DLSw+ SAP/MAC Filtering Techniques

Contents

Introduction

This document provides sample configurations for data-link switching plus (DLSw+) Service Access Point (SAP) and MAC filtering techniques.

Filtering can be used to enhance the scalability of a DLSw+ network. For example, you can use filtering to:

- Reduce traffic across a WAN link (especially important on very low-speed links and in environments with NetBIOS).
- Enhance the security of a network by controlling access to certain devices.
- Enhance the CPU performance and scalability of data-center DLSw+ routers.

DLSw+ offers several options that can be used to perform filtering. Filtering can be done on MAC addresses, SAP, or NetBIOS names.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configure for DLSw+ SAP Filtering Techniques

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Using the network topology depicted in the Network Diagram section, the requirement is to stop all NetBIOS traffic at remote locations from reaching the Central router (Sao Paulo). DLSw+ offers several options to accomplish this task, which are analyzed in the following sections.

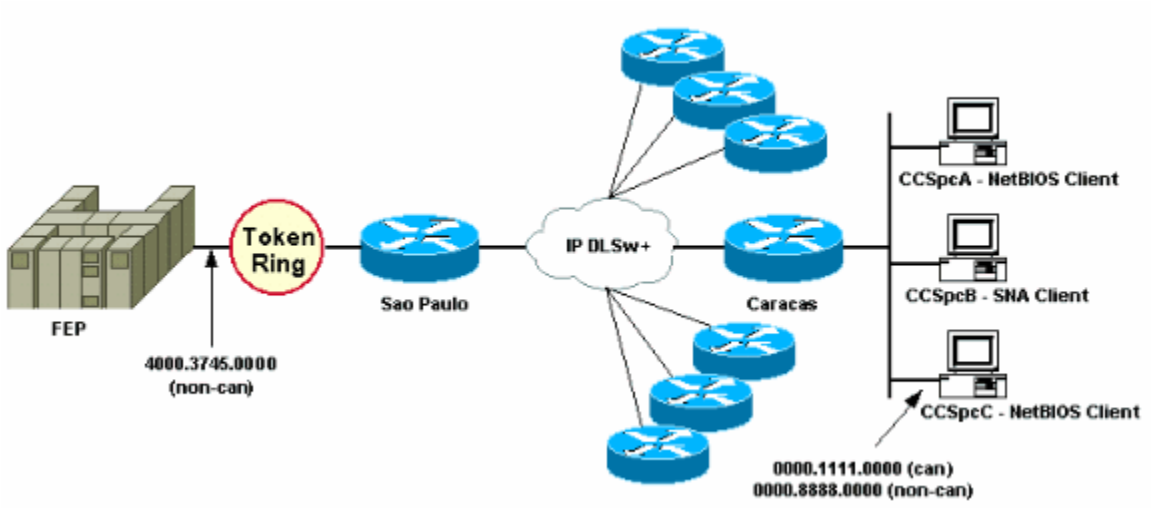
Note: NetBIOS traffic uses SAP values 0xF0 (for commands) and 0xF1 (for responses). Typically, network administrators use the above-mentioned SAP values to filter (accept or deny) this protocol.

Note: NetBIOS clients use the NetBIOS functional MAC address (C000.0000.0080) as the destination MAC (DMAC) on their NetBIOS Name Query packets. As mentioned earlier, all frames have SAP values of 0xF0 or 0xF1.

For this test, the CCSpcC PC is configured to connect to the MAC address of the FEP using SAP 0xF0. In reality this traffic looks the same as NetBIOS, at least from a SAP perspective. Therefore, you can observe the corresponding debugs in the DLSw+ router when this traffic arrives.

Network Diagram

This section uses the network setup shown in this diagram.



In the network diagram, a data center router (Sao Paulo) is depicted with a connection to the mainframe. This router receives multiple DLSw+ peer connections from all the remote branches. Each remote branch has both Systems Network Architecture (SNA) and NetBIOS clients. There are no NetBIOS servers in the data center that need to get accessed from the remote offices.

For simplicity, the configuration details of only one remote office (Caracas) are shown. The network diagram also shows the MAC address value of the front-end processor (FEP) and the remote PC called CCSpcC. MAC addresses are shown in both canonical (Ethernet) and non-canonical (Token Ring) format.

