

マルチシャーシ マルチリンク PPP (MMP) (パート 2)

内容

[概要](#)

[前提条件](#)

[例](#)

[スタックグループ内のAS5200 \(ダイヤラが設定された場合\)](#)

[オフロードサーバの使用](#)

[物理インターフェイスを使用するオフロードサーバ](#)

[非同期、シリアルおよび他の非ダイヤラインターフェイス](#)

[マルチシャーシからのダイヤルアウト](#)

[マルチシャーシへのダイヤル](#)

[設定および制限](#)

[プロトコルごとのインターフェイス構成の設定](#)

[グローバル・プロトコル構成の設定](#)

[トラブルシューティング](#)

[SGBP が正常に動作していることの確認](#)

[PPPマルチリンクのデバッグ](#)

[VPN/L2Fのデバッグ](#)

[関連情報](#)

概要

このドキュメントでは、シスコのアクセス サーバ プラットフォームにおける「スタック」またはマルチシャーシ環境でのマルチリンク PPP (MP) のサポート (マルチシャーシ マルチリンク PPP という名称で MMP と呼ばれる場合もあり) のサポートについて引き続き説明します。

このドキュメントは、2 部で構成されたドキュメントの第 2 部です。詳細については、[このドキュメントの第 1 部を参照してください。](#)

前提条件

このドキュメントの前提条件は、[このドキュメントの第 1 部](#)に記載されています。

例

[スタックグループ内のAS5200 \(ダイヤラが設定された場合\)](#)

ダイヤラが物理インターフェイスに設定されている場合、仮想テンプレート インターフェイスを

指定する必要はまったくありません。仮想アクセス インターフェイスは、ダイヤラ インターフェイスと、そのダイヤラ インターフェイスに関連付けられている物理インターフェイスとの間を補強するパッシブ インターフェイスとして機能します。

つまり、定義する必要があるのは、スタック グループ名、共通パスワード、およびすべてのスタック メンバーにわたるスタック グループ メンバーだけです。次の例に示すように、仮想テンプレート インターフェイスは定義されません。

```
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
```

次の例は、E1 コントローラからのものです。

```
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
```

バンドル インターフェイスが作成されると、ダイヤラ インターフェイスから PPP コマンドだけを使用してクローンが作成されます。その後の投影される PPP リンクも、ダイヤラ インターフェイスから PPP コマンドを使用してクローンが作成されます。図 3 に、ダイヤラ インターフェイスがバンドル インターフェイスの上にどのように配置されるかを示しています。この図をダイヤラ インターフェイスがない [図 2](#) と比較してください。

