

멀티샐시 MMP(Multilink PPP)(2부)

목차

[소개](#)

[사전 요구 사항](#)

[예](#)

[스택의 AS5200\(다이얼러 사용\)](#)

[오프로드 서버 사용](#)

[물리적 인터페이스를 사용하여 서버 오프로드](#)

[비동기, 직렬 및 기타 비 다이얼러 인터페이스](#)

[멀티샐시에서 전화 걸기](#)

[멀티샐시에 전화 걸기](#)

[구성 및 제한 사항](#)

[프로토콜별 인터페이스 컨피그레이션](#)

[전역 프로토콜 컨피그레이션 구성](#)

[문제 해결](#)

[SGBP가 제대로 작동 및 실행 중인지 확인](#)

[PPP 멀티링크 디버깅](#)

[VPN/L2F 디버깅](#)

[관련 정보](#)

소개

이 문서에서는 Cisco Systems의 액세스 서버 플랫폼에서 "스택" 또는 다중 샐시 환경 (MMP(Multichassis Multilink PPP의 경우)에서 MP(Multilink PPP)를 지원하는 방법에 대해 계속 설명합니다.

이 문서는 두 부분으로 구성된 문서의 2부입니다. 자세한 내용은 [이 문서 중 1부](#)를 참조하십시오.

사전 요구 사항

이 문서에 대한 사전 요구 사항은 [이 문서 중 1부에 나와 있습니다](#).

예

스택의 AS5200(다이얼러 사용)

물리적 인터페이스에 다이얼러가 구성된 경우 가상 템플릿 인터페이스를 지정할 필요가 없습니다. 가상 액세스 인터페이스는 다이얼러 인터페이스와 다이얼러 인터페이스와 연결된 물리적 인터페이스 간에 버튼 역할을 합니다.

간단히 말해, 모든 스택 멤버에 대해 스택 그룹 이름, 공통 비밀번호 및 스택 그룹 멤버만 정의해야 합니다. 다음 예와 같이 정의된 가상 템플릿 인터페이스가 없습니다.

```
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
```

다음 예는 E1 컨트롤러의 예입니다.

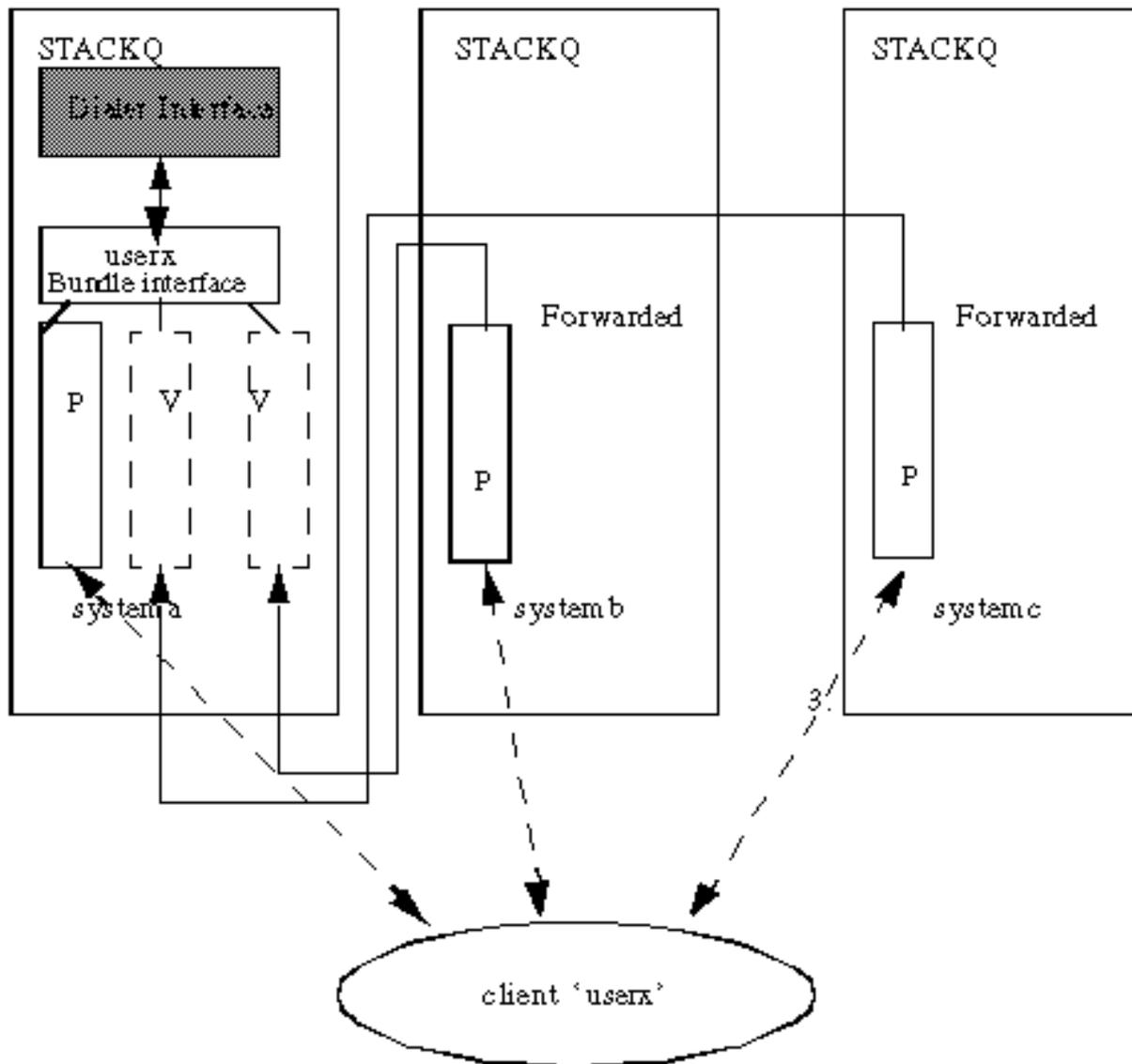
```
controller E1 0
  framing crc4
  linecode hdb3
  pri-group timeslots 1-31
  interface Serial0:15
  no ip address
  encapsulation ppp
  no ip route-cache
  ppp authentication chap
  ppp multilink
```