Configure LSAP Output Access Lists at Remote Offices

Using this method, all remote offices must be configured with the **lsap-output-list** option. No other configuration changes are required in the central router.

The **lsap-output-list** links to a SAP access list (SAP ACL) that currently only allows SNA SAPs (for example, 0x00, 0x04, 0x08, and so on) to go toward the central router, and denies everything else. Refer to Understanding Service Access Point Access Control Lists for more

information on how to perform filtering based on SAPs.

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 ! 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	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

The **debug dlsw** command is used to see how the Caracas router reacts when it receives the NetBIOS traffic.

```
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
```

If the remote office router (Caracas) does not have reachability information for 4000.3745.0000, and it gets an explorer that looks for that MAC address using some of the "prohibited" SAPs, then the request is blocked.

```
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
```

Consider the case where the remote office router (Caracas) does have reachability information for 4000.3745.0000. For instance, another station (using the allowed SAPs) already asked for the FEP MAC address. In this situation the "offender" PC (CCSpcC) sends its NULL XID, but the router stops it.

```
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
```

Configure dlsw icannotreach saps at the Central Router

Using the **dlsw icannotreach saps** command allows you to filter those protocols you know are not allowed to be sent across. If you know only what must be explicitly denied, use the **dlsw icannotreach saps** command on the central router(s), as shown in these configurations.

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 ! interface Serial0/1 ip address 1.1.1.2 255.255.255.0 no ip directed-broadcast ! 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 **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

You can configure the central router (include the **dlsw icannotreach saps** command) on the fly, even when the remote peers are already up. This output shows the debug on one of the remote routers, which indicates the reception of the CapExId message. This message instructs the remote offices not to send any frames with SAP 0xF0/F1 toward the central router.

```
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:
*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
```

After the CapExId message is received, the Caracas router learns that Sao Paulo does not support SAP 0xF0.

```
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.
```

The **show** command output displayed here, taken at the central router, shows the configuration change where SAP 0xF0 is not supported.

```
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.
```

This is the **debug** output from the Caracas router when the NetBIOS PC station attempts the connection:

```
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
```

Configure dlsw icanreach saps at the Central Router

Configuring the **dlsw icanreach saps** command is useful when you know exactly what type of traffic is allowed and you want to make sure that all other traffic is denied. For example, when you configure **dlsw icanreach saps 4**, you explicitly deny all saps except 0x04 (and 0x05, the response).

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 ! interface Serial0/1 ip address 1.1.1.2 255.255.255.0 no ip directed-broadcast ! 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 **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

Note in this **show** command output that the Caracas router recognizes that Sao Paulo only supports frames destined to saps 0x04 and 0x05. All other saps are unsupported.

```
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.
```

You can use the **show dlsw capabilities local** command to verify that the configuration changes at the central router appear in the DLSw+

code.

```
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 Filtering Techniques

Using the network diagram shown in this document, make the central router receive frames destined to the FEP MAC address (4000.3745.0000) only.

Configure dlsw icanreach mac-address at the Central Router

Using the **dlsw icanreach mac-address** command, all remote offices have an entry on their DLSw+ reachability table for the host MAC address that points to the central router IP address. This entry is in the UNCONFIRM state, which indicates that if the remote office router receives a local test or XID for the host, it sends a CUR_ex (Can U Reach Explorer) message to the central router only.

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 ! interface Serial0/1 ip address 1.1.1.2 255.255.255.0 no ip directed-broadcast ! bridge 1 protocol ieee	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
end                                      clockrate 32000
                                         !
                                         end
```

Here, the Caracas router has created a permanent entry in its reachability cache. If the entry is not fresh, the state is UNCONFIRM. Refer to the DLSw+ Troubleshooting Guide Reachability Chapter for more information on how DLSw+ routers cache MAC addresses and NetBIOS names.

```
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
```