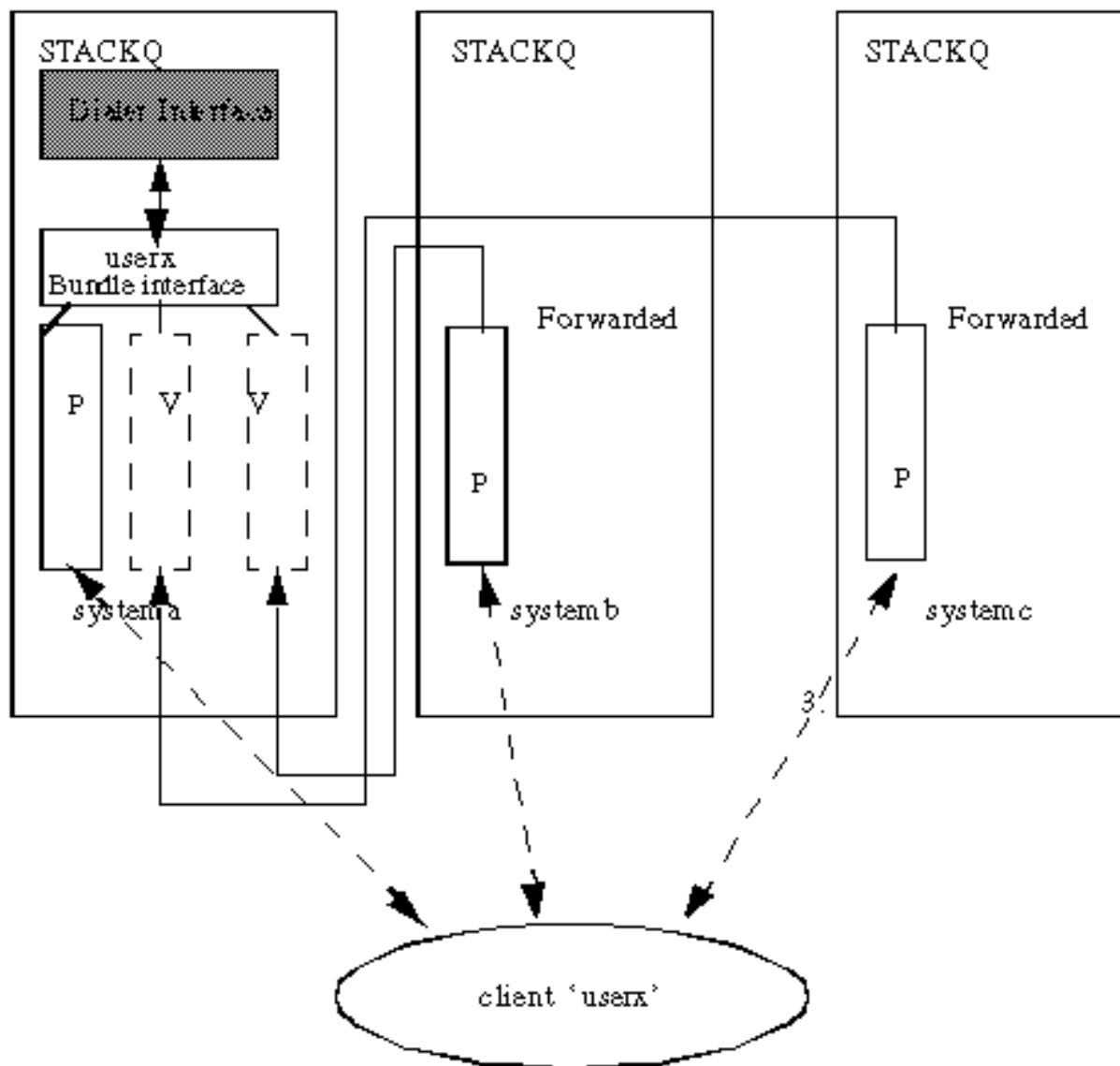
PRI および BRI は、デフォルトではダイヤラ インターフェイスです。(dialer rotary コマンドによる) 明示的なダイヤラなしで設定された PRI でも、次の例に示すように Serial0:23 のダイヤラ インターフェイスです。

```

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