번들 인터페이스가 생성되면 다이얼러 인터페이스의 PPP 명령만 사용하여 복제됩니다. 후속 예상 PPP 링크는 다이얼러 인터페이스의 PPP 명령으로 복제됩니다. 그림 3은 다이얼러 인터페이스가 번들 인터페이스 위에 어떻게 위치하는지 보여줍니다. 다이얼러 인터페이스가 없는 [그림 2](#)와 비교합니다.

기본적으로 PRI 및 BRI는 다이얼러 인터페이스입니다. 명시적 다이얼러(dialer rotary 명령을 통해) 없이 구성된 PRI는 다음 예와 같이 여전히 Serial0:23의 다이얼러 인터페이스입니다.

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

그림 3: 시스템, 시스템, 시스템으로 스택 그룹 그룹 스택입니다. *systema*의 링크는 다이얼러 인터페이스에 구성됩니다.



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)

오프로드 서버 사용

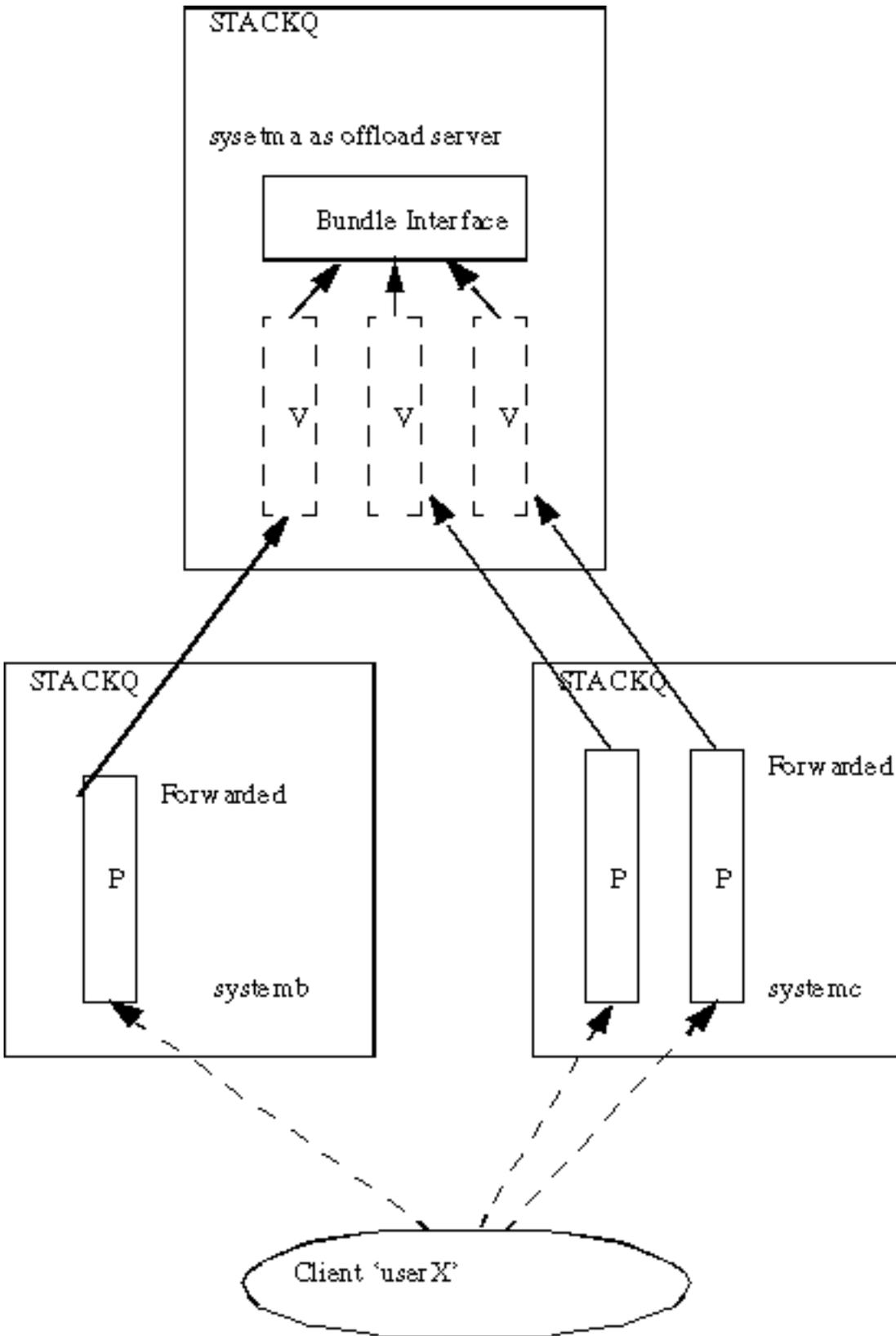
*systema*는 `sgbp seed-bid` 명령을 사용하여 오프로드 서버로 지정됩니다. 다른 모든 스택 그룹 멤버는 `sgbp seed-bid default` 명령을 사용하여 정의해야 합니다(또는 `sgbp seed-bid` 명령을 정의하지 않으면 이 기본값으로 설정됩니다).

```
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
```

그림 4: 을 오프로드 서버로 사용합니다.



물리적 인터페이스를 사용하여 서버 오프로드

또한 지정된 오프로드 서버에 다른 스택 멤버와 동일한 텔코 헛트 그룹(예: PRI)을 제공하려는 물리적 인터페이스(예: PRI)가 있는 경우 이 문서의 섹션에 나와 있는 AS5200(다이얼러 사용) 구성과 오프로드 서버 사용을 결합하여 이러한 작업을 수행하도록 구성할 수 있습니다.

오프로드된 예상 PPP 링크 및 번들 인터페이스는 컨피그레이션 소스에 대한 가상 템플릿을 사용합니다. 첫 번째 링크가 있는 연결이 다이얼러 인터페이스에 연결된 물리적 디바이스에 도착하며, 번들 인터페이스의 컨피그레이션 소스 및 이후의 모든 예상 PPP 링크는 다이얼러 인터페이스 컨피그

레이션입니다. 따라서 이러한 변형은 첫 번째 링크가 도착하는 스택 멤버에 따라 공존합니다.

다이얼러 및 가상 템플릿 인터페이스에 필요한 컨피그레이션의 복잡성 때문에 이 컨피그레이션을 사용하지 않는 것이 좋습니다.