The output of the **show dlsw capabilities** command on the Caracas router confirms that this remote office knows the MAC address 4000.3745.0000 is reachable via the peer 1.1.1.1. Also note the line that says "icanreach mac-exclusive : no". It indicates that the central router is capable of reaching other MAC addresses besides the host. Therefore, if any of the remote offices look for other MAC address, they can send their requests to the central router. However, with the inclusion of the **icanreach mac-address 4000.3745.0000** command, all remote branches are aware of the location of this important resource. If you want to place further restrictions on what frames arrive at the central router, refer to Configure dlsw icanreach mac-exclusive at 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 <mask ffff.ffff.ffff>
   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.
```

You can use the **mask** parameter as **dlsw icanreach mac-address 4000.3745.0000** *mask ffff.ffff.ffff* . When you use this parameter, note that MAC addresses are typically presented in hexadecimal format (0x4000.3745.0000). Therefore an all-ones mask (in binary) is represented by the hexadecimal number 0xFFFF.FFFF.FFFF.

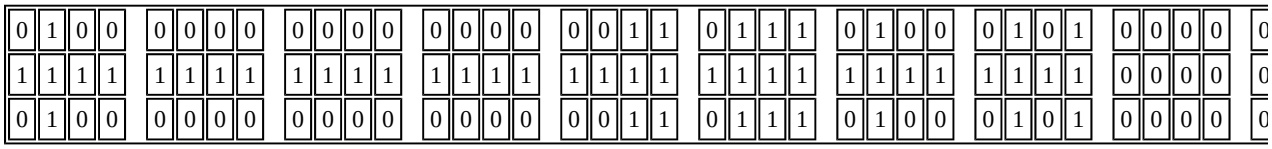
Here is an example of how to determine if a particular input MAC is included under an already configured **dlsw icanreach mac-address** command:

1. Start with a router configured with the **dlsw icanreach mac-address 4000.3745.0000 mask ffff.ffff** 0000 command.

2. Evaluate whether or not the input MAC address 4000.3745.0009 is included by the previous router configuration command.

3. First, convert the MAC address (4000.3745.0009) and the configured MASK (FFFF.FFFF.0000) from hexadecimal to binary representation. The first two rows in this table show this step.

4. Then, perform a logical AND operation between those two binary numbers, and convert the result to hexadecimal representation (4000.3745.0000). The result of this operation is depicted in the third row of this table.



5. If the result of the AND operation matches the MAC address in the **dlsw icanreach mac-address** command (in our example, 4000.3745.0000), then the input MAC address (4000.3745.0009) is allowed by the **dlsw icanreach mac-address** command. In our example, any input MAC address within the range 4000.3745.0000 to 4000.3745.FFFF is included by the **dlsw icanreach mac-address** command. You can verify this by repeating the same steps for any MAC addresses in this range.

These are a few more examples:

- **dlsw icanreach mac-address 4000.3745.0000 mask ffff.ffff.ffff**—This command only includes the MAC address 4000.3745.0000. No other MAC addresses pass this mask.

- **dlsw icanreach mac-address 4000.0000.3745 mask ffff.0000.ffff**—This command includes all the MAC addresses in the range 4000.XXXX.3745 where XXXX is 0x0000-0xFFFF.

Configure dlsw icanreach mac-exclusive at the Central Router

With the **dlsw icanreach mac-exclusive** command configured at the central router, you ensure that only packets destined to the MAC addresses previously defined (in this case 4000.3745.0000) are allowed at the central location.

Note that this filtering information is exchanged between all the DLSw+ peers using CapExId messages. You save WAN bandwidth by configuring the filtering information at the central location, even though the actions (such as blocking frames) occur at the remote routers themselves.

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

```
end
```

```
 no ip mroute-cache
 clockrate 32000
!
end
```

Observe in this output that the Caracas router knows the MAC address 4000.3745.0000 is reachable via peer 1.1.1.1. The difference between this example and the previous scenario is that here we show "icanreach mac-exclusive : yes", which means that the remote offices do not send frames toward the central router other than those destined for 4000.3745.0000.

```
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 <mask ffff.ffff.ffff>
   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.
```

The **debug** output here shows how the Caracas router reacts to incoming traffic destined to any MAC address other than 4000.3745.0000 (4000.3745.0080 is used here). Caracas does not use Sao Paulo for frames not destined to the host (4000.3745.0000). In this case, Sao Paulo is the only remote peer configured in Caracas, so this router has no other peer to which to send it.

```
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
```

If you configure a router with the **dlsw icanreach mac-exclusive** command without defining any MAC address using the **dlsw icanreach mac-address** command, the router advertises to its peers that it can reach no MAC addresses at all. Therefore you will lose communication through that peer.

Note: The sample configuration here is shown only as an example. It is a mistake and **should not be used**.

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

This **debug** output indicates what happens at the Caracas router when it receives a frame destined to 4000.3745.0000. Note that Caracas only has one DLSw remote-peer (Sao Paulo), but in the previous configuration , Sao Paulo indicated to its peers that it cannot reach any MAC addresses.

