DLSw+ SAP/MAC-Filtertechniken

Inhalt

Einführung

Dieses Dokument enthält Beispielkonfigurationen für Data Link Switching plus (DLSw+) Service Access Point (SAP)- und MAC-Filtertechniken.

Die Filterung kann verwendet werden, um die Skalierbarkeit eines DLSw+-Netzwerks zu verbessern. Sie können z. B. Filterung verwenden, um:

- Reduzieren Sie den Datenverkehr über eine WAN-Verbindung (besonders wichtig bei Verbindungen mit sehr niedriger Geschwindigkeit und in Umgebungen mit NetBIOS).
- Erhöhen Sie die Sicherheit eines Netzwerks, indem Sie den Zugriff auf bestimmte Geräte kontrollieren.
- Verbessern Sie die CPU-Leistung und Skalierbarkeit von DLSw+-Routern im Rechenzentrum.

DLSw+ bietet mehrere Optionen, die zum Filtern verwendet werden können. Die Filterung kann mit MAC-Adressen, SAP- oder NetBIOS-Namen erfolgen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Konfigurieren für DLSw+ SAP-Filtertechniken

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Mithilfe der im Abschnitt Netzwerkdiagramm dargestellten Netzwerktopologie muss verhindert werden, dass der gesamte NetBIOS-Datenverkehr an Remote-Standorten den Central Router (Sao Paulo) erreicht. DLSw+ bietet mehrere Optionen zur Durchführung dieser Aufgabe, die in den folgenden Abschnitten analysiert werden.

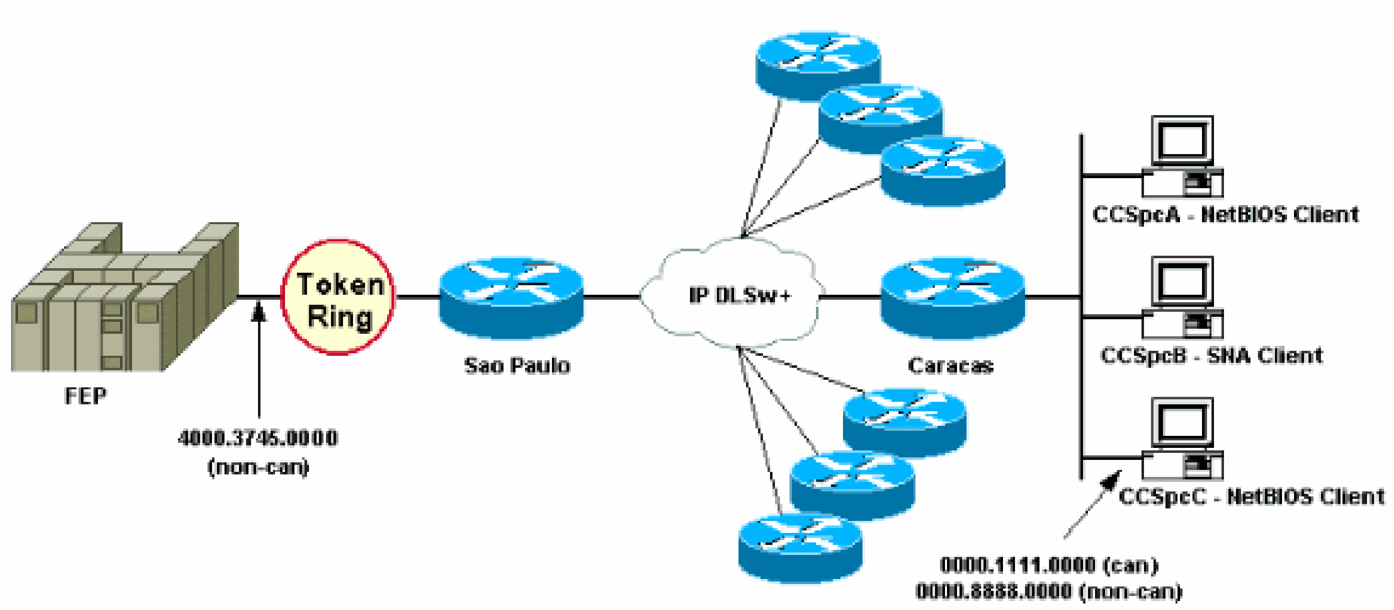
Hinweis: Der NetBIOS-Datenverkehr verwendet die SAP-Werte 0xF0 (für Befehle) und 0xF1 (für Antworten). In der Regel verwenden Netzwerkadministratoren die oben genannten SAP-Werte, um dieses Protokoll zu filtern (akzeptieren oder ablehnen).

