

DLSw+ SAP/MAC 필터링 기술

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[DLSw+ SAP 필터링 기술에 대한 구성](#)

[네트워크 다이어그램](#)

[원격 사무실에서 LSAP 출력 액세스 목록 구성](#)

[중앙 라우터에서 dlsw icantralach sap 구성](#)

[중앙 라우터에서 dlsw icanreach saps 구성](#)

[DLSw+ MAC 필터링 기법](#)

[중앙 라우터에서 dlsw icanreach mac-address 구성](#)

[중앙 라우터에서 dlsw icanreach mac-exclusive 구성](#)

[원격 라우터에서 dlsw mac-address 구성](#)

[중앙 라우터에서 dlsw icanreach mac-exclusive remote 구성](#)

[관련 정보](#)

소개

이 문서에서는 DLSw+(Service Access Point) 및 MAC 필터링 기술에 대한 샘플 컨피그레이션을 제공합니다.

필터링을 사용하여 DLSw+ 네트워크의 확장성을 높일 수 있습니다. 예를 들어, 필터링을 사용하여 다음을 수행할 수 있습니다.

- WAN 링크를 통한 트래픽 감소(특히 NetBIOS를 사용하는 환경에서 매우 빠른 링크 및 중요).
- 특정 디바이스에 대한 액세스를 제어하여 네트워크 보안을 강화합니다.
- 데이터 센터 DLSw+ 라우터의 CPU 성능 및 확장성을 향상시킵니다.

DLSw+는 필터링을 수행하는 데 사용할 수 있는 몇 가지 옵션을 제공합니다. MAC 주소, SAP 또는 NetBIOS 이름에서 필터링할 수 있습니다.

[사전 요구 사항](#)

[요구 사항](#)

이 문서에 대한 특정 요건이 없습니다.

[사용되는 구성 요소](#)

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팀 표기 규칙](#)을 참조하십시오.

DLSw+ SAP 필터링 기술에 대한 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 [명령 조회 도구](#)(등록된 고객만 해당)를 사용합니다.

[Network Diagram](#) 섹션에 설명된 네트워크 토폴로지를 사용하여 원격 위치의 모든 NetBIOS 트래픽이 중앙 라우터(상파울루)에 도달하지 못하도록 차단해야 합니다. DLSw+는 이 작업을 수행하기 위한 몇 가지 옵션을 제공하며, 이 옵션은 다음 섹션에서 분석됩니다.

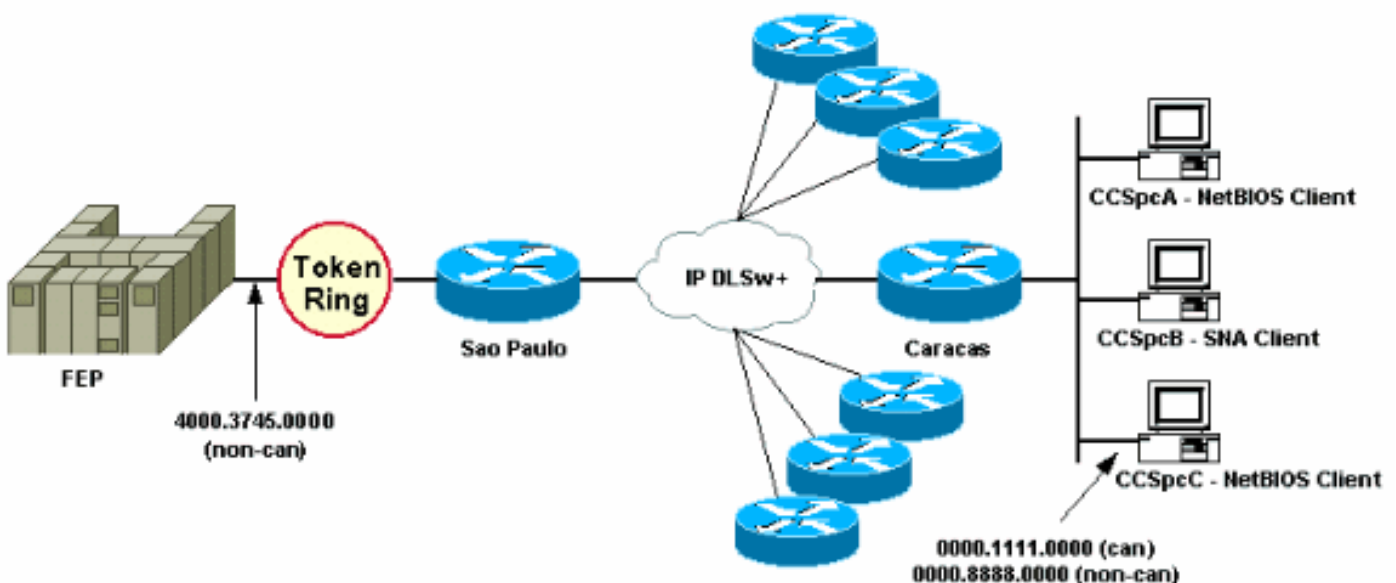
참고: NetBIOS 트래픽은 SAP 값 0xF0(명령의 경우) 및 0xF1(응답의 경우)을 사용합니다. 일반적으로 네트워크 관리자는 위에서 언급한 SAP 값을 사용하여 이 프로토콜을 필터링(수락 또는 거부)합니다.

참고: NetBIOS 클라이언트는 NetBIOS 이름 쿼리 패킷에서 NetBIOS 기능 MAC 주소(C000.0000.0080)를 대상 MAC(DMAC)으로 사용합니다. 앞에서 언급한 대로 모든 프레임에는 0xF0 또는 0xF1의 SAP 값이 있습니다.

이 테스트의 경우 CCSpcC PC는 SAP 0xF0을 사용하여 FEX의 MAC 주소에 연결하도록 구성됩니다. 실제로 이 트래픽은 NetBIOS와 동일하며, 적어도 SAP의 관점에서 볼 수 있습니다. 따라서 이 트래픽이 도착하면 DLSw+ 라우터에서 해당 디버그를 관찰할 수 있습니다.

네트워크 다이어그램

이 섹션에서는 이 다이어그램에 표시된 네트워크 설정을 사용합니다.



네트워크 다이어그램에서 데이터 센터 라우터(상파울루)는 메인프레임과 연결되어 있습니다. 이 라

우터는 모든 원격 지사에서 여러 DLSw+ 피어 연결을 수신합니다. 각 원격 브랜치에는 SNA(Systems Network Architecture) 및 NetBIOS 클라이언트가 모두 있습니다. 데이터 센터에는 원격 사무실에서 액세스해야 하는 NetBIOS 서버가 없습니다.