```

図 3 : systema、systemb、およびsystemcで構成されるスタック stackq。systema



Legend

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

オフロードサーバの使用

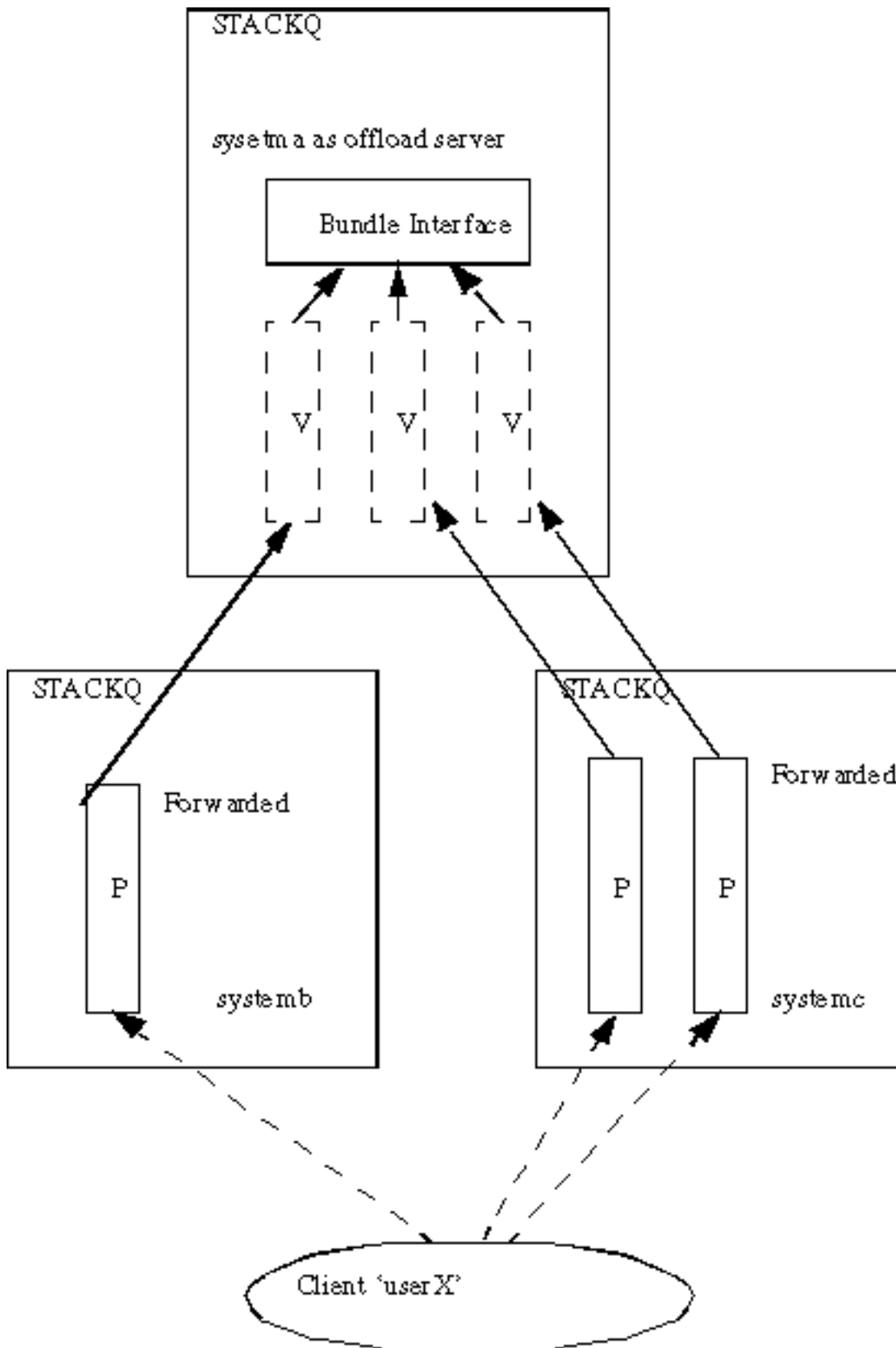
systema sgbp seed-bid コマンドを使用して) オフロード サーバとして指定されます。他のスタックグループメンバーはすべて、sgbp seed-bid default コマンドを使用して定義する必要があります (または、sgbp seed-bid コマンドを定義していない場合、デフォルトで sgbp seed-bid default になります)。

```
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
```

図 4 : systema



物理インターフェイスを使用するオフロードサーバ

指定されたオフロードサーバに、他のスタックメンバーと同じ通信事業者ハントグループに
 応答させたい物理インターフェイス（たとえば、PRI）が組み込まれている場合、そのように応答
 させるには、このドキュメントの「[スタック内の AS5200（ダイヤラを設定）](#)」セクションと「
[オフロードサーバの使用](#)」セクションで示した各設定を組み合わせることで設定できます。

オフロードされ投影される PPP リンクとそのバンドル インターフェイスでは、設定ソースの仮
 想テンプレートを使用します。最初のリンクがある接続は、ダイヤラ インターフェイスに接続さ

れている物理デバイスに達します。また、バンドル インターフェイスとその後の投影される PPP リンクすべての設定のソースは、ダイヤラ インターフェイス設定です。このため、これらのバリエーションは最初のリンクが達するスタック メンバーに基づいて共存します。