Hinweis: NetBIOS-Clients verwenden die funktionale NetBIOS-MAC-Adresse (C000.000.0080) als Ziel-MAC (DMAC) für ihre NetBIOS-Namensabfragepakete. Wie bereits erwähnt, haben alle Frames SAP-Werte 0xF0 oder 0xF1.

Für diesen Test ist der CCSpcC-PC so konfiguriert, dass er mithilfe von SAP 0xF0 eine Verbindung zur MAC-Adresse des FEP herstellt. In Wirklichkeit sieht dieser Datenverkehr zumindest aus SAP-Perspektive genauso aus wie NetBIOS. Daher können Sie die entsprechenden Debuggen im DLSw+-Router beobachten, wenn dieser Datenverkehr eingeht.

Netzwerkdiagramm

In diesem Abschnitt wird die in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet.



Im Netzwerkdiagramm wird ein Rechenzentrums-Router (Sao Paulo) mit einer Verbindung zum Mainframe dargestellt. Dieser Router empfängt mehrere DLSw+-Peer-Verbindungen von allen Remote-Zweigstellen. Jede Außenstelle verfügt sowohl über System Network Architecture (SNA)- als auch über NetBIOS-Clients. Im Rechenzentrum befinden sich keine NetBIOS-Server, auf die von den Außenstellen aus zugegriffen werden muss.

Aus Gründen der Einfachheit werden die Konfigurationsdetails von nur einer Außenstelle (Caracas) angezeigt. Das Netzwerkdiagramm zeigt auch den MAC-Adresswert des Front-End-Prozessors (FEP) und des Remote-PCs mit dem Namen CCSpcC. MAC-Adressen werden sowohl im kanonischen (Ethernet-) als auch im nicht-kanonischen (Token Ring-)Format angezeigt.

Konfigurieren von LSAP-Ausgabenzugriffslisten in Außenstellen

Bei dieser Methode müssen alle Außenstellen mit der Option **"lsap-output-list"** konfiguriert werden. Im zentralen Router sind keine weiteren Konfigurationsänderungen erforderlich.

Die **SLSAP-Output-Liste** verweist auf eine SAP-Zugriffsliste (SAP ACL), die derzeit nur SNA-SAPs (z. B. 0x00, 0x04, 0x08 usw.) den Wechsel zum zentralen Router ermöglicht und alles andere verweigert. Weitere Informationen zur Durchführung von auf SAPs basierenden Filtern finden Sie unter Grundlagen der Zugriffskontrolllisten für Service Access Points.

CARACAS	SAO PAULO

`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`
`!`
	`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`

<table>
<tr>
<td><pre>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></td>
<td><pre>

!
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></td>
</tr>
</table>

Mit dem **Befehl debug dlsw** wird angezeigt, wie der Caracas-Router reagiert, wenn er den NetBIOS-Datenverkehr empfängt.

```
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
```

Wenn der Router in der Außenstelle (Caracas) über keine Erreichbarkeitsinformationen für 4000.3745.000 verfügt und einen Explorer erhält, der mithilfe einiger der "verbotenen" SAPs nach dieser MAC-Adresse sucht, wird die Anforderung blockiert.

```
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
```

Beispiel: Der Router der Außenstelle (Caracas) verfügt über Informationen zur Erreichbarkeit für 4000.3745.000. Beispielsweise hat bereits eine andere Station (unter Verwendung der zulässigen SAPs) nach der FEP-MAC-Adresse gefragt. In dieser Situation sendet der "Straftäter"-PC (CCSpcC) seine NULL-XID, aber der Router beendet sie.

```
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
```

Konfigurieren Sie dlsw icannotreach saps auf dem zentralen Router.

Mit dem Befehl **dlsw icannotreach saps** können Sie die Protokolle filtern, von denen Sie wissen, dass sie nicht weitergeleitet werden dürfen. Wenn Sie nur wissen, was explizit abgelehnt werden muss, verwenden Sie den Befehl **dlsw icannotreach saps** auf den zentralen Routern, wie in diesen Konfigurationen gezeigt.