간소화를 위해 원격 사무실(카라카스)의 컨피그레이션 세부사항만 표시됩니다. 네트워크 다이어그램에는 FIP(Front-End Processor)의 MAC 주소 값과 CCSpcC라는 원격 PC도 나와 있습니다. MAC 주소는 표준(이더넷) 및 비표준(토큰 링) 형식으로 표시됩니다.

원격 사무실에서 LSAP 출력 액세스 목록 구성

이 방법을 사용하면 모든 원격 사무실을 `lsap-output-list` 옵션으로 구성해야 합니다. 중앙 라우터에서는 다른 컨피그레이션 변경이 필요하지 않습니다.

`lsap-output-list`는 현재 SNA SAP(예: 0x00, 0x04, 0x08 등)만 중앙 라우터로 이동할 수 있는 SAP ACL(SAP ACL)에 대한 링크를 제공하며 그 밖의 모든 것을 거부합니다. SAP를 기반으로 필터링을 수행하는 방법에 대한 자세한 내용은 [서비스 액세스 포인트 액세스 제어 목록 이해](#)를 참조하십시오.

카라카스	상파울루
<pre> Current configuration: ! hostname CARACAS ! dlsw local-peer peer-id 1.1.1.2 dlsw remote-peer 0 tcp 1.1.1.1 lsap-output-list 200 dlsw bridge-group 1 ! interface Ethernet0/0 no ip directed-broadcast bridge-group 1 ! interface Serial0/1 ip address 1.1.1.2 255.255.255.0 no ip directed-broadcast ! access-list 200 permit 0x0000 0x0D0D access-list 200 deny 0x0000 0xFFFF ! bridge 1 protocol ieee ! end </pre>	<pre> Current configuration: ! hostname SAOPAULO ! source-bridge ring-group 3 dlsw local-peer peer-id 1.1.1.1 dlsw remote-peer 0 tcp 1.1.1.2 ! interface TokenRing0/0 no ip directed-broadcast ring-speed 16 source-bridge 10 1 3 source-bridge spanning ! interface Serial1/0 ip address 1.1.1.1 255.255.255.0 no ip directed-broadcast no ip mroute-cache clockrate 32000 ! end </pre>

`debug dlsw` 명령은 Caracas 라우터가 NetBIOS 트래픽을 수신할 때 어떻게 반응하는지 확인하는데 사용됩니다.

CARACAS#`debug dlsw`

```

DLSw reachability debugging is on at event level for all protocol traffic
DLSw peer debugging is on
DLSw local circuit debugging is on

```

DLSw core message debugging is on
 DLSw core state debugging is on
 DLSw core flow control debugging is on
 DLSw core xid debugging is on

원격 사무실 라우터(카라카스)에 4000.3745.0000에 대한 연결 가능 정보가 없고 "금지된" SAP 중 일부를 사용하여 해당 MAC 주소를 찾는 탐색기를 가져오면 요청이 차단됩니다.

CARACAS#

```
*Mar 1 01:02:16.387: DLSW Received-ctlQ : CLSI Msg : TEST_STN.Ind dlen: 40
*Mar 1 01:02:16.387: CSM: Received CLSI Msg : TEST_STN.Ind dlen: 40 from DLSw Port0
*Mar 1 01:02:16.387: CSM: smac 0000.8888.0000, dmac 4000.3745.0000, ssap F0, dsap 0
*Mar 1 01:02:16.387: DLSw: dsap(0) ssap(F0) filtered to peer 1.1.1.1(2065)
*Mar 1 01:02:16.387: DLSw: frame output access list filtered to peer 1.1.1.1(2065)
*Mar 1 01:02:16.387: CSM: Write to peer 1.1.1.1(2065) not ok - PEER_FILTERED
```

원격 사무실 라우터(카라카스)에 4000.3745.0000에 대한 연결 가능 정보가 있는 경우를 가정해 보십시오. 예를 들어, 다른 스테이션(허용된 SAP 사용)에서 이미 FIP MAC 주소를 요청했습니다. 이 경우 "범죄자" PC(CCSpcC)는 NULL XID를 전송하지만 라우터는 이를 중지합니다.

CARACAS#

```
*Mar 1 01:03:24.439: DLSW Received-ctlQ : CLSI Msg : ID_STN.Ind dlen: 46
*Mar 1 01:03:24.439: CSM: Received CLSI Msg : ID_STN.Ind dlen: 46 from DLSw Port0
*Mar 1 01:03:24.443: CSM: smac 0000.8888.0000, dmac 4000.3745.0000, ssap F0, dsap F0
*Mar 1 01:03:24.443: DLSw: new_ckt_from_clsi(): DLSw Port0 0000.8888.0000:F0-
>4000.3745.0000:F0
*Mar 1 01:03:24.443: DLSw: START-TPFSM (peer 1.1.1.1(2065)): event:CORE-ADD CIRCUIT
state:CONNECT
*Mar 1 01:03:24.443: DLSw: dtp_action_u(), peer add circuit for peer 1.1.1.1(2065)
*Mar 1 01:03:24.443: DLSw: END-TPFSM (peer 1.1.1.1(2065)): state:CONNECT->CONNECT
*Mar 1 01:03:24.443: DLSw: START-FSM (872415295): event:DLC-Id state:DISCONNECTED
*Mar 1 01:03:24.443: DLSw: core: dlsw_action_a()
*Mar 1 01:03:24.447: DISP Sent : CLSI Msg : REQ_OPNSTN.Req dlen: 116
*Mar 1 01:03:24.447: DLSw: END-FSM (872415295): state:DISCONNECTED->LOCAL_RESOLVE
*Mar 1 01:03:24.447: DLSW Received-ctlQ : CLSI Msg : REQ_OPNSTN.Cfm CLS_OK dlen: 116
*Mar 1 01:03:24.447: DLSw: START-FSM (872415295): event:DLC-ReqOpnStn.Cnf state:LOCAL_RESOLVE
*Mar 1 01:03:24.447: DLSw: core: dlsw_action_b()
*Mar 1 01:03:24.447: CORE: Setting lf : bits 8 : size 1500
*Mar 1 01:03:24.451: DLSw: dsap(F0) ssap(F0) filtered to peer 1.1.1.1(2065)
*Mar 1 01:03:24.451: DLSw: frame output access list filtered to peer 1.1.1.1(2065)
*Mar 1 01:03:24.451: DLSw: peer 1.1.1.1(2065) unreachable - reason code 1
*Mar 1 01:03:24.451: DLSw: END-FSM (872415295): state:LOCAL_RESOLVE->CKT_START
```

중앙 라우터에서 dlsw icantralach sap 구성

dlsw icannottreach saps 명령을 사용하면 전송할 수 없는 것으로 알고 있는 프로토콜을 필터링할 수 있습니다. 명시적으로 거부해야 하는 것만 알고 있는 경우 이러한 컨피그레이션에 표시된 대로 중앙 라우터에서 dlsw icantralach saps 명령을 사용합니다.