この設定は、ダイヤラおよび仮想テンプレート インターフェイスに必要な設定が複雑なため、推奨されません。

非同期、シリアルおよび他の非ダイヤラインターフェイス

非同期デバイスおよびシリアル デバイスをダイヤラ インターフェイスとして設定できます (この場合は、このドキュメントの「[スタック内の AS5200 \(ダイヤラを設定\)](#)」セクションに戻ってください) が、非同期インターフェイス、シリアル インターフェイス、およびその他のダイヤラ以外のインターフェイスのダイヤラ設定なしでマルチシャーシ MP のサポートを選択できます。この場合、すべての設定のソースが次に示すように仮想テンプレート インターフェイスで定義されます。

```
#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
```

マルチシャーシからのダイヤルアウト

現在、マルチシャーシの設定ではダイヤルアウトをサポートしていません。Layer 2 Forwarding (L2F; レイヤ 2 転送) プロトコルがダイヤルアウト (発信) をサポートしていないためです。

その結果、オフロードサーバ (ルートがダイヤラプロファイル上などでスプーフィングされるところ) が同じスタックグループでフロントエンドスタックメンバーにダイヤルを開始することはありません。スプーフィングされたすべてのルートは、フロントエンドのスタック メンバーに設定する必要があります。これは、これらのフロントエンドのスタック メンバーが物理的なダイヤル接続 (PRI など) があるスタック メンバーであるためです。

次に回避策をいくつか示します。

- `sgbp ppp-forward` コマンドがフロントエンドのスタック メンバーに対して発行されると、こ

これはすべての PPP および PPP マルチリンク コールが Stack Group Bidding Protocol (SGBP) ビディングでのコールの所有者 (オフロード サーバなど) に自動的に転送されることを意味します。ネットワーク アクセス サーバ (NAS) のダイヤル アウト (発信) を利用して、IP ルーティング コンバージェンス (IP 専用) の処理に任せる必要があります。たとえば、次のように、1.1.1.1 にダイヤルし、このアドレスを NAS 上の dialer map ステートメントに配置し、スタティック ルートを NAS に配置します。

```
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
```

このダイヤルがリモート ピアに接続すると、PPP 接続がリモート ピアとオフロード サーバ間で形成されます。フロントエンドのスタック メンバーは、完全にバイパスされます。オフロードサーバ上の PPP は、ピアへのホストルート 1.1.1.1 をインストールします。この時点で、IP ルーティング プロトコルはそこからオフロードサーバ上のホストルートに収束します。これは、ルーティング メトリックがルートをそこに集約するためです。注：ルーティング コンバージェンスでは遅延が発生します。

- `sgbp ppp-forward` コマンドがフロントエンドのスタック メンバーに対して定義されない場合、これはその PPP マルチリンク コールが SGBP ビディングでのコールの所有者に自動的に転送されることを意味します。このため、フロントエンドのスタック メンバーからリモートピアへのダイヤラは、フロントエンドとリモートピア間の PPP 接続全体に及びます。これは、NAS があたかもスタック グループの一部ではないかのような動作です。注：これは接続がストレート PPP (PPP マルチリンクではなく) である場合に発生します。

マルチシャシへのダイヤル

クライアントとスタックメンバーの間で IP ルーティング (Enhanced Interior Gateway Routing Protocol (EIGRP) や Open Shortest Path First (OSPF) など) が流れ、最終的に入札に勝った場合 (オフロードサーバなど)、次のヒントを参照してください。

接続済みルートのクライアント側への設定を防ぐ

次に示すように、1.1.1.2 が NAS のアドレスであるクライアントの 1.1.1.2 (透過的なフレーム フォワード) を設定します。

```
int bri0

dialer map 1.1.1.2 ....
```

