostizierten PPP-Verbindungen ist die Konfiguration der Dialer-Schnittstelle. Daher existieren diese Varianten gleichzeitig, abhängig vom Stack-Element, auf dem die erste Verbindung ankommt.

Diese Konfiguration wird aufgrund der Komplexität der Konfigurationen, die für die Dialer- und virtuellen Vorlagenschnittstellen erforderlich sind, nicht empfohlen.

[Async-, Serial- und andere Nicht-Dialer-Schnittstellen](#)

Sie können zwar asynchrone und serielle Geräte als Dialer-Schnittstellen konfigurieren (in diesem Fall wird sie [in einem Stack auf AS5200](#) zurückgesetzt [\(mit Dialern\)](#), wie in diesem Abschnitt dieses Dokuments gezeigt), Sie können jedoch Multichassis-MP ohne Dialer-Konfiguration für asynchrone, serielle und andere Nicht-Dialer-Schnittstellen unterstützen. Die Quelle aller Konfigurationen wird dann in der virtuellen Vorlagenschnittstelle definiert, wie unten gezeigt.

```
#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
  encaps ppp
  ppp multilink
  ppp authen chap
  :

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

[Wählen von einem Multichassis aus](#)

Derzeit **unterstützt** die Multi-Chassis-Konfiguration **kein Dialout**, da das Layer 2 Forwarding (L2F)-Protokoll das Wählen nicht unterstützt.

Daher kann der Offload-Server (bei dem eine Route gepooadet wird, ein Wählprofil usw.) keine Dial-Funktion für das Front-End-Stack-Element in derselben Stack-Gruppe initiieren. Spoofing-Routen müssen auf den Front-End-Stack-Elementen installiert werden, da es sich um solche handelt, die über physische Wählverbindungen verfügen (z. B. PRI).

Einige Workarounds sind wie folgt:

- Wenn der Befehl **sgbp ppp-forward** für das Front-End-Stack-Element ausgegeben wird, bedeutet dies, dass alle PPP- und PPP-Multilink-Anrufe automatisch an den Bieter des Stack

Group Biding Protocol (SGBP) weitergeleitet werden, z. B. an einen Offload-Server. Sie müssen sich darauf verlassen, dass der Network Access Server (NAS) sich abwählt und IP-Routing-Konvergenz (nur für IP) den Kurs übernimmt. Wenn Sie beispielsweise 1.1.1.1 wählen möchten, geben Sie diese Adresse in die Wählplan-Anweisung auf dem NAS-Gerät ein, und legen Sie eine statische Route auf das NAS-Gerät wie folgt fest:

```
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
```

Wenn das Wählen mit dem Remote-Peer verbunden wird, wird die PPP-Verbindung zwischen dem Remote-Peer und dem Offload-Server gebildet. Das Front-End-Stack-Element wird vollständig umgangen. PPP wird auf dem Offload-Server installiert und anschließend eine Host-Route zum Peer 1.1.1.1. An diesem Punkt konvergiert das IP-Routing-Protokoll von der Host-Route am Offload-Server, da die Routing-Metrik die Route dort abstuft. **Hinweis:** Routing-Konvergenz führt zu Latenz.

- Wenn der Befehl **sgbp ppp-forward** nicht für das Front-End-Stack-Element definiert ist, bedeutet dies, dass nur PPP-Multilink-Anrufe automatisch an den SGBP-Bieter weitergeleitet werden, z. B. an einen Offload-Server. Daher erstreckt sich ein Dialer vom Front-End-Stack-Element zum Remote-Peer über die PPP-Verbindung zwischen dem Front-End und dem Remote-Peer - dasselbe Verhalten, als ob das NAS nicht Teil einer Stack-Gruppe wäre. **Hinweis:** Dies geschieht, solange die Verbindung gerade PPP (und nicht PPP Multilink) ist.

Wählen mit mehreren Chassis

Wenn IP-Routing (z. B. Enhanced Interior Gateway Routing Protocol (EIGRP) und Open Shortest Path First (OSPF)) zwischen dem Client und dem Stack-Element fließen, das schließlich den Zuschlag erhält (z. B. der Offload-Server), folgen Sie diesen Tipps:

Verhindern der Installation einer verbundenen Route auf Clientseite

Konfigurieren Sie Client 1.1.1.2, wobei 1.1.1.2 die Adresse des NAS ist (der transparente Frame-Forwarder), wie unten gezeigt.