카라카스	상파울루
<pre>Current configuration: ! hostname CARACAS ! dlsw local-peer peer-id 1.1.1.2 dlsw remote-peer 0 tcp</pre>	<pre>Current configuration: ! hostname SAOPAULO ! source-bridge ring-group 3 dlsw local-peer peer-id 1.1.1.1 dlsw remote-peer 0 tcp 1.1.1.2</pre>

<pre> 1.1.1.1 dlsw bridge-group 1 ! interface Ethernet0/0 no ip directed- broadcast bridge-group 1 ! interface Serial0/1 ip address 1.1.1.2 255.255.255.0 no ip directed- broadcast ! bridge 1 protocol ieee ! end </pre>	<pre> dlsw icannotreach sap F0 ! interface TokenRing0/0 no ip directed-broadcast ring-speed 16 source-bridge 10 1 3 source-bridge spanning ! interface Serial1/0 ip address 1.1.1.1 255.255.255.0 no ip directed-broadcast no ip mroute-cache clockrate 32000 ! end </pre>
---	---

원격 피어가 이미 작동 중인 경우에도 중앙 라우터(**dlsw icantralach saps** 명령 포함)를 즉시 구성할 수 있습니다. 이 출력은 CapExId 메시지의 수신을 나타내는 원격 라우터 중 하나의 디버그를 표시합니다. 이 메시지는 원격 사무실에 SAP 0xF0/F1을 사용하는 프레임을 중앙 라우터로 전송하지 않도록 지시합니다.

CARACAS#**debug dlsw peers**

DLSw peer debugging is on

```

*Mar  1 18:30:30.388: DLSw: START-TPFSM (peer 1.1.1.1(2065)): event:SSP-CAP MSG RCVD
state:CONNECT
*Mar  1 18:30:30.388: DLSw: dtp_action_p() runtime cap rcvd for peer 1.1.1.1(2065)
*Mar  1 18:30:30.392: DLSw: Recv CapExId Msg from peer 1.1.1.1(2065)
*Mar  1 18:30:30.392: DLSw: received fhpr capex from peer 1.1.1.1(2065): support: false, fst-
prio: false
*Mar  1 18:30:30.392: DLSw: Pos CapExResp sent to peer 1.1.1.1(2065)
*Mar  1 18:30:30.392: DLSw: END-TPFSM (peer 1.1.1.1(2065)): state:CONNECT->CONNECT

```

CapExId 메시지가 수신되면 Caracas 라우터는 상파올로가 SAP 0xF0을 지원하지 않음을 알게 됩니다.

CARACAS#**show dlsw capabilities**

```

DLSw: Capabilities for peer 1.1.1.1(2065)
 vendor id (OUI)           : '00C' (cisco)
 version number            : 2
 release number            : 0
 init pacing window        : 20
 unsupported saps : F0
 num of tcp sessions       : 1
 loop prevent support      : no
 icanreach mac-exclusive  : no
 icanreach netbios-excl.  : no
 reachable mac addresses   : none
 reachable netbios names  : none
 V2 multicast capable     : yes
 DLSw multicast address   : none
 cisco version number     : 1
 peer group number        : 0
 peer cluster support     : no
 border peer capable      : no
 peer cost                 : 3
 biu-segment configured   : no
 UDP Unicast support      : yes

```

```
Fast-switched HPR supp    : no
NetBIOS Namecache length : 15
local-ack configured     : yes
priority configured      : no
cisco RSVP support       : no
configured ip address    : 1.1.1.1
peer type                : conf
version string           :
```

Cisco Internetwork Operating System Software

IOS (tm) C2600 Software (C2600-JK203S-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)

Copyright (c) 1986-1999 by cisco Systems, Inc.

중앙 라우터에서 가져온 **show** 명령 출력은 SAP 0xF0이 지원되지 않는 컨피그레이션 변경을 보여줍니다.

```
SAOPAULO#show dlsw capabilities local
```

DLSw: Capabilities for local peer 1.1.1.1

```
vendor id (OUI)          : '00C' (cisco)
version number           : 2
release number           : 0
init pacing window      : 20
unsupported saps : F0
num of tcp sessions     : 1
loop prevent support     : no
icanreach mac-exclusive : no
icanreach netbios-excl. : no
reachable mac addresses : none
reachable netbios names : none
V2 multicast capable    : yes
DLSw multicast address  : none
cisco version number    : 1
peer group number       : 0
peer cluster support    : yes
border peer capable     : no
peer cost                : 3
biu-segment configured  : no
UDP Unicast support     : yes
Fast-switched HPR supp. : no
NetBIOS Namecache length : 15
cisco RSVP support      : no
current border peer     : none
version string          :
```

Cisco Internetwork Operating System Software

IOS (tm) C2600 Software (C2600-JK203S-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)

Copyright (c) 1986-1999 by cisco Systems, Inc.

NetBIOS PC 스테이션에서 연결을 시도할 때 Caracas 라우터의 디버그 출력입니다.

```
CARACAS#debug dlsw peers
```