たとえば、クライアントとオフロードサーバ間で EIGRP を実行させる場合、オフロードサーバ上のルーティング テーブルで、1.1.1.2 に到達するために、ルートが仮想アクセス インターフェイスを経由する必要があることを示します。これは、クライアント側の PPP IP Control Protocol (IPCP) で BRI インターフェイスへの接続済みルート 1.1.1.2 を設定するためです。次に、EIGRP では、PPP セッションを介した (L2F を介した) オフロードサーバへのこのルートをアドバタイズします。このため、オフロードサーバ上の EIGRP では、1.1.1.2 に到達するために、このクライアントにルーティングする必要があることを指示します。クライアントのルート 1.1.1.1 は仮想アクセス インターフェイスへのルートです。

これで、クライアント 1.1.1.1 宛ての packets が作成されました。IP ルーティングは packets を仮想アクセス インターフェイスに送信します。仮想アクセス インターフェイスは、IP/ユーザデータ

プロトコル(UDP)/L2F/PPPカプセル化をカプセル化し、パケットをL2F NAS(1.1.1.2)に送信します。この時点ではすべてが正常です。次に、IP ルーティングでは、パケットを (たとえば) イーサネット インターフェイスを通じて送送するのではなく、仮想アクセス インターフェイスを通じて再度送送します。これは、ルーティング テーブルで、NAS に到達するためにクライアントを通過する必要があることを示しているためです。これにより、ルーティング ループが発生し、L2F トンネルを介した入出力が無効にされます。

これが発生しないようにするために、IPCP で接続済みルートをクライアント側に設定することを許可しないでください。

注：これは、クライアントとCiscoホームゲートウェイの間でIPルーティングプロトコルが実行されている場合にのみ該当します。

クライアント設定は、次のとおりです。

```
int bri0  
  
no peer neighbor-route
```

クライアント側の dialer map

クライアントがマルチシャーシ環境にダイヤルする場合、マルチリンク バンドルのそれぞれの潜在的なビディングでのコールの所有者に対してダイヤラを定義します。たとえば、マルチシャーシ スタックにオフロード サーバが 4 つ存在する場合、クライアント側に 4 つの dialer map を定義する必要があります。

以下に、いくつかの例を示します。

```
client 1.1.1.1  
  
int bri0  
  
dialer map 1.1.1.3 ...
```

この例では、1.1.1.3 がただ 1 つのオフロード サーバです。

1.1.1.2 宛てのパケットは BRI にルーティングされ、ダイヤラは、dialer map の一致があるため、この宛先にダイヤルします。オフロード サーバの 1.1.1.4 は実際にビディングでのコールの所有者となり、そこに PPP セッションが投影されます。EIGRP は、クライアントとオフロード サーバとの間で交換されます。クライアントのIPルーティングテーブルには、BRI0へのルート 1.1.1.4 (オフロードサーバ) が設定されています。クライアントでは、1.1.1.4宛てのパケットが BRI0にルーティングされます。ただし、ダイヤラは一致しないためダイヤルできません。

注：オフロードサーバへのアクセスがクライアントの要件である場合は、常にクライアント上のすべての潜在的なSGBP送信権獲得に対してダイヤラマップを定義してください。

設定および制限

- マルチシャーシ MP には、エンタープライズ j イメージが必要です。
- アクセス サーバごとに定義できるスタック グループは 1 つだけです。

- MP リアセンブル遅延の原因となる、スタック メンバー間の高遅延 WAN リンクによって、マルチシャーシ MP の効率が低下するおそれがあります。
- インターフェイスは、PRI、[M]BRI、シリアル、および非同期の各デバイスでサポートされます。
- ダイアルアウト (発信) はサポートされません。

プロトコルごとのインターフェイス構成の設定

実用上は、仮想テンプレートに特定のプロトコルのアドレスを設定しないでください。

```
interface virtual-template 1
```

```
ip address 1.1.1.2 255.0.0.0
```

```
:
```

仮想テンプレート インターフェイスは、任意の数の仮想アクセス インターフェイスのクローンをダイナミックに作成するための元になるテンプレートとして役立ちます。インターフェイスごとのプロトコル固有のアドレスを仮想テンプレート インターフェイスに指定しないでください。IP アドレスはネットワーク インターフェイスごとに一意でなければならないため、仮想テンプレート インターフェイスに一意の IP アドレスを指定することは誤りです。代わりに、以下のことを行います。

```
interface virtual-template 1
```

```
ip unnum e0
```

```
:
```