비동기, 직렬 및 기타 비 다이얼러 인터페이스

비동기 및 직렬 장치를 다이얼러 인터페이스로 구성할 수 있지만(이 경우 [스택의 AS5200\(다이얼러 사용\)](#)(이 문서의 해당 섹션에 표시된 대로) 비동기, 직렬 및 기타 다이얼러 인터페이스에 대한 다이얼러 컨피그레이션 없이 멀티샷시 MP를 지원하도록 선택할 수 있습니다. 그러면 아래와 같이 모든 컨피그레이션의 소스가 가상 템플릿 인터페이스에 정의됩니다.

```
#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
```

멀티샷시에서 전화 걸기

현재 멀티샷시 컨피그레이션은 L2F(Layer 2 Forwarding) 프로토콜이 다이얼아웃을 지원하지 않으므로 다이얼아웃을 지원하지 않습니다.

따라서 오프로드 서버(경로가 스푸핑된 위치, 다이얼러 프로파일 등에서)가 동일한 스택 그룹의 프론트 엔드 스택 멤버에 다이얼을 시작할 수 없습니다. 스푸핑된 경로는 물리적 다이얼 연결(예: PRI)이 있는 경로이므로 프론트 엔드 스택 멤버에 설치해야 합니다.

몇 가지 해결 방법은 다음과 같습니다.

- 프론트 엔드 스택 멤버에 **sgbp-ppp-forward** 명령이 실행된 경우, 이는 모든 PPP 및 PPP 멀티 링크 통화가 오프로드 서버 등 SGBP(Stack Group Bauding Protocol) 입찰 승자에게 자동으로 전달됨을 의미합니다. NAS(Network Access Server)에서 전화를 걸어 IP 라우팅 컨버전스(IP에만 해당)를 진행해야 합니다. 예를 들어 1.1.1.1으로 전화를 걸려면 NAS의 다이얼러 맵 문에 이 주소를 넣고 다음과 같이 NAS에 고정 경로를 설정합니다.

```
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
```

다이얼이 원격 피어에 연결되면 원격 피어와 오프로드 서버 간에 PPP 연결이 형성됩니다. 프론트 엔드 스택 멤버가 완전히 우회됩니다. 오프로드 서버의 PPP는 호스트 경로를 피어 (1.1.1.1)에 설치합니다. 이 시점에서 IP 라우팅 프로토콜은 라우팅 메트릭이 거기서 경로를 이동하므로 오프로드 서버의 호스트 경로로 변환됩니다. **참고:** 라우팅 컨버전스는 레이턴시를 초래합니다.

- **sbgp ppp-forward** 명령이 프론트 엔드 스택 멤버에 정의되지 않은 경우 PPP 멀티링크 통화만 오프로드 서버와 같은 SGBP 입찰 승자에게 자동으로 전달됩니다. 따라서 프론트 엔드 스택 멤버에서 원격 피어로의 다이얼러는 프론트엔드와 원격 피어 간의 PPP 연결을 포괄합니다. 이는 NAS가 스택 그룹에 속하지 않은 것과 동일한 동작입니다. **참고:** 연결이 PPP 멀티링크가 아닌 직선 PPP인 경우 이 문제가 발생합니다.

멀티새시에 전화 걸기

IP 라우팅(예: EIGRP(Enhanced Interior Gateway Routing Protocol) 및 OSPF(Open Shortest Path First))이 클라이언트와 BID(예: 오프로드 서버)를 획득한 스택 멤버 간에 흐르는 경우, 다음은 몇 가지 팁입니다.

클라이언트 측에 연결된 경로 설치 방지

클라이언트 1.1.1.2을 구성합니다. 여기서 1.1.1.2은 NAS(투명 프레임 전달자)의 주소입니다(아래 참조).

```
int bri0  
  
dialer map 1.1.1.2 ....
```

예를 들어 EIGRP가 클라이언트와 오프로드 서버 간에 실행되는 경우 오프로드 서버의 라우팅 테이블은 경로가 가상 액세스 인터페이스를 통해 1.1.1.2으로 이동해야 함을 나타냅니다. 클라이언트 측의 PPP IP 제어 프로토콜(IPCP)은 BRI 인터페이스에 연결된 경로 1.1.1.2을 설치하기 때문입니다. 그런 다음 EIGRP는 L2F를 통해 이 경로를 PPP 세션을 통해 오프로드 서버로 광고합니다. 오프로드 서버의 EIGRP는 1.1.1.2에 도달하려면 클라이언트에 라우팅해야 함을 나타냅니다. 클라이언트의 경로 1.1.1.1은 가상 액세스 인터페이스로 전달됩니다.