DLSw peer debugging is on

```
*Mar  1 18:40:27.575: DLSw: new_ckt_from_clsi(): DLSw Port0 0000.8888.0000:F0-
>4000.3745.0000:F0
*Mar  1 18:40:27.575: DLSw: START-TPFSM (peer 1.1.1.1(2065)): event:CORE-ADD CIRCUIT
state:CONNECT
*Mar  1 18:40:27.579: DLSw: dtp_action_u(), peer add circuit for peer 1.1.1.1(2065)
*Mar  1 18:40:27.579: DLSw: END-TPFSM (peer 1.1.1.1(2065)): state:CONNECT->CONNECT
*Mar  1 18:40:27.579: DLSw: START-FSM (1409286242): event:DLC-Id state:DISCONNECTED
*Mar  1 18:40:27.579: DLSw: core: dlsw_action_a()
*Mar  1 18:40:27.579: DISP Sent : CLSI Msg : REQ_OPNSTN.Req  dlen: 116
*Mar  1 18:40:27.579: DLSw: END-FSM (1409286242): state:DISCONNECTED->LOCAL_RESOLVE
*Mar  1 18:40:27.583: DLSw Received-ctlQ : CLSI Msg : REQ_OPNSTN.Cfm CLS_OK dlen: 116
```

```
*Mar 1 18:40:27.583: DLSw: START-FSM (1409286242): event:DLC-ReqOpnStn.Cnf state:LOCAL_RESOLVE
*Mar 1 18:40:27.583: DLSw: core: dlsw_action_b()
*Mar 1 18:40:27.583: CORE: Setting lf : bits 8 : size 1500
*Mar 1 18:40:27.583: peer_cap_filter(): Filtered by SAP to peer 1.1.1.1(2065), s: F0 d:F0
*Mar 1 18:40:27.583: DLSw: frame cap filtered (1) to peer 1.1.1.1(2065)
*Mar 1 18:40:27.583: DLSw: peer 1.1.1.1(2065) unreachable - reason code 1
```

중앙 라우터에서 dlsw icanreach saps 구성

dlsw icanreach saps 명령은 허용되는 트래픽 유형을 정확히 파악하고 다른 모든 트래픽이 거부되도록 하려는 경우 유용합니다. 예를 들어 dlsw icanreach saps 4를 구성할 때 0x04(및 0x05, 응답)를 제외한 모든 AP를 명시적으로 거부합니다.

카라카스	상파울루
<pre>Current configuration: ! hostname CARACAS ! dlsw local-peer peer-id 1.1.1.2 dlsw remote-peer 0 tcp 1.1.1.1 dlsw bridge-group 1 ! interface Ethernet0/0 no ip directed- broadcast bridge-group 1 ! interface Serial0/1 ip address 1.1.1.2 255.255.255.0 no ip directed- broadcast ! bridge 1 protocol ieee ! end</pre>	<pre>Current configuration: ! hostname SAOPAULO ! source-bridge ring-group 3 dlsw local-peer peer-id 1.1.1.1 dlsw remote-peer 0 tcp 1.1.1.2 dlsw icanreach sap 0 4 ! interface TokenRing0/0 no ip directed-broadcast ring-speed 16 source-bridge 10 1 3 source-bridge spanning ! interface Serial1/0 ip address 1.1.1.1 255.255.255.0 no ip directed-broadcast no ip mroute-cache clockrate 32000 ! end</pre>

이 show 명령 출력에서 Caracas 라우터는 Sao Paulo가 0x04 및 0x05로 향하는 프레임만 지원한다는 사실을 인식합니다. 다른 모든 AP는 지원되지 않습니다.

CARACAS#show dlsw capabilities

```
DLSw: Capabilities for peer 1.1.1.1(2065)
 vendor id (OUI)      : '00C' (cisco)
 version number      : 2
 release number      : 0
 init pacing window  : 20
 unsupported saps   : 0 2 6 8 A C E 10 12 14 16 18 1A 1C 1E 20 22 24 26 28
2A 2C 2E 30 32 34 36 38 3A 3C 3E 40 42 44 46 48 4A 4C 4E 50 52 54 56 58 5A 5C 5E
60 62 64 66 68 6A 6C 6E 70 72 74 76 78 7A 7C 7E 80 82 84 86 88 8A 8C 8E 90 92 94
96 98 9A 9C 9E A0 A2 A4 A6 A8 AA AC AE B0 B2 B4 B6 B8 BA BC BE C0 C2 C4 C6 C8 CA
CC CE D0 D2 D4 D6 D8 DA DC DE E0 E2 E4 E6 E8 EA EC EE F0 F2 F4 F6 F8 FA FC FE
 num of tcp sessions : 1
 loop prevent support : no
 icanreach mac-exclusive : no
 icanreach netbios-excl. : no
```

```

reachable mac addresses : none
reachable netbios names : none
V2 multicast capable : yes
DLSw multicast address : none
cisco version number : 1
peer group number : 0
peer cluster support : no
border peer capable : no
peer cost : 3
biu-segment configured : no
UDP Unicast support : yes
Fast-switched HPR supp. : no
NetBIOS Namecache length : 15
local-ack configured : yes
priority configured : no
cisco RSVP support : no
configured ip address : 1.1.1.1
peer type : conf
version string :

```

Cisco Internetwork Operating System Software

IOS (tm) C2600 Software (C2600-JK2O3S-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)

Copyright (c) 1986-1999 by cisco Systems, Inc.

show dlsw capabilities local 명령을 사용하여 중앙 라우터의 컨피그레이션 변경 사항이 DLSw+ 코드에 나타나는지 확인할 수 있습니다.

SAOPAULO#**show dlsw capabilities local**

DLSw: Capabilities for local peer 1.1.1.1

```

vendor id (OUI) : '00C' (cisco)
version number : 2
release number : 0
init pacing window : 20

```

unsupported saps : 0 2 6 8 A C E 10 12 14 16 18 1A 1C 1E 20 22 24 26 28

```

2A 2C 2E 30 32 34 36 38 3A 3C 3E 40 42 44 46 48 4A 4C 4E 50 52 54 56 58 5A 5C 5E
60 62 64 66 68 6A 6C 6E 70 72 74 76 78 7A 7C 7E 80 82 84 86 88 8A 8C 8E 90 92 94
96 98 9A 9C 9E A0 A2 A4 A6 A8 AA AC AE B0 B2 B4 B6 B8 BA BC BE C0 C2 C4 C6 C8 CA
CC CE D0 D2 D4 D6 D8 DA DC DE E0 E2 E4 E6 E8 EA EC EE F0 F2 F4 F6 F8 FA FC FE

```

```

num of tcp sessions : 1
loop prevent support : no
icanreach mac-exclusive : no
icanreach netbios-excl. : no
reachable mac addresses : none
reachable netbios names : none
V2 multicast capable : yes
DLSw multicast address : none
cisco version number : 1
peer group number : 0
peer cluster support : yes
border peer capable : no
peer cost : 3
biu-segment configured : no
UDP Unicast support : yes
Fast-switched HPR supp. : no
NetBIOS Namecache length : 15
cisco RSVP support : no
current border peer : none
version string :

```

Cisco Internetwork Operating System Software

IOS (tm) C2600 Software (C2600-JK2O3S-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)

Copyright (c) 1986-1999 by cisco Systems, Inc.