グローバル・プロトコル構成の設定

単一のアクセス ルータにダイヤルし、アクセス サーバに一意のグローバル アドレスがある (DECnet など) と想定するクライアントでは、いくつかのアクセス サーバで構成されたマルチシャーシ マルチリンクのスタック グループに実際にダイヤルするようになりました。この種の状況では、単一のアクセス サーバにあるスタック グループの終了を決定してください。この終了を行うには、指定されたアクセス サーバで `sgbp seed-bid offload` コマンドを発行します (または、最も高いビディングを指定します)。

トラブルシューティング

問題がある場合、まず最初に 1 つのスタック メンバーに集中し、他のすべてのスタック メンバーを無効にします。次に PPP マルチリンク接続をテストし、通常の Challenge Handshake Authentication Protocol (CHAP) 認証を実行し、設定の誤りがないかインターフェイス設定をチェックしたりなどします。そのスタック メンバーが機能していることを確認できた場合は、他のスタック メンバーを有効にして、次のようにトラブルシューティングを続けます。

1. SGBP が正常に動作していることを確認します。
2. PPP マルチリンクをデバッグします。
3. VPN および L2F をデバッグします。

SGBP が正常に動作していることの確認

`show sgbp` コマンドを発行して、すべてのメンバーの状態が **ACTIVE** であることを確認します。あるいは、状態が **IDLE**、**AUTHOK**、または **ACTIVE** のものがないか探します。前に述べたように、**IDLE** は、意図的に非アクティブ状態にしているすべてのリモート スタック メンバーにとっては有効な状態です。

上記のような問題が見つかった場合、コマンドの `debug sgbp hellos` と `debug sgbp error` をオンにします。2 つのスタック メンバー (たとえば、`systema systemb`) 間の認証は、(`systema` 上で) 次のようにならなければなりません。

```
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 CHAP systemb` から応答を受信します。同様に、`systemb systema` から応答を受信します。

認証に失敗すると、次のメッセージが表示されます。

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

このメッセージは、リモートの `systemb stackq systema` で定義されているパスワードと一致しないことを示しています。

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

このメッセージは、`systema TACACS+`

通常、スタック グループの `stackq` のすべてのスタック メンバー間で共通のシークレットを定義します。このシークレットは、ローカルで定義でき、また **TACACS+** によっても定義できます。

それぞれのスタック メンバーに定義されるローカル ユーザ名は、次のようになります。

```
username stackq password blah
```

この共通のシークレットは、スタック メンバーの **SGBP** ビディングと調停を容易にするためのものです。

リモート クライアントがスタック メンバーにダイヤルインする際の **PPP** リンクの認証については、このドキュメントの「[PPP マルチリンクのデバッグ](#)」セクションを参照してください。

配線またはルーティングの問題の場合、よくあるエラーの 1 つ (このエラーは実際上 **SGBP hello** メッセージで受信されます) は、スタック メンバーのローカルで定義された IP アドレスとは異なる、同じスタック メンバーの送信元 IP アドレスを使用することです。

```
systema#debug sgbp error
```

```
%SGBP-7-DIFFERENT - systemb's addr 1.1.1.2 is different from hello's addr 3.3.4.5
```

このメッセージは、`systemb SGBP hello IP systemb` に対して (`sGBP member` コマンドを使用して) ローカルで設定された IP アドレスと一致していないことを意味しています。これを修正するには、`systemb SGBP hello`

もう 1 つのよくあるエラーの原因は、次のようなエラーの原因です。