이제 클라이언트 1.1.1.1으로 향하는 패킷이 있습니다. IP 라우팅은 패킷을 가상 액세스 인터페이스로 전송합니다. 가상 액세스 인터페이스는 UDP(IP/User Data Protocol)/L2F/PPP 캡슐화를 캡슐화하고 L2F NAS(1.1.1.2)으로 패킷을 전송합니다. 이 시점에서는 모든 것이 정상입니다. 그런 다음 이 더넷 인터페이스를 통해 패킷을 전송하는 대신 IP 라우팅은 가상 액세스 인터페이스를 통해 패킷을 다시 전송합니다. 이는 라우팅 테이블이 NAS에 액세스하려면 클라이언트를 통과해야 함을 나타내기 때문입니다. 이렇게 하면 라우팅 루프가 생성되고 L2F 터널을 통한 입력과 출력이 효과적으로 비활성화됩니다.

이를 방지하려면 IPCP가 클라이언트 측에 연결된 경로를 설치하도록 허용하지 마십시오.

참고: 클라이언트와 Cisco 홈 게이트웨이 간에 일부 IP 라우팅 프로토콜이 실행되는 경우에만 해당됩니다.

클라이언트 컨피그레이션은 다음과 같습니다.

```
int bri0

no peer neighbor-route
```

클라이언트의 다이얼러 맵

클라이언트가 멀티샷시 환경으로 다이얼하는 경우 항상 멀티링크 번들의 잠재적 승자에게 다이얼러를 정의합니다. 예를 들어 멀티샷시 스택에 4개의 오프로드 서버가 있는 경우 클라이언트 측에 4개의 다이얼러 맵이 정의되어 있어야 합니다.

예를 들면 다음과 같습니다.

```
client 1.1.1.1

int bri0

dialer map 1.1.1.3 ...
```

이 예에서 1.1.1.3은 하나의 오프로드 서버일 뿐입니다.

BRI로 1.1.1.2 경로를 향하는 패킷과 다이얼러가 다이얼러 맵과 일치하기 때문에 대상에 다이얼러가 다이얼링합니다. 오프로드 서버 1.1.1.4이 실제로 입찰을 획득하고 PPP 세션이 여기에 투영됩니다. EIGRP는 클라이언트와 오프로드 서버 간에 교환됩니다. 클라이언트의 IP 라우팅 테이블이 BRI0에 대한 경로 1.1.1.4(오프로드 서버)으로 채워져 있습니다. 이제 클라이언트에서 1.1.1.4으로 향하는 패킷이 BRI0으로 라우팅됩니다. 그러나 다이얼러가 일치하지 않으므로 다이얼러가 전화를 걸 수 없습니다.

참고: 클라이언트의 요구 사항이 오프로드 서버에 액세스할 때마다 항상 클라이언트의 모든 잠재적 SGBP 입찰 승자에 대한 다이얼러 맵을 정의합니다.

구성 및 제한 사항

- 멀티샷시 MP에는 엔터프라이즈 j 이미지가 필요합니다.
- 각 액세스 서버에 대해 하나의 스택 그룹만 정의할 수 있습니다.
- 스택 멤버 간의 대기 시간이 긴 WAN 링크를 통해 MP 리어셈블리 지연이 발생하여 멀티샷시 MP가 비효율적일 수 있습니다.
- 인터페이스는 PRI, [M]BRI, 직렬 및 비동기 디바이스에 대해 지원됩니다.
- 전화 걸기가 지원되지 않습니다.