<table>
<tr><th>CARACAS</th><th>SAO PAULO</th></tr>
<tr><td><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></td><td><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 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></td></tr>
</table>

Sie können den zentralen Router (einschließlich des Befehls **dlsw icannotreach saps**) während der Fahrt konfigurieren, auch wenn die Remote-Peers bereits aktiv sind. Diese Ausgabe zeigt das Debuggen auf einem der Remote-Router an, was den Empfang der CapExId-Meldung anzeigt. Diese Meldung weist die Außenstellen an, keine Frames mit SAP 0xF0/F1 an den zentralen Router zu senden.

```
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
```

Nachdem die CapExId-Nachricht empfangen wurde, erfährt der Caracas-Router, dass Sao Paulo SAP 0xF0 nicht unterstützt.

```
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-JK2O3S-M), Version 12.0(7)T,  RELEASE SOFTWARE (fc2)
 Copyright (c) 1986-1999 by cisco Systems, Inc.
```

Die hier angezeigte Befehlsausgabe **show** am zentralen Router zeigt die Konfigurationsänderung, bei der SAP 0xF0 nicht unterstützt wird.

```
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-JK2O3S-M), Version 12.0(7)T,  RELEASE SOFTWARE (fc2)
 Copyright (c) 1986-1999 by cisco Systems, Inc.
```

Dies ist die **Debug**-Ausgabe vom Caracas-Router, wenn die NetBIOS-PC-Station die Verbindung versucht:

```
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
```

Konfigurieren Sie dlsw icanreach saps auf dem zentralen Router.

Die Konfiguration des Befehls **dlsw icanreach saps** ist nützlich, wenn Sie genau wissen, welche Art von Datenverkehr zulässig ist, und Sie sicherstellen möchten, dass der gesamte andere Datenverkehr abgelehnt wird. Wenn Sie beispielsweise **dlsw icanreach saps 4** konfigurieren, verweigern Sie explizit alle Saps außer 0x04 (und 0x05, die Antwort).

<table>
<tr><th>CARACAS</th><th>SAO PAULO</th></tr>
<tr><td><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
</pre></td><td><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
</pre></td></tr>
</table>

```
 ip address 1.1.1.2
255.255.255.0
 no ip directed-
broadcast
!
bridge 1 protocol ieee
!
end
```

```
 ip address 1.1.1.1
255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 clockrate 32000
!
end
```

Beachten Sie in dieser **show**-Befehlsausgabe, dass der Caracas-Router erkennt, dass Sao Paulo nur Frames unterstützt, die auf die Werte 0x04 und 0x05 ausgerichtet sind. Alle anderen Saps werden nicht unterstützt.

```
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.
```

Mit dem **lokalen** Befehl **show dlsw-Funktionen** können Sie überprüfen, ob die Konfigurationsänderungen am zentralen Router im DLSw+-Code angezeigt werden.

```
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-Filtertechniken

Stellen Sie mithilfe des Netzwerkdiagramms in diesem Dokument sicher, dass der zentrale Router Frames empfängt, die nur für die FEP-MAC-Adresse (4000.3745.000) bestimmt sind.

Konfigurieren der CMC-Adresse von dlsw icanreach auf dem zentralen Router

Mit dem Befehl **dlsw icanreach mac-address** haben alle Außenstellen einen Eintrag in ihrer DLSw+-Erreichbarkeitstabelle für die MAC-Adresse des Hosts, die auf die IP-Adresse des zentralen Routers zeigt. Dieser Eintrag befindet sich im UNCONFIRM-Status. Dieser gibt an, dass, wenn der Router der Außenstelle einen lokalen Test oder eine XID für den Host empfängt, er nur eine CUR_ex (Can U Reach Explorer)-Nachricht an den zentralen Router sendet.

CARACAS	SAO PAULO
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 !	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

interface Serial0/1 ip address 1.1.1.2 255.255.255.0 no ip directed- broadcast ! bridge 1 protocol ieee ! end	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

Hier hat der Caracas-Router einen permanenten Eintrag im Erreichbarkeitscache erstellt. Wenn der Eintrag nicht frisch ist, lautet der Status UNCONFIRM (NICHT BESTÄTIGT). Im Kapitel Erreichbarkeit des DLSw+-Fehlerbehebungsleitfadens finden Sie weitere Informationen dazu, wie DLSw+-Router MAC-Adressen und NetBIOS-Namen zwischenspeichern.