```
%SGBP-7-MISCONF, Possible misconfigured member routerk (1.1.1.6)
このメッセージは、systemk
```

PPPマルチリンクのデバッグ

まず、PPP でクライアントとスタック メンバーが正しく認証されたかどうかを調べます。

次の例では、CHAP 認証について、より複雑なため具体的に説明しています。よくある例として、CHAP 認証でシスコプラットフォームがローカル ユーザ名とともにクライアントとして使用されることがあります (Terminal Access Controller Access Control System Plus (TACACS+) もサポートされていますが、ここでは示していません)。

クライアントの userx	スタック stackq
<pre>#config username stackq password blah</pre>	<pre>#config username userx password blah</pre>

ダイヤラ インターフェイスが含まれていない

オフロード サーバにはダイヤラ インターフェイスがないため、仮想アクセス インターフェイスのインターフェイス設定の別のソースが必要になります。解決策は、仮想テンプレート インターフェイスを使用することです。

1. まず、それぞれのスタック メンバーにマルチリンクのグローバル仮想テンプレート番号を定義します。

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

2. 対象の物理インターフェイス (PRI、BRI、非同期、同期シリアルなど) にダイヤラ インターフェイスを設定していなかった場合、次のように定義できます。

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

注：仮想テンプレートに特定のIPアドレスを定義しないでください。これは、投影される仮想アクセス インターフェイスが、必ず仮想テンプレート インターフェイスからのクローンとして作成されるためです。その後の PPP リンクも、仮想アクセス インターフェイスのクローンを作成済みでアクティブにして、スタック メンバーに投影される場合、2 つの仮想インターフェイスに同じ IP アドレスがあると、それらの間で IP を誤ってルーティングさせる原因となります。

ダイヤラ インターフェイスが含まれている

ダイヤラが物理インターフェイスに設定されている場合、インターフェイス設定がダイヤラ インターフェイスにあるため、仮想テンプレート インターフェイスを指定する必要はありません。この場合、仮想アクセス インターフェイスは、ダイヤラ インターフェイスと、そのダイヤラ インターフェイスに関連付けられているメンバーのインターフェイスとの間を補強するパッシブ インターフェイスとして機能します。

注：ダイヤラーインターフェイスDialer 1は、PPPマルチリンクセッションで次のように表示されます。

```
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 および NCP

すべてのメンバーのインターフェイスの LCP 状態は「up」でなければなりません。IPCP、ATCP、および他の NCP は、バンドル インターフェイスでのみ up でなければなりません。

バンドル インターフェイス Virtual-Access4 の show int の出力は、次のようになります。

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

他のすべてのメンバーのインターフェイスの show int の出力は、次のようになります。

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

VPN/L2Fのデバッグ

次のコマンドをオンにします。

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

物理インターフェイスで着信コールを受け付けて、そのコールをターゲットのスタック メンバーに転送する際に、次のように表示されます。

```
Serial0:21 VPN Forwarding
```

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

ターゲットのスタック メンバーで、次のように表示される場合は、

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

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

仮想テンプレート インターフェイスの定義をチェックしてください。通常、仮想テンプレート インターフェイスは、着信コールを受け付ける物理インターフェイスの PPP インターフェイスのパラメータと一致している必要があります。

次の最小設定を覚えておいてください (例として CHAP を使用)。

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

次のように表示される場合があります。

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

上記のメッセージが表示された場合、最初に着信コールを受けたスタック メンバーから、同じクライアントのバンドル インターフェイスが存在する (またはオフロードのシナリオでのように、バンドル インターフェイスをこれから作成する) スタック メンバーに、L2F で PPP リンクを正常に投影したことを意味しています。

よくあるエラーとしては、共通のスタック名 (stackq) のユーザ名を定義しないことや、すべてのスタック メンバーに対するスタックのパスワードを一致させないことです。

次のコマンドを実行します。

```
debug vpdn l2f-error
```

この結果、次のメッセージが表示されます。

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

この場合、各スタック メンバーでユーザ名とパスワードの一致について修正します。

[関連情報](#)

- [このドキュメントの第 1 部](#)
- [Cisco IOS ソフトウェアの仮想アクセス PPP 機能](#)
- [VPDN について](#)
- [テクニカルサポート - Cisco Systems](#)