```
int bri0

dialer map 1.1.1.2 ....
```

Wenn z. B. EIGRP zwischen dem Client und dem Offload-Server ausgeführt wird, gibt die Routing-Tabelle auf dem Offload-Server an, dass die Route zum Erreichen von 1.1.1.2 über die virtuelle Zugriffsschnittstelle verlaufen sollte. Der Grund hierfür ist, dass das PPP IP Control Protocol (IPCP) auf Client-Seite eine verbundene Route 1.1.1.2 zur BRI-Schnittstelle installiert. EIGRP kündigt diese Route dann über die PPP-Sitzung (über L2F) an den Offload-Server an. EIGRP auf dem Offload-Server gibt daher an, dass für den Zugriff auf 1.1.1.2 eine Route zum Client erfolgen sollte - die Route 1.1.1.1 des Clients ist die virtuelle Zugriffsschnittstelle.

Nun ist ein Paket für den Client 1.1.1.1 vorgesehen. IP-Routing sendet das Paket an die virtuelle Zugriffsschnittstelle. Die virtuelle Zugriffsschnittstelle kapselt die IP/User Data Protocol (UDP)/L2F/PPP-Kapselung und sendet das Paket an das L2F NAS - 1.1.1.2. An diesem Punkt ist

alles normal. Anstatt das Paket über die Ethernet-Schnittstelle zu senden (z. B.), sendet das IP-Routing es dann erneut über die virtuelle Zugriffsschnittstelle. Dies liegt daran, dass die Routing-Tabelle angibt, dass zum Erreichen des NAS der Client durchlaufen werden muss. Dadurch wird eine Routingschleife erstellt und die Ein- und Ausgabe über den L2F-Tunnel effektiv deaktiviert.

Um dies zu verhindern, lassen Sie nicht zu, dass IPCP eine verbundene Route auf Client-Seite installiert.

Hinweis: Dies gilt nur, wenn ein IP-Routing-Protokoll zwischen dem Client und dem Cisco Home Gateway ausgeführt wird.

Die Client-Konfiguration ist wie folgt:

```
int bri0

no peer neighbor-route
```

Dialer-Karten auf dem Client

Wenn der Client eine Multi-Chassis-Umgebung wählt, definieren Sie immer die Wähler für jeden potenziellen Gewinner des Multi-Link-Pakets. Wenn es z. B. vier Offload-Server im Multi-Chassis-Stack gibt, sollten auf Client-Seite vier Dialer-Karten definiert sein.

Beispiel:

```
client 1.1.1.1

int bri0

dialer map 1.1.1.3 ...
```

In diesem Beispiel ist 1.1.1.3 nur ein Offload-Server.

Ein Paket, das für 1.1.1.2 bestimmt ist, wird an die BRI weitergeleitet, und der Dialer wählt das Ziel, da eine Dialerzuordnung vorhanden ist. Der Offload-Server 1.1.1.4 gewinnt tatsächlich das Angebot, und die PPP-Sitzung wird dort prognostiziert. EIGRP wird zwischen dem Client und dem Offload-Server ausgetauscht. Die IP-Routing-Tabelle auf dem Client wird mit der Route 1.1.1.4 (Offload-Server) zu BRI0 gefüllt. Auf dem Client wird nun ein für 1.1.1.4 bestimmtes Paket an BRI0 weitergeleitet. Der Wähler kann jedoch nicht wählen, da es keine Dialer-Übereinstimmung gibt.

Hinweis: Definieren Sie immer Dialer Maps für alle potenziellen SGBP-Bieter auf Clients, wenn der Zugriff auf die Offload-Server eine Anforderung der Clients ist.

Konfiguration und Einschränkungen

- Das j-Image der Enterprise-Klasse ist für Multichassis MP erforderlich.
- Für jeden Zugriffsserver kann nur eine Stack-Gruppe definiert werden.
- WAN-Verbindungen mit hoher Latenz zwischen Stack-Elementen, die Verzögerungen bei der MP-Reassemblierung verursachen, können zu ineffizienter Multichassis-MP führen.

- Schnittstellen werden für PRI-, [M]BRI-, serielle und asynchrone Geräte unterstützt.
- Dialout wird nicht unterstützt.

Konfiguration von Schnittstellenkonfigurationen pro Protokoll

Konfigurieren Sie aus praktischen Gründen keine spezifische Protokolladresse auf der virtuellen Vorlage.