DLSw+ MAC 필터링 기법

이 문서에 표시된 [네트워크 다이어그램](#)을 사용하여 중앙 라우터가 FIP MAC 주소 (4000.3745.0000)으로 향하는 프레임만 수신하도록 합니다.

중앙 라우터에서 dlsw icanreach mac-address 구성

dlsw icanreach mac-address 명령을 사용하면 모든 원격 사무소는 중앙 라우터 IP 주소를 가리키는 호스트 MAC 주소에 대한 DLSw+ 연결 가능 테이블에 항목이 있습니다. 이 항목은 UNCONFIRM 상태에 있으며, 이는 원격 사무실 라우터가 호스트에 대한 로컬 테스트 또는 XID를 수신할 경우 중앙 라우터에만 CUR_ex(Can U Reach Explorer) 메시지를 전송함을 나타냅니다.

카라카스	상파울루
<pre> Current configuration: ! hostname CARACAS ! dlsw local-peer peer-id 1.1.1.2 dlsw remote-peer 0 tcp 1.1.1.1 dlsw bridge-group 1 ! interface Ethernet0/0 no ip directed-broadcast bridge-group 1 ! interface Serial0/1 ip address 1.1.1.2 255.255.255.0 no ip directed-broadcast ! bridge 1 protocol ieee ! end </pre>	<pre> Current configuration: ! hostname SAOPAULO ! source-bridge ring-group 3 dlsw local-peer peer-id 1.1.1.1 dlsw remote-peer 0 tcp 1.1.1.2 dlsw icanreach mac-address 4000.3745.0000 mask ffff.ffff.ffff ! interface TokenRing0/0 no ip directed-broadcast ring-speed 16 source-bridge 10 1 3 source-bridge spanning ! interface Serial1/0 ip address 1.1.1.1 255.255.255.0 no ip directed-broadcast no ip mroute-cache clockrate 32000 ! end </pre>

여기서 Caracas 라우터는 연결 캐시에 영구 항목을 생성했습니다. 항목이 비어 있지 않으면 상태가 UNCONFIRM입니다. DLSw+ 라우터가 MAC 주소 및 NetBIOS 이름을 캐시하는 방법에 대한 자세한 내용은 DLSw+ 문제 해결 [설명서](#) 연결 가능성 장을 참조하십시오.

```

CARACAS#show dlsw reachability
DLSw Local MAC address reachability cache list
Mac Addr      status      Loc.      port      rif
0000.8888.0000 FOUND      LOCAL    TBridge-001  --no rif--

DLSw Remote MAC address reachability cache list
Mac Addr      status      Loc.      peer
4000.3745.0000 UNCONFIRM REMOTE 1.1.1.1(2065)

DLSw Local NetBIOS Name reachability cache list
NetBIOS Name  status      Loc.      port      rif

DLSw Remote NetBIOS Name reachability cache list
NetBIOS Name  status      Loc.      peer
          
```

Caracas 라우터에서 **show dlsw capabilities** 명령을 출력하면 이 원격 사무소가 피어 1.1.1.1을 통해

MAC 주소 4000.3745.0000에 연결할 수 있음을 확인합니다. "icanreach mac-exclusive:아니요." 이는 중앙 라우터가 호스트 이외의 다른 MAC 주소에 연결할 수 있음을 나타냅니다. 따라서 원격 사무실 중 하나라도 다른 MAC 주소를 찾는 경우 중앙 라우터로 요청을 보낼 수 있습니다. 그러나 icanreach mac-address 4000.3745.0000 명령을 포함하면 모든 원격 지사에서 이 중요한 리소스의 위치를 인식합니다. 중앙 라우터에 도착하는 프레임에 대해 추가 제한을 두려면 [중앙 라우터](#)에서 dls w icanreach mac-exclusive 구성 을 참조하십시오.

CARACAS#show dls w capabilities

```
DLsw: Capabilities for peer 1.1.1.1(2065)
 vendor id (OUI)           : '00C' (cisco)
 version number            : 2
 release number            : 0
 init pacing window        : 20
 unsupported saps           : none
 num of tcp sessions       : 1
 loop prevent support      : no
 icanreach mac-exclusive  : no
 icanreach netbios-excl.  : no
 reachable mac addresses   : 4000.3745.0000
```

```
reachable netbios names   : none
V2 multicast capable      : yes
DLsw multicast address    : none
cisco version number      : 1
peer group number         : 0
peer cluster support      : no
border peer capable       : no
peer cost                  : 3
biu-segment configured    : no
UDP Unicast support       : yes
Fast-switched HPR supp.   : no
NetBIOS Namecache length : 15
local-ack configured      : yes
priority configured       : no
cisco RSVP support        : no
configured ip address     : 1.1.1.1
peer type                  : conf
version string             :
```

Cisco Internetwork Operating System Software

IOS (tm) C2600 Software (C2600-JK203S-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)

Copyright (c) 1986-1999 by cisco Systems, Inc.

mask 매개 변수를 dls w icanreach mac-address 4000.3745.0000 mask ffff.ffff.ffff로 사용할 수 있습니다. 이 매개 변수를 사용하면 일반적으로 MAC 주소가 16진수 형식(0x4000.3745.0000)으로 표시됩니다. 따라서 all-ones 마스크(이진)는 16진수 0xFFFF.FFFF.FFFF로 표시됩니다.

다음은 이미 구성된 dls w icanreach mac-address 명령에 특정 입력 MAC이 포함되어 있는지 여부를 확인하는 방법의 예입니다.

1. dls w icanreach mac-address 4000.3745.0000 mask ffff.ffff 0000 명령으로 구성된 라우터로 시작합니다.
2. 이전 라우터 컨피그레이션 명령에서 입력 MAC 주소 4000.3745.0009을 포함할지 여부를 평가합니다.
3. 먼저 MAC 주소(4000.3745.0009) 및 구성된 마스크(FFFF.FFFF.0000)를 16진수로 변환합니다. 이 테이블의 처음 두 행은 이 단계를 보여줍니다.

4. 그런 다음 두 이진 숫자 간에 논리 AND 작업을 수행하고 결과를 16진수 표시 (4000.3745.0000)으로 변환합니다. 이 작업의 결과는 이 테이블의 세 번째 행에 표시됩니다.
5. AND 작업의 결과가 `dlsw icanreach mac-address` 명령(예: 4000.3745.0000)의 MAC 주소와 일치하면 `dlsw icanreach mac-address` 명령에서 입력 MAC 주소(4000.3745.0009)을 사용할 수 있습니다. 이 예에서는 4000.3745.0000~4000.3745.FFFF 범위의 입력 MAC 주소가 `dlsw icanreach mac-address` 명령에 포함됩니다. 이 범위의 모든 MAC 주소에 대해 동일한 단계를 반복하여 이를 확인할 수 있습니다.