```
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
```

Die Ausgabe des Befehls **show dlsw functions** auf dem Caracas-Router bestätigt, dass diese Außenstelle weiß, dass die MAC-Adresse 4000.3745.000 über Peer 1.1.1 erreichbar ist. Beachten Sie auch die Zeile "icanreach mac-exklusiv: Nein". Sie weist darauf hin, dass der zentrale Router neben dem Host auch andere MAC-Adressen erreichen kann. Wenn eine der Außenstellen daher nach anderen MAC-Adressen sucht, können sie ihre Anfragen an den zentralen Router senden. Mit der Aufnahme des Befehls **icanreach mac-address 4000.3745.0000** sind jedoch alle Außenstellen über den Speicherort dieser wichtigen Ressource informiert. Wenn Sie weitere Einschränkungen für die eingehenden Frames am zentralen Router festlegen möchten, lesen Sie Configure dlsw icanreach mac-excluded auf dem Central Router.

```
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  : 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-JK2O3S-M), Version 12.0(7)T,  RELEASE SOFTWARE (fc2)
 Copyright (c) 1986-1999 by cisco Systems, Inc.
```

Sie können den **mask** Parameter als **dlsw icanreach MAC-Adresse 4000.3745.000***mask ffff.ffff.ffff* verwenden. Wenn Sie diesen Parameter verwenden, beachten Sie, dass MAC-Adressen in der Regel im hexadezimalen Format angezeigt werden (0x4000.3745.000). Daher wird eine All-One-Maske (binär) durch die Hexadezimalzahl 0xFFFF.FFFF.FFFF dargestellt.

Nachfolgend finden Sie ein Beispiel, wie Sie bestimmen können, ob eine bestimmte Eingabe-MACs unter einem bereits konfigurierten Befehl **dlsw icanreach mac-address** enthalten ist:

1. Beginnen Sie mit einem Router, der mit dem Befehl **dlsw icanreach mac-address 4000.3745.000 mask ffff.ffff** 000 konfiguriert ist.
2. Prüfen Sie, ob die Eingabe-MAC-Adresse 4000.3745.0009 durch den vorherigen Router-Konfigurationsbefehl enthalten ist oder nicht.
3. Konvertieren Sie zunächst die MAC-Adresse (4000.3745.0009) und die konfigurierte MASK (FFFF.FFFF.000) von der hexadezimalen in die binäre Darstellung. Die ersten beiden Zeilen in dieser Tabelle zeigen diesen Schritt.
4. Führen Sie dann einen logischen AND-Vorgang zwischen diesen beiden Binärzahlen aus, und konvertieren Sie das Ergebnis in eine hexadezimale Darstellung (4000.3745.000). Das Ergebnis dieser Operation wird in der dritten Zeile dieser Tabelle dargestellt.
5. Wenn das Ergebnis des AND-Vorgangs mit der MAC-Adresse im Befehl **dlsw icanreach mac-address** (in unserem Beispiel 4000.3745.0000) übereinstimmt, wird die Eingabe-MAC-Adresse (4000.3745.0009) von der -Adresse zugelassen w icanreach mac-address-Befehl. In unserem Beispiel ist jede Eingabe-MAC-Adresse im Bereich 4000.3745.000 bis 4000.3745.FFFF im Befehl **dlsw icanreach mac-address** enthalten. Sie können dies überprüfen, indem Sie die gleichen Schritte für alle MAC-Adressen in diesem Bereich wiederholen.

Hier einige weitere Beispiele:

- **dlsw icanreach mac-address 4000.3745.0000 mask ffff.ffff.ffff** - Dieser Befehl enthält nur die MAC-Adresse 4000.3745.0000. Diese Maske wird von keiner anderen MAC-Adresse übergeben.
- **dlsw icanreach mac-address 4000.000.3745 mask ffff.0000.ffff** - Dieser Befehl enthält alle MAC-Adressen im Bereich 4000.XXXX.3745, wobei XXXX 0x000-0xFFX entspricht FF.

Konfigurieren Sie dlsw icanreach mac-exklusiv auf dem zentralen Router.

Mit dem Befehl **dlsw icanreach mac-exklusiv**, der auf dem zentralen Router konfiguriert ist, stellen Sie sicher, dass nur Pakete an den zuvor definierten MAC-Adressen (in diesem Fall 4000.3745.000) am zentralen Standort zugelassen sind.

Beachten Sie, dass diese Filterinformationen unter Verwendung von CapExId-Nachrichten zwischen allen DLSw+-Peers ausgetauscht werden. Sie sparen WAN-Bandbreite, indem Sie die Filterinformationen am zentralen Standort konfigurieren, obwohl die Aktionen (z. B. Blockieren von Frames) bei den Remote-Routern selbst stattfinden.

<table>
<tr><th>CARACAS</th><th>SAO PAULO</th></tr>
<tr><td><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></td><td><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></td></tr>
</table>

Beachten Sie in dieser Ausgabe, dass der Caracas-Router weiß, dass die MAC-Adresse 4000.3745.000 über Peer 1.1.1.1 erreichbar ist. Der Unterschied zwischen diesem Beispiel und dem vorherigen Szenario besteht darin, dass hier "icanreach mac-exklusiv: ja", d. h. die Außenstellen senden keine Frames an den zentralen Router, die nicht für 4000.3745.000 bestimmt sind.