```
interface virtual-template 1

ip address 1.1.1.2 255.0.0.0

:
```

Die virtuelle Vorlagenschnittstelle dient als Vorlage, aus der eine beliebige Anzahl virtueller Zugriffsschnittstellen dynamisch geklont wird. Sie sollten für die virtuelle Vorlagenschnittstelle keine protokollspezifische Adresse für jede Schnittstelle angeben. Da eine IP-Adresse für jede Netzwerkschnittstelle eindeutig sein muss, ist die Angabe einer eindeutigen IP-Adresse in der virtuellen Vorlagenschnittstelle falsch. Gehen Sie stattdessen wie folgt vor:

```
interface virtual-template 1

ip unnum e0

:
```

Konfiguration globaler Protokollkonfigurationen

Ein Client, der sich in einem einzelnen Access-Router einwählt und erwartet, dass der Access-Server über eine eindeutige globale Adresse (z. B. DECnet) verfügt, wählt nun tatsächlich die Multi-Chassis-Stack-Gruppe mit mehreren Access-Servern. In einer solchen Situation wird die Stack-Gruppe deterministisch an einem einzelnen Zugriffsserver terminiert. Geben Sie dazu den Befehl **sgbp seed-bid** auf dem designierten Zugriffsserver an (oder geben Sie den höchsten Anbieter an).

Fehlerbehebung

Wenn Probleme auftreten, müssen Sie zunächst zu einem einzelnen Stack-Element zurückkehren und alle anderen Stack-Elemente deaktivieren. Testen Sie anschließend Ihre PPP-Multilink-Verbindungen, und führen Sie die übliche Challenge Handshake Authentication Protocol (CHAP)-Authentifizierung und -Schnittstellenkonfiguration durch, um Konfigurationsfehler usw. zu erkennen. Wenn Sie zufrieden sind, können Sie die anderen Stack-Elemente aktivieren und dann wie folgt vorgehen:

1. Stellen Sie sicher, dass SGBP betriebsbereit ist.
2. Debuggen Sie PPP Multilink.
3. Debuggen von VPN und L2F

Sicherstellen, dass SGBP ordnungsgemäß läuft

Geben Sie den Befehl **show sgbp** ein, um sicherzustellen, dass alle Mitgliedstaaten AKTIV sind.

Achten Sie andernfalls auf IDLE-, AUTHOK- oder ACTIVE-Status. Wie bereits erwähnt, ist IDLE ein gültiger Zustand für alle Remote-Stack-Elemente, die absichtlich inaktiv sind.

Wenn Sie ein Problem wie oben beschrieben finden, aktivieren Sie den Befehl **debug sgbp hellos** und **debug sgbp error**. Die Authentifizierung zwischen zwei Stack-Elementen, z. B. zwischen `systema` und `system b`, sollte wie folgt sein (auf `systema`):

```
systema# debug sgdg 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` sendet eine CHAP-artige Herausforderung und erhält eine Antwort vom `system b`. Ebenso sendet `systemb` eine Herausforderung und erhält eine Antwort von `systema`.

Wenn die Authentifizierung fehlschlägt, sehen Sie:

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

Das bedeutet, dass das Remote-System-Passwort für `stackq` nicht mit dem auf `systema` definierten Passwort übereinstimmt.

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

Dies bedeutet, dass `systema` weder lokal noch über TACACS+ einen Benutzernamen oder ein Kennwort definiert hat.

Definieren Sie im Allgemeinen einen gemeinsamen geheimen Schlüssel für alle Stack-Elemente für die Stack-Gruppe-`Stackq`. Sie können sie lokal oder über TACACS+ definieren.

Ein lokaler Benutzername, der für die einzelnen Stack-Elemente definiert wird, ist:

```
username stackq password blah
```

Dieses gemeinsame Geheimnis ist es, die Geboten und Schiedsgerichtsbarkeit von Stack-Mitgliedern zu erleichtern.

Im Abschnitt [Debuggen von PPP Multilink](#) dieses Dokuments wird die PPP-Link-Authentifizierung erläutert, wenn sich ein Remote-Client bei den Stack-Elementen einwählt.

Bei Kabel- oder Routing-Problemen liegt ein häufiger Fehler darin, dass die Quell-IP-Adresse des Stack-Elements (die tatsächlich in der SGBP Hello-Nachricht empfangen wird) von der lokal definierten IP-Adresse für dasselbe Stack-Element abweicht.

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

Dies bedeutet, dass die Quell-IP-Adresse des SGBP hello, der vom `system b` empfangen wurde, nicht mit der lokal für `systemb` konfigurierten IP-Adresse übereinstimmt (über den Befehl `sgbp member`). Korrigieren Sie dies, indem Sie `systemb` aufrufen und nach mehreren Schnittstellen suchen, über die das SGBP Hello die Nachricht übertragen kann.

Eine weitere häufige Fehlerursache ist:

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

Das bedeutet, dass Sie das `system` nicht lokal definiert haben, sondern ein anderes Stack-Element dies tut.

Debuggen von PPP Multilink

Zunächst muss überprüft werden, ob der Client und das Stack-Element auf PPP korrekt authentifiziert wurden.

In diesem Beispiel wird die CHAP-Authentifizierung veranschaulicht, da sie stärker beteiligt ist. Als vertrautes Beispiel verwendet es eine Cisco Plattform als Client zusammen mit lokalen Benutzernamen (Terminal Access Controller Access Control System Plus (TACACS+) wird ebenfalls unterstützt, wird aber hier nicht gezeigt).