```
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
```

Configure dlsw mac-address at the Remote Routers

In this example, each remote office router is manually configured and directed to the desired central router when looking for specific MAC addresses. This reduces unnecessary traffic that goes to the wrong peer. If the remote office only has one remote peer configured, then this configuration is not beneficial. However, if multiple remote peers are configured, this configuration directs the remote site router to the right place without wasting WAN bandwidth.

One new DLSw+ remote peer (2.2.2.1) is configured at the Caracas router.

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**	Current configuration: ! hostname SAOPAULO !

```
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
```

```
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
```

Beginning with an empty reachability table at the Caracas router, note that the entry for the FEP is in UNCONFIRM status:

```
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
```

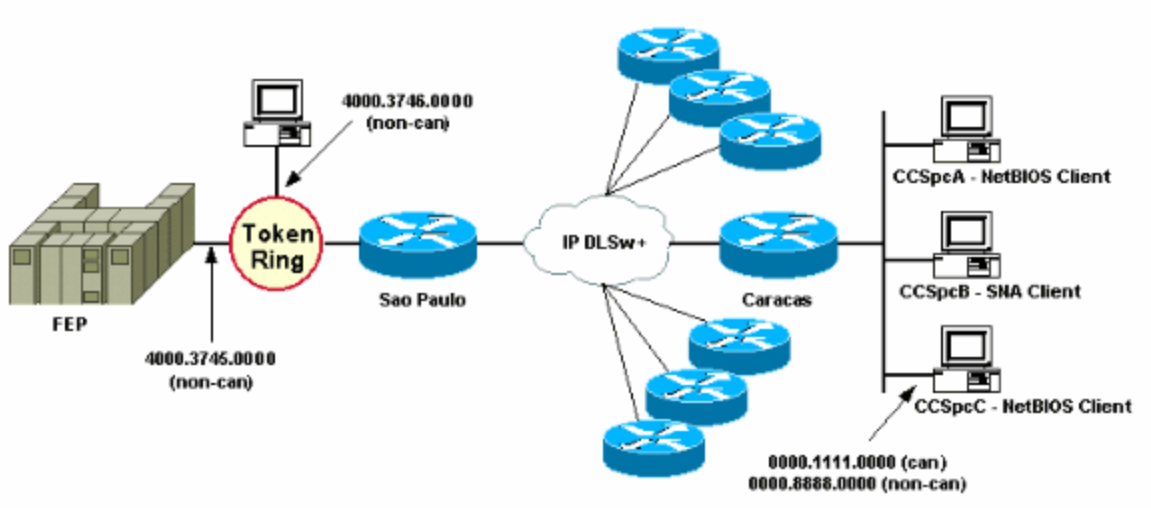
When the first packet arrives looking for FEP, only the packets to peer 1.1.1.1 (Sao Paulo) are sent and not to 2.2.2.1. Therefore, you save WAN bandwidth and CPU resources on the other peers.

```
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
```

Configure dlsw icanreach mac-exclusive remote at the Central Router

At this point, the network diagram and design requirements are changed. This is the new network example:



In this example, a new SNA device (4000.3746.0000) is added at the Sao Paulo location. This machine needs to establish communication with a device at another location (peer 3.3.3.1). The Sao Paulo router runs this configuration.

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
```

With this Sao Paulo configuration, the Sao Paulo router informs all its peers that, due to the **mac-exclusive** command, it can only reach the MAC address 4000.3745.0000. As shown in this **debug** output, this also prevents the new SNA device (4000.3746.0000) from establishing communication through DLSw+.

```
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
```

To fix this, make these changes to the Sao Paulo configuration.

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 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
```

With the **remote** keyword, other devices at the central router are allowed (that are not specified in the **dlsw icanreach mac-address** command) to make outgoing connections. This is the **debug** output on Sao Paulo when the device 4000.3746.0000 started its connection.

```
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
```

Related Information

- **DLSw Support Page**
- **DLSw+ Design Guide**
- **DLSw+ Troubleshooting Guide**
- **Understanding Service Access Point Access Control Lists**