다음은 몇 가지 예입니다.

- `dlsw icanreach mac-address 4000.3745.0000 mask ffff.ffff.ffff`—이 명령은 MAC 주소 4000.3745.0000만 포함합니다. 이 마스크를 전달하는 다른 MAC 주소는 없습니다.
- `dlsw icanreach mac-address 4000.0000.3745 mask ffff.0000.ffff`—이 명령은 4000.XXXX.3745 범위의 모든 MAC 주소를 포함합니다. 여기서 XXXX는 0x000-0xFFFF입니다.

중앙 라우터에서 `dlsw icanreach mac-exclusive` 구성

중앙 라우터에 `dlsw icanreach mac-exclusive` 명령이 구성된 경우, 중앙 위치에서 이전에 정의한 MAC 주소로 향하는 패킷만 허용되도록 합니다(이 경우 4000.3745.0000).

이 필터링 정보는 CapExId 메시지를 사용하여 모든 DLSw+ 피어 간에 교환됩니다. 원격 라우터 자체에서 작업(예: 차단 프레임)이 발생하는 경우에도 중앙 위치에서 필터링 정보를 구성하여 WAN 대역폭을 저장합니다.

카라카스	상파울루
<pre> Current configuration: ! hostname CARACAS ! dlsw local-peer peer- id 1.1.1.2 dlsw remote-peer 0 tcp 1.1.1.1 dlsw bridge-group 1 ! interface Ethernet0/0 no ip directed- broadcast bridge-group 1 ! interface Serial0/1 ip address 1.1.1.2 255.255.255.0 no ip directed- broadcast ! bridge 1 protocol ieee ! end </pre>	<pre> Current configuration: ! hostname SAOPAULO ! source-bridge ring-group 3 dlsw local-peer peer-id 1.1.1.1 dlsw remote-peer 0 tcp 1.1.1.2 dlsw icanreach mac-exclusive dlsw icanreach mac-address 4000.3745.0000 mask ffff.ffff.ffff ! interface TokenRing0/0 no ip directed-broadcast ring-speed 16 source-bridge 10 1 3 source-bridge spanning ! interface Serial1/0 ip address 1.1.1.1 255.255.255.0 no ip directed-broadcast no ip mroute-cache clockrate 32000 ! end </pre>

이 출력에서 Caracas 라우터가 피어 1.1.1.1을 통해 MAC 주소 4000.3745.0000에 도달할 수 있음을 알고 있음을 확인합니다. 이 예와 이전 시나리오의 차이점은 여기서 "icanreach mac-exclusive:"에 "입니다. 즉, 원격 지사에서 4000.3745.0000으로 향하는 프레임이 아닌 중앙 라우터로 프레임을 전

송하지 않습니다.

CARACAS#show dlsw capabilities

```
DLSw: Capabilities for peer 1.1.1.1(2065)
 vendor id (OUI)           : '00C' (cisco)
 version number            : 2
 release number           : 0
 init pacing window       : 20
 unsupported saps         : none
 num of tcp sessions      : 1
 loop prevent support     : no
 icanreach mac-exclusive : yes
 icanreach netbios-excl. : no
 reachable mac addresses : 4000.3745.0000
```

```
reachable netbios names  : none
V2 multicast capable     : yes
DLSw multicast address   : none
cisco version number     : 1
peer group number       : 0
peer cluster support     : no
border peer capable     : no
peer cost                : 3
biu-segment configured  : no
UDP Unicast support      : yes
Fast-switched HPR supp. : no
NetBIOS Namecache length : 15
local-ack configured     : yes
priority configured      : no
cisco RSVP support      : no
configured ip address    : 1.1.1.1
peer type                : conf
version string           :
```

Cisco Internetwork Operating System Software

IOS (tm) C2600 Software (C2600-JK203S-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)

Copyright (c) 1986-1999 by cisco Systems, Inc.

디버그 출력에서는 Caracas 라우터가 4000.3745.0000 이외의 MAC 주소로 향하는 수신 트래픽에 어떻게 반응하는지 보여줍니다(4000.3745.0080은 여기에서 사용). 카라카스는 호스트에게 전달되지 않는 프레임에 상파올로를 사용하지 않습니다(4000.3745.0000). 이 경우 상파올로는 카라카스에 구성된 유일한 원격 피어이므로 이 라우터에는 전송할 다른 피어가 없습니다.

CARACAS#debug dlsw

```
DLSw reachability debugging is on at event level for all protocol traffic
DLSw peer debugging is on
DLSw local circuit debugging is on
DLSw core message debugging is on
DLSw core state debugging is on
DLSw core flow control debugging is on
DLSw core xid debugging is on
```

```
*Mar 1 22:41:33.200: DLSW Received-ctlQ : CLSI Msg : TEST_STN.Ind  dlen: 40
*Mar 1 22:41:33.204: CSM: Received CLSI Msg : TEST_STN.Ind  dlen: 40 from DLSw Port0
*Mar 1 22:41:33.204: CSM: smac 0000.8888.0000, dmac 4000.3745.0080, ssap 4 , dsap 0
*Mar 1 22:41:33.204: broadcast filter failed mac check
*Mar 1 22:41:33.204: CSM: Write to all peers not ok - PEER_NO_CONNECTIONS
```

dlsw icanreach mac-address 명령을 사용하여 MAC 주소를 정의하지 않고 dlsw icanreach **mac-exclusive** 명령으로 라우터를 구성할 경우, 라우터는 MAC 주소가 전혀 연결되지 않도록 피어에게 알립니다.따라서 해당 피어를 통해 통신이 끊깁니다.

참고: 샘플 컨피그레이션은 예시로만 표시됩니다.그것은 실수이므로 사용해서는 안 된다.