Client-Benutzer	Jedes Element des Stack-Stackq
<pre>#config username stackq password blah</pre>	<pre>#config username userx password blah</pre>

Keine Dialer-Schnittstellen beteiligt

Da auf dem Offload-Server keine Dialer-Schnittstelle vorhanden ist, muss eine weitere *Quelle für die Schnittstellenkonfiguration* virtueller Zugriffsschnittstellen vorhanden sein. Die Antwort sind virtuelle Vorlagenschnittstellen.

1. Stellen Sie zuerst sicher, dass die globale virtuelle Multilink-Vorlagenummer für jedes Stack-Element definiert ist.

```
#config
Multilink virtual-template 1
```

2. Wenn Sie keine Dialer-Schnittstellen für die betreffenden physischen Schnittstellen konfiguriert haben (z. B. PRI, BRI, asynchrone und synchrone serielle Schnittstellen), können Sie Folgendes definieren:

```
interface virtual-template 1
ip unnumbered e0
ppp authen chap
ppp Multilink
```

Hinweis: Sie definieren keine bestimmte IP-Adresse auf der virtuellen Vorlage. Dies liegt daran, dass projizierte virtuelle Zugriffsschnittstellen immer von der virtuellen Vorlagenschnittstelle geklont werden. Wenn eine nachfolgende PPP-Verbindung auch auf

ein Stack-Element projiziert wird, dessen virtuelle Zugriffsschnittstelle bereits geklont und aktiv ist, verfügen Sie über identische IP-Adressen auf den beiden virtuellen Schnittstellen, sodass IP irrtümlich zwischen ihnen weitergeleitet wird.

Einbezogene Dialer-Schnittstellen

Wenn Dialer auf den physischen Schnittstellen konfiguriert werden, muss keine virtuelle Vorlagenschnittstelle angegeben werden, da sich die Schnittstellenkonfiguration in der Dialer-Schnittstelle befindet. In diesem Fall fungiert die virtuelle Zugriffsschnittstelle als passive Schnittstelle, die zwischen der Dialer-Schnittstelle und den mit der Dialer-Schnittstelle verknüpften Mitgliedsschnittstellen unterteilt wird.

Hinweis: Die Dialer-Schnittstelle Dialer 1 wird in der PPP-Multilink-Sitzung wie folgt angezeigt:

```
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 und NCP

Die LCP-Zustände an allen Mitgliedsschnittstellen müssen UP sein. IPCP, ATCP und andere NCP sollten nur auf der Paketschnittstelle aktiv sein.

Paketschnittstelle Virtual-Access4 **zeigt int-Ausgabe an:**

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

Alle anderen Mitgliedschnittstellen sollten die folgende **show int**-Ausgabe aufweisen:

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

Debuggen von VPN/L2F

Schalten Sie Folgendes ein:

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

Wenn die physische Schnittstelle den eingehenden Anruf annimmt und nun an das Ziel-Stack-Element weitergeleitet wird, sehen Sie Folgendes:

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

Wenn Sie auf dem Ziel-Stack-Element Folgendes sehen:

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

Überprüfen Sie dann Ihre Definition der virtuellen Vorlagenschnittstelle. Im Allgemeinen muss die virtuelle Vorlagenschnittstelle den PPP-Schnittstellenparametern der physischen Schnittstelle entsprechen, die einen eingehenden Anruf angenommen hat.

Beachten Sie die Mindestkonfiguration (z. B. mit CHAP):

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

Sie sehen möglicherweise Folgendes:

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

Wenn Sie die obige Meldung sehen, bedeutet dies, dass L2F die PPP-Verbindung erfolgreich vom Stack-Element projiziert hat, das den eingehenden Anruf zuerst an das Stack-Element geleitet hat, in dem sich die Paketschnittstelle für denselben Client befindet (oder wie im Offload-Szenario erstellt wird).

Ein häufiger Fehler besteht darin, dass der Benutzername für den gemeinsamen Stapelnamen (Stackq) nicht definiert wurde oder dass das Stack-Kennwort nicht mit allen Stack-Elementen übereinstimmt.

Geben Sie den folgenden Befehl ein:

```
debug vpdn l2f-error
```

Die folgenden Meldungsergebnisse:

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

Korrigieren Sie in diesem Fall die Übereinstimmung von Benutzername und Kennwort für die einzelnen Stack-Elemente.

[Zugehörige Informationen](#)

- [Teil 1 dieses Dokuments](#)
- [Virtual Access PPP-Funktionen der Cisco IOS-Software](#)
- [VPDN im Überblick](#)
- [Technischer Support - Cisco Systems](#)