프로토콜별 인터페이스 컨피그레이션

모든 실용적인 목적으로 가상 템플릿에 특정 프로토콜 주소를 구성하지 마십시오.

```
interface virtual-template 1

ip address 1.1.1.2 255.0.0.0
```

:

가상 템플릿 인터페이스는 여러 가상 액세스 인터페이스가 동적으로 복제되는 템플릿 역할을 합니

다. 가상 템플릿 인터페이스에 인터페이스별 프로토콜 특정 주소를 지정하면 안 됩니다. IP 주소는 각 네트워크 인터페이스에 대해 고유해야 하므로 가상 템플릿 인터페이스에서 고유한 IP 주소를 지정하는 것은 잘못된 작업입니다. 대신 다음을 수행합니다.

```
interface virtual-template 1
```

```
ip unnum e0
```

```
:
```

전역 프로토콜 컨피그레이션 구성

단일 액세스 라우터로 전화를 걸며 액세스 서버에 고유한 전역 주소(예: DECnet)가 있을 것으로 예상하는 클라이언트가 이제 여러 액세스 서버로 구성된 멀티캐시 멀티링크 스택 그룹에 실제로 전화를 겁니다. 이러한 상황에서는 단일 액세스 서버에서 스택 그룹을 결정적으로 종료합니다. 이렇게 하려면 지정된 액세스 서버에서 **sgbp seed-bid offload** 명령을 실행하거나 가장 높은 입찰을 지정합니다.

문제 해결

문제가 발생할 경우 가장 먼저 해야 할 일은 단일 스택 멤버로 돌아가 다른 모든 스택 멤버를 비활성화하는 것입니다. 그런 다음 PPP 멀티링크 연결을 테스트하고 일반적인 CHAP(Challenge Handshake Authentication Protocol) 인증 및 인터페이스 컨피그레이션에서 컨피그레이션 오류 등을 확인합니다. 정상적으로 작동하는 경우 다른 스택 멤버를 활성화한 다음 다음과 같이 진행합니다.

1. SGBP가 실행 중인지 확인합니다.
2. PPP 멀티링크를 디버깅합니다.
3. 디버그 VPN 및 L2F

SGBP가 제대로 작동 및 실행 중인지 확인

show sgbp 명령을 실행하여 모든 멤버 상태가 ACTIVE인지 확인합니다. 그렇지 않으면 IDLE, AUTHOK 또는 ACTIVE 상태를 확인합니다. 앞에서 언급한 것처럼 IDLE는 의도적으로 비활성화된 모든 원격 스택 멤버에 대해 유효한 상태입니다.

위에서 설명한 대로 문제가 발견되면 debug sgbp hello 및 debug sgbp error 명령을 설정합니다. 두 스택 멤버 간 인증(예: systema와 systemb 간)은 다음과 같습니다.

```
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
```

systema는 CHAP 스타일 챌린지를 전송하고 systemb에서 응답을 . 마찬가지로, systemb는 과제를 전송하고 시스템으로부터 응답을 .

인증이 실패하면 다음을 볼 수 있습니다.

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

즉, stackq에 대한 원격 암호가 에 정의된 암호와 일치하지 않습니다.

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

즉, 에 로컬 또는 TACACS+를 통해 정의된 사용자 이름 또는 비밀번호가 없습니다.

일반적으로 스택 그룹 stackq의 모든 스택 멤버에 대해 공통 암호를 . 로컬 또는 TACACS+를 통해 정의할 수 있습니다.

각 스택 멤버에 정의된 로컬 사용자 이름은 다음과 같습니다.

```
username stackq password blah
```

이 일반적인 비결은 스택 멤버 SGBP 입찰 및 중재 작업을 용이하게 하는 것입니다.

원격 클라이언트가 스택 [멤버에](#) 전화를 걸 때 PPP 링크 인증에 대한 설명은 이 문서의 Debugging PPP Multilink 섹션을 참조하십시오.

배선 또는 라우팅 문제의 경우 한 가지 일반적인 오류는 스택 멤버의 소스 IP 주소(SGBP hello 메시지에서 실제로 수신됨)가 동일한 스택 멤버에 대해 로컬로 정의된 IP 주소와 다르다는 것입니다.

```
systema#debug sgbp error
```

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

즉, systemb에서 받은 SGBP hello의 소스 IP 주소가 systemb에 대해 로컬로 구성된 IP 주소와 일치하지 않습니다(sgbp member 명령을 통해). systemb로 이동하여 SGBP hello가 메시지를 전송할 수 있는 여러 인터페이스를 확인하여 이를 수정합니다.

오류의 또 다른 일반적인 원인은 다음과 같습니다.

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

즉, 시스템이 로컬에 정의되어 않지만 다른 스택 멤버는 정의되어 있습니다.

PPP 멀티링크 디버깅

첫 번째 확인 사항은 클라이언트와 스택 멤버가 PPP에서 올바르게 인증되었는지 여부입니다.

