DLSw+ SAP/MAC フィルタリング技術

目次

概要

このドキュメントでは、data-link switching plus（DLSW+; データリンク スイッチング プラス）Service Access Point（SAP; サービス アクセス ポイント）および MAC のフィルタリング方式の設定例を紹介しています。

フィルタリングを使用すると、DLSw+ ネットワークのスケーラビリティを強化できます。 たとえば、フィルタリングを次の目的に使用できます。

- WAN リンクを経由するトラフィックを削減する（きわめて低速なリンクおよび NetBIOS が存在する環境で特に重要）。
- 特定のデバイスへのアクセスを制御することによりネットワークのセキュリティを高める。
- データセンターの DLSw+ ルータの CPU パフォーマンスとスケーラビリティを高める。

DLSw+ には、フィルタリングの実行に使用できるいくつかのオプションがあります。 フィルタリングは、MAC アドレス、SAP、または NetBIOS 名に対して実行できます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

DLSw+ SAP/MAC のフィルタリング テクニックの設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

「ネットワーク ダイアグラム」セクションに示されているネットワーク トポロジを使用して、すべての NetBIOS トラフィックを、リモート ロケーションで中央ルータ（Sao Paulo）に到達しないようにすることが要件です。 DLSw+ にはこの作業を実施するためのいくつかのオプションがあります。これらのオプションは以降のセクションで分析しています。

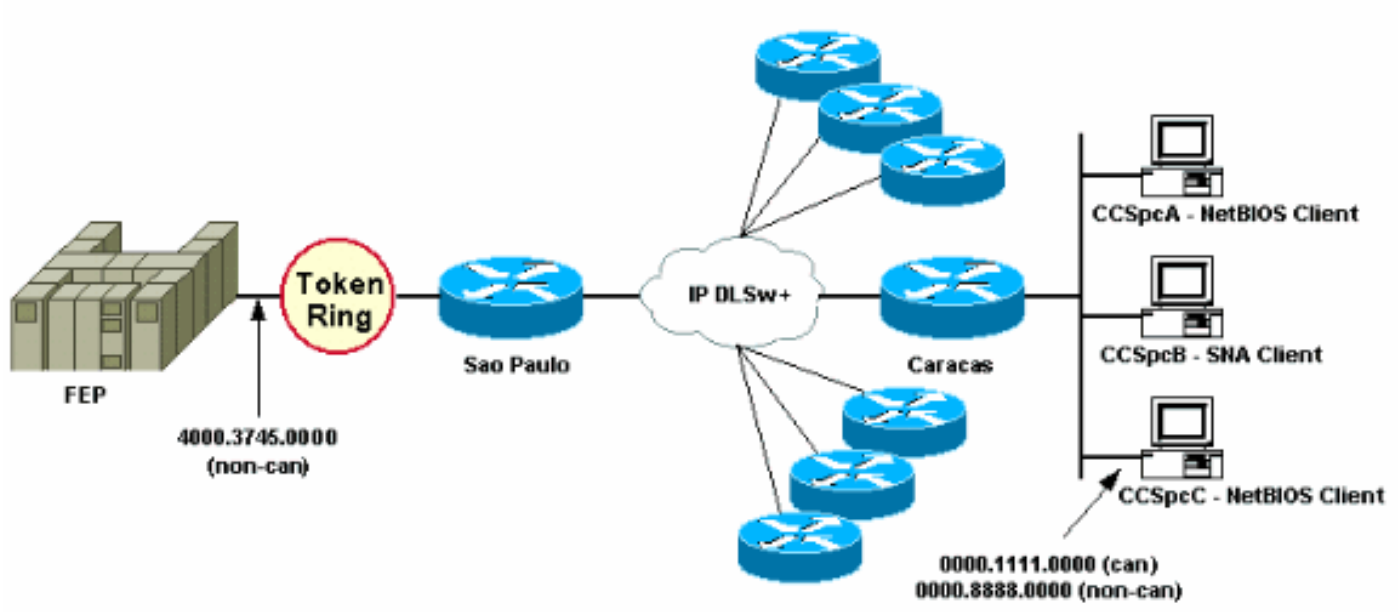
注: NetBIOS トラフィックでは SAP 値 0xF0（コマンド用）と 0xF1（応答用）が使用されます。通常、ネットワーク管理者は上記の SAP 値を使用して、このプロトコルのフィルタリング（受け入れまたは拒否）を行います。

注: NetBIOS クライアントでは、NetBIOS Name Query パケット上で宛先 MAC（DMAC）として NetBIOS 機能 MAC アドレス（C000.0000.0080）を使用します。 すでに述べたように、すべてのフレームには 0xF0 または 0xF1 の SAP 値があります。

このテストのため、SAP 0xF0 を使用する FEP の MAC アドレスに接続するよう CCSpcC PC が設定されています。 実際には、少なくとも SAP の観点からは、このトラフィックは NetBIOS と同じに見えます。 そのため、このトラフィックが着信した際に、DLSw+ ルータでは対応するデバッグを観察できます。

ネットワーク図

このセクションでは、次のダイアグラムに示されるネットワーク構成を使用しています。



このネットワーク ダイアグラムでは、データセンター ルータ (Sao Paulo) がメインフレームに接続されて示されています。 このルータは、すべてのリモート ブランチからの複数の DLSw+ ピア接続を受けています。 各リモート ブランチには Systems Network Architecture (SNA; システム ネットワーク アーキテクチャ) クライアントと NetBIOS クライアントの