```
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-JK2O3S-M), Version 12.0(7)T,  RELEASE SOFTWARE (fc2)
 Copyright (c) 1986-1999 by cisco Systems, Inc.
```

Die **Debug**-Ausgabe zeigt hier, wie der Caracas-Router auf eingehenden Datenverkehr reagiert, der an eine andere MAC-Adresse als 4000.3745.0000 (hier 4000.3745.0080 verwendet) gerichtet ist. Caracas verwendet Sao Paulo nicht für Frames, die nicht für den Gastgeber bestimmt sind (4000.3745.000). In diesem Fall ist Sao Paulo der einzige Remote-Peer, der in Caracas konfiguriert ist, daher hat dieser Router keinen anderen Peer, an den er gesendet werden kann.

```
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
```

Wenn Sie einen Router mit dem Befehl **dlsw icanreach mac-exklusiv** konfigurieren, ohne eine MAC-Adresse mit dem Befehl **dlsw icanreach mac-address** zu definieren, teilt der Router seinen Peers mit, dass er überhaupt keine MAC-Adressen erreichen kann. Daher verlieren Sie die Kommunikation über diesen Peer.

Hinweis: Die hier gezeigte Beispielkonfiguration wird nur als Beispiel angezeigt. Das ist ein Fehler und **sollte nicht verwendet werden**.

SAO PAULO

```
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
```

Diese **Debug**-Ausgabe gibt an, was beim Caracas-Router geschieht, wenn ein Frame für 4000.3745.0000 empfangen wird. Beachten Sie, dass Caracas nur über einen DLSw-Remote-Peer (Sao Paulo) verfügt. In der vorherigen Konfiguration hat Sao Paulo seinen Peers jedoch mitgeteilt, dass keine MAC-Adressen erreicht werden können.

```
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
```

Konfigurieren der DLSW-MAC-Adresse auf den Remote-Routern

In diesem Beispiel wird jeder Router in der Außenstelle manuell konfiguriert und an den gewünschten zentralen Router weitergeleitet, wenn er nach bestimmten MAC-Adressen sucht. Dadurch wird unnötiger Datenverkehr reduziert, der an den falschen Peer geleitet wird. Wenn in der Außenstelle nur ein Remote-Peer konfiguriert ist, ist diese Konfiguration nicht hilfreich. Wenn jedoch mehrere Remote-Peers konfiguriert sind, wird der Router am Remote-Standort mithilfe dieser Konfiguration an den richtigen Ort weitergeleitet, ohne dass die WAN-Bandbreite verschwendet wird.

Am Caracas-Router wird ein neuer DLSw+-Remote-Peer (2.2.2.1) konfiguriert.

CARACAS	SAO PAULO
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	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

Beachten Sie, dass sich der Eintrag für FEP im UNCONFIRM-Status befindet, beginnend mit einer leeren Erreichbarkeitstabelle am Caracas-Router:

```
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-lf(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
```

Wenn das erste Paket auf der Suche nach FEP ankommt, werden nur die Pakete an Peer 1.1.1.1 (Sao Paulo) gesendet und nicht an 2.2.2.1. Daher sparen Sie WAN-Bandbreite und CPU-Ressourcen auf den anderen Peers ein.

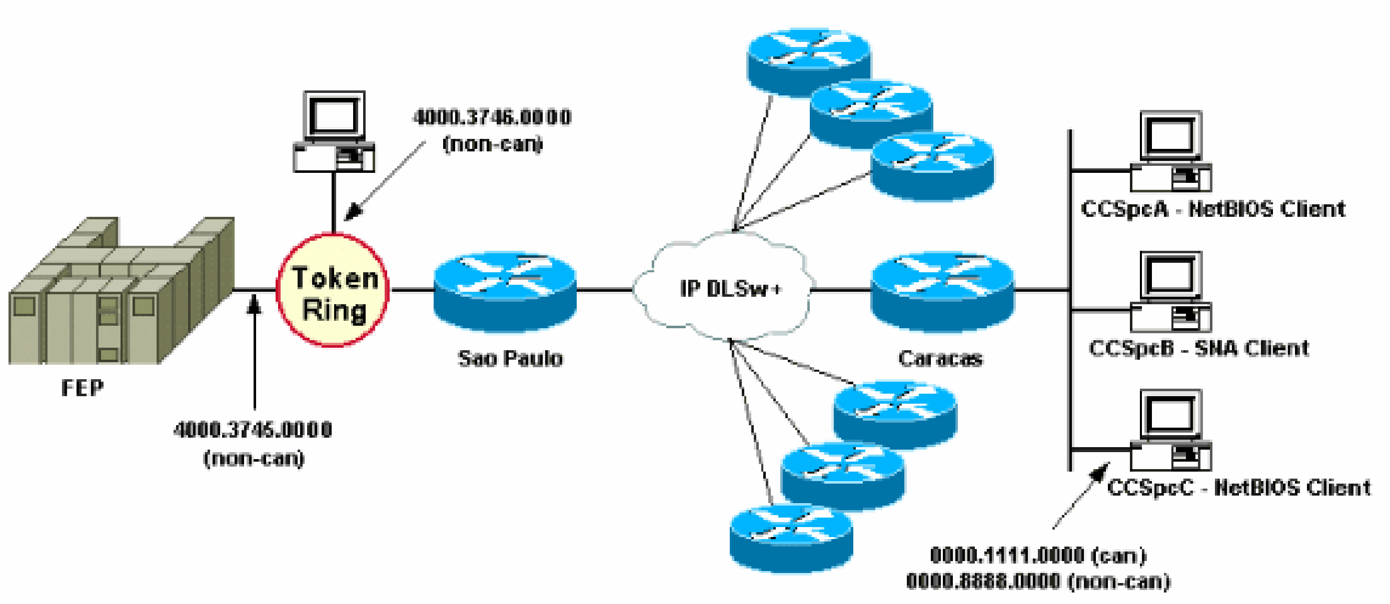
```
CARACAS#debug dlsw reachability verbose sna
 DLSw reachability debugging is on at verbose level for SNA traffic

 *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
```

Konfigurieren Sie dlsw icanreach mac-exklusive Remote am zentralen Router.

An diesem Punkt werden das Netzwerkdiagramm und die Design-Anforderungen geändert. Dies ist das neue Netzwerkbeispiel:



In diesem Beispiel wird am Standort Sao Paulo ein neues SNA-Gerät (4000.3746.000) hinzugefügt. Diese Maschine muss die Kommunikation mit einem Gerät an einem anderen Standort (Peer 3.3.3.1) herstellen. Diese Konfiguration wird vom Sao Paulo-Router ausgeführt.

SAO PAULO
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
```

Mit dieser Konfiguration von Sao Paulo informiert der Sao Paulo-Router alle seine Peers, dass er aufgrund des **MAC-exklusiven** Befehls nur die MAC-Adresse 4000.3745.000 erreichen kann. Wie in dieser **Debug**-Ausgabe gezeigt, verhindert dies auch, dass das neue SNA-Gerät (4000.3746.000) eine Kommunikation über DLSw+ aufbaut.

```
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
```

Nehmen Sie diese Änderungen an der Konfiguration von Sao Paulo vor, um dies zu beheben.

SAO PAULO

<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 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</pre>

Mit dem **remote**-Schlüsselwort können andere Geräte am zentralen Router (die nicht im **Befehl dlsw icanreach mac-address** angegeben sind) ausgehende Verbindungen herstellen. Dies ist die **Debug-**Ausgabe auf Sao Paulo, wenn das Gerät 4000.3746.000 seine Verbindung gestartet.

```
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
```

Zugehörige Informationen

- DLSw-Support-Seite
- DLSw+ Designleitfaden
- Leitfaden zur DLSw+-Fehlerbehebung
- Übersicht über die Zugriffskontrolllisten für Service Access Points