상파울루

```
Current configuration:
!
hostname SAOPAULO
!
source-bridge ring-group 3
dlsw local-peer peer-id 1.1.1.1
dlsw remote-peer 0 tcp 1.1.1.2
dlsw icanreach mac-exclusive
!
interface TokenRing0/0
  no ip directed-broadcast
  ring-speed 16
  source-bridge 10 1 3
  source-bridge spanning
!
interface Serial1/0
  ip address 1.1.1.1 255.255.255.0
  no ip directed-broadcast
  no ip mroute-cache
  clockrate 32000
!
end
```

이 디버그 출력은 Caracas 라우터에서 4000.3745.0000으로 향하는 프레임 수신할 때 발생하는 작업을 나타냅니다. Caracas에는 하나의 DLSw 원격 피어(상파울루)만 있지만 이전 컨피그레이션에서 상파울로는 피어에게 MAC 주소에 연결할 수 없음을 나타냅니다.

CARACAS#**show debug**

```
DLSw:
  DLSw Peer debugging is on
  DLSw RSVP debugging is on
DLSw reachability debugging is on at verbose level for SNA traffic
  DLSw basic debugging for peer 1.1.1.1(2065) is on
DLSw core message debugging is on
DLSw core state debugging is on
DLSw core flow control debugging is on
DLSw core xid debugging is on
  DLSw Local Circuit debugging is on
```

CARACAS#

```
Mar  2 21:37:42.570: DLSW Received-ctlQ : CLSI Msg : TEST_STN.Ind  dlen: 40
Mar  2 21:37:42.570: CSM: update local cache for mac 0000.8888.0000, DLSw Port0
Mar  2 21:37:42.570: DLSW+: DLSw Port0 I d=4000.3745.0000-0 s=0000.8888.0000-F0
Mar  2 21:37:42.570: CSM: test_frame_proc: ws_status = NO_CACHE_INFO
Mar  2 21:37:42.570: CSM: mac address NOT found in PEER reachability list
Mar  2 21:37:42.570: broadcast filter failed mac check
Mar  2 21:37:42.574: CSM: Write to all peers not ok - PEER_NO_CONNECTIONS
Mar  2 21:37:42.574: CSM: csm_peer_put returned rc_ssp not OK
```

[원격 라우터에서 dlsw mac-address 구성](#)

이 예에서는 특정 MAC 주소를 찾을 때 각 원격 사무실 라우터가 수동으로 구성되고 원하는 중앙 라우터로 연결됩니다. 이렇게 하면 잘못된 피어로 이동하는 불필요한 트래픽이 줄어듭니다. 원격 사무실에 하나의 원격 피어만 구성된 경우 이 구성은 좋지 않습니다. 그러나 여러 원격 피어가 구성된 경우 이 컨피그레이션은 WAN 대역폭을 낭비하지 않고 원격 사이트 라우터를 올바른 위치로 보냅니다.

Caracas 라우터에 새 DLSw+ 원격 피어(2.2.2.1) 1개가 구성됩니다.

카라카스	상파울루
<pre> Current configuration: ! hostname CARACAS ! dlsw local-peer peer-id 1.1.1.2 dlsw remote-peer 0 tcp 1.1.1.1 dlsw remote-peer 0 tcp 2.2.2.1 dlsw mac-addr 4000.3745.0000 remote-peer ip-address 1.1.1.1 dlsw bridge-group 1 ! interface Ethernet0/0 no ip directed-broadcast bridge-group 1 ! interface Serial0/1 ip address 1.1.1.2 255.255.255.0 no ip directed-broadcast ! interface Serial0/2 ip address 2.2.2.2 255.255.255.0 no ip directed-broadcast clockrate 64000 ! bridge 1 protocol ieee ! end </pre>	<pre> Current configuration: ! hostname SAOPAULO ! source-bridge ring- group 3 dlsw local-peer peer-id 1.1.1.1 dlsw remote-peer 0 tcp 1.1.1.2 ! interface TokenRing0/0 no ip directed- broadcast ring-speed 16 source-bridge 10 1 3 source-bridge spanning ! interface Serial1/0 ip address 1.1.1.1 255.255.255.0 no ip directed- broadcast no ip mroute-cache clockrate 32000 ! end </pre>

Caracas 라우터의 빈 연결 가능 테이블부터 시작하여 FIP에 대한 항목이 UNCONFIRM 상태임을 확인합니다.

```

CARACAS#show dlsw reachability
DLSw Local MAC address reachability cache list
Mac Addr      status      Loc.      port      rif

DLSw Remote MAC address reachability cache list
Mac Addr      status      Loc.      peer
4000.3745.0000 UNCONFIRM REMOTE 1.1.1.1(2065) max-1f(4472)

DLSw Local NetBIOS Name reachability cache list
NetBIOS Name  status      Loc.      port      rif

DLSw Remote NetBIOS Name reachability cache list
NetBIOS Name  status      Loc.      peer
          
```

첫 번째 패킷이 FIP를 찾아 도착하면 피어 1.1.1.1(상파울로)에 대한 패킷만 2.2.2.1으로 전송되므로 다른 피어에 WAN 대역폭 및 CPU 리소스를 저장합니다.

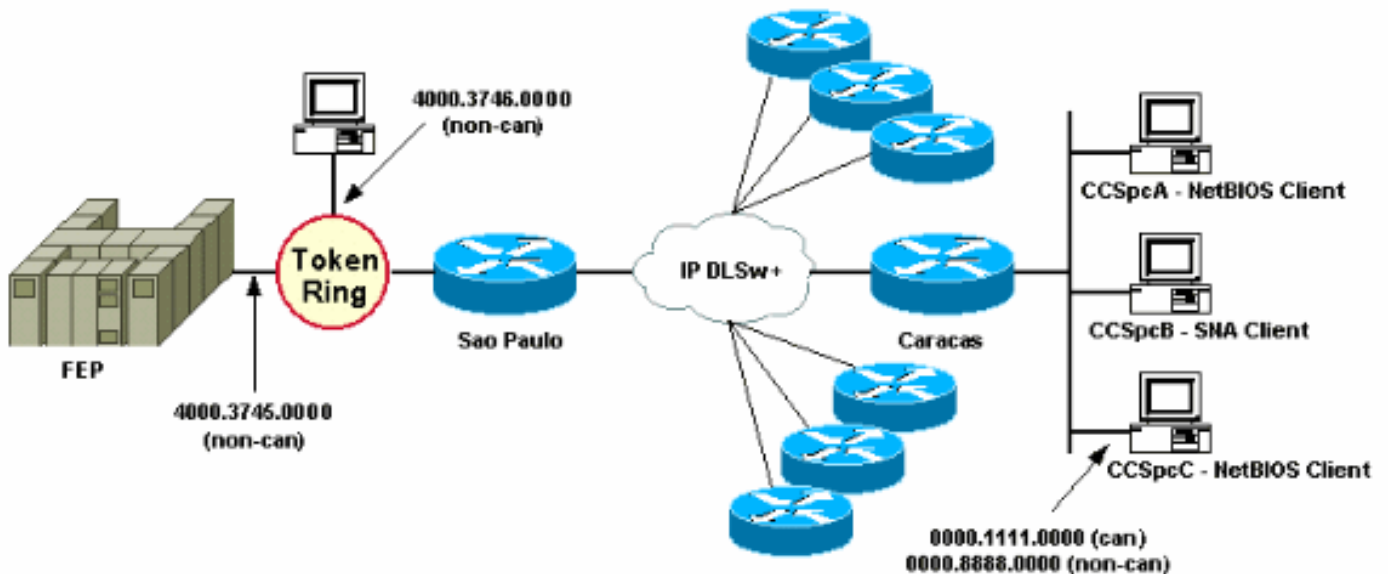
CARACAS#**debug dlsw reachability verbose sna**