이 예에서는 CHAP 인증을 보여 줍니다. 익숙한 예로, 로컬 사용자 이름과 함께 Cisco 플랫폼을 클라이언트로 사용합니다(TACACS+(Terminal Access Controller Access Control System Plus)도 지원되지만 여기에 표시되지 않음).

클라이언트 사용자	스택 스택의 모든 멤버
#config username stackq password blah	#config username userx password blah

다이얼러 인터페이스 없음

오프로드 서버에 다이얼러 인터페이스가 없으므로 가상 액세스 인터페이스의 또 다른 *인터페이스 컨피그레이션* 소스가 있어야 합니다. 그 답은 가상 템플릿 인터페이스입니다.

1. 먼저 멀티링크 전역 가상 템플릿 번호가 각 스택 멤버에 정의되어 있는지 확인합니다.

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

2. 문제의 물리적 인터페이스(예: PRI, BRI, 비동기 및 동기 시리얼)에 대해 다이얼러 인터페이스를 구성하지 않은 경우 다음을 정의할 수 있습니다.

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

참고: 가상 템플릿에 특정 IP 주소를 정의하지 않습니다. 이는 예상 가상 액세스 인터페이스가 항상 가상 템플릿 인터페이스에서 복제되기 때문입니다. 또한 후속 PPP 링크가 이미 복제되고 활성화된 가상 액세스 인터페이스가 있는 스택 멤버에 예상될 경우 두 가상 인터페이스에 동일한 IP 주소가 있으므로 IP가 둘 간에 잘못 라우팅됩니다.

다이얼러 인터페이스 포함

다이얼러가 물리적 인터페이스에 구성된 경우 인터페이스 컨피그레이션이 다이얼러 인터페이스에 있으므로 가상 템플릿 인터페이스를 지정할 필요가 없습니다. 이 경우 가상 액세스 인터페이스는 패시브 인터페이스 역할을 하며 다이얼러 인터페이스와 연결된 멤버 인터페이스 간에 버팀링됩니다.

참고: 다이얼러 인터페이스인 다이얼러 1은 다음과 같이 PPP 멀티링크 세션에 표시됩니다.

```
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 및 NCP

모든 멤버 인터페이스의 LCP 상태는 UP이어야 합니다. IPCP, ATCP 및 기타 NCP는 번들 인터페이스에서만 작동되어야 합니다.

번들 인터페이스 Virtual-Access4 **show int** 출력은 다음과 같이 읽어야 합니다.

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

다른 모든 멤버 인터페이스에는 다음과 같은 **show int** 출력이 있어야 합니다.

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

VPN/L2F 디버깅

다음은 켜십시오.

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

물리적 인터페이스에서 수신 통화를 수락하고 이제 대상 스택 멤버에 전달되는 경우 다음을 확인할 수 있습니다.

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

대상 스택 멤버에서 다음을 볼 수 있습니다.

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

그런 다음 가상 템플릿 인터페이스의 정의를 확인합니다. 일반적으로 가상 템플릿 인터페이스는 수신 통화를 수락한 물리적 인터페이스의 PPP 인터페이스 매개변수와 일치해야 합니다.

CHAP를 예로 사용하여 최소 구성을 기억하십시오.

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

다음 항목이 표시될 수 있습니다.

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

위 메시지가 표시되면 L2F가 먼저 수신 통화를 수행한 스택 멤버에서 동일한 클라이언트에 대한 번들 인터페이스가 있는 스택 멤버로(또는 오프로드 시나리오와 같이 생성)로의 PPP 링크를 성공적으로 예측했음을 의미합니다.

일반적인 오류는 공통 스택 이름(stackq)에 대한 사용자 이름을 정의하지 못하거나 모든 스택 멤버에 대한 스택 비밀번호와 일치하지 않는 것입니다.

다음 명령을 실행합니다.

```
debug vpdn l2f-error
```

다음 메시지 결과:

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

이 경우 각 스택 멤버에 대해 사용자 이름과 비밀번호 일치를 수정합니다.

관련 정보

- [이 문서의 1부](#)
- [Cisco IOS 소프트웨어의 가상 액세스 PPP 기능](#)
- [VPDN 이해](#)
- [Technical Support - Cisco Systems](#)