DLSw reachability debugging is on at verbose level for SNA traffic

```
*Mar 2 18:38:59.324: CSM: update local cache for mac 0000.8888.0000, DLSw Port0
*Mar 2 18:38:59.324: DLSw+: DLSw Port0 I d=4000.3745.0000-0 s=0000.8888.0000-F0
*Mar 2 18:38:59.324: CSM: test_frame_proc: ws_status = UNCONFIRMED
*Mar 2 18:38:59.324: CSM: Write to peer 1.1.1.1(2065) ok
*Mar 2 18:38:59.324: CSM: csm_peer_put returned rc_ssp 1
*Mar 2 18:38:59.328: CSM: adding new icr pend record - test_frame_proc
*Mar 2 18:38:59.328: CSM: update local cache for mac 0000.8888.0000, DLSw Port0
*Mar 2 18:38:59.328: CSM: Received CLSI Msg : TEST_STN.Ind dlen: 40 from DLSw Port0
```

중앙 라우터에서 **dlsw icanreach mac-exclusive remote** 구성

이때 네트워크 다이어그램 및 설계 요구 사항이 변경됩니다.다음은 새로운 네트워크 예입니다.



이 예에서는 새로운 SNA 디바이스(4000.3746.0000)이 상파울루 위치에 추가됩니다.이 컴퓨터는 다른 위치(피어 3.3.3.1)에서 디바이스와 통신을 설정해야 합니다. 상파울루 라우터가 이 컨피그레이션을 실행합니다.

상파울루

```
Current configuration:
!
hostname SAOPAULO
!
source-bridge ring-group 3
dlsw local-peer peer-id 1.1.1.1
dlsw remote-peer 0 tcp 1.1.1.2
dlsw remote-peer 0 tcp 3.3.3.1
dlsw icanreach mac-exclusive
dlsw icanreach mac-address 4000.3745.0000 mask
ffff.ffff.ffff
!
interface TokenRing0/0
no ip directed-broadcast
ring-speed 16
source-bridge 10 1 3
source-bridge spanning
!
```

```
interface Serial1/0
 ip address 1.1.1.1 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 clockrate 32000
!
end
```

이 상파울루 컨피그레이션을 통해 상파울루 라우터는 **mac-exclusive** 명령으로 인해 MAC 주소 4000.3745.0000에만 도달할 수 있다고 모든 피어에 알립니다. 이 디버그 출력에 표시된 것처럼 새로운 SNA 장치(4000.3746.0000)이 DLSw+를 통한 통신을 설정하지 못하도록 합니다.

```
SAOPAULO#debug dlsw reachability verbose sna
DLSw reachability debugging is on at verbose level for SNA traffic
```

```
SAOPAULO#
Mar  3 00:20:27.737: CSM: Deleting Reachability cache
Mar  3 00:20:44.485: CSM: mac address NOT found in LOCAL list
Mar  3 00:20:44.485: CSM: 4000.3746.0000 DID NOT pass local mac excl. filter
Mar  3 00:20:44.485: CSM: And it is a test frame - drop frame
```

이 문제를 해결하려면 상파울루 구성을 변경하십시오.

상파울루

```
Current configuration:
!
hostname SAOPAULO
!
source-bridge ring-group 3
dlsw local-peer peer-id 1.1.1.1
dlsw remote-peer 0 tcp 1.1.1.2
dlsw icanreach mac-exclusive remote
dlsw icanreach mac-address 4000.3745.0000 mask
ffff.ffff.ffff
!
interface TokenRing0/0
 no ip directed-broadcast
 ring-speed 16
 source-bridge 10 1 3
 source-bridge spanning
!
interface Serial1/0
 ip address 1.1.1.1 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 clockrate 32000
!
end
```

remote 키워드를 사용하면 중앙 라우터의 다른 디바이스(dlsw icanreach mac-address 명령에 지정되지 않음)가 발신 연결을 설정할 수 있습니다. 이것은 장치 4000.3746.0000 연결을 시작할 때 상파울루의 디버그 출력입니다.

```
SAOPAULO#debug dlsw reachability verbose sna
DLSw reachability debugging is on at verbose level for SNA traffic
```



```
Mar 3 00:28:26.916: CSM: update local cache for mac 4000.3746.0000, TokenRing0/0
Mar 3 00:28:26.916: CSM: Received CLSI Msg : TEST_STN.Ind  dlen: 40 from TokenRing0/0
Mar 3 00:28:26.916: CSM: smac c000.3746.0000, dmac 0000.8888.0000, ssap 4 , dsap 0
Mar 3 00:28:26.916: CSM: test_frame_proc: ws_status = FOUND
Mar 3 00:28:26.920: CSM: sending TEST to TokenRing0/0
Mar 3 00:28:26.924: CSM: update local cache for mac 4000.3746.0000, TokenRing0/0
Mar 3 00:28:26.924: CSM: Received CLSI Msg : ID_STN.Ind  dlen: 54 from TokenRing0/0
Mar 3 00:28:26.924: CSM: smac c000.3746.0000, dmac 0000.8888.0000, ssap 4 , dsap 8
Mar 3 00:28:26.924: CSM: new_connection: ws_status = FOUND
Mar 3 00:28:26.924: CSM: Calling csm_to_core with CLSI_START_NEWDL
```

[관련 정보](#)

- [DLSw 지원 페이지](#)
- [DLSw+ 설계 가이드](#)
- [DLSw+ 문제 해결 가이드](#)
- [서비스 액세스 포인트 액세스 제어 목록 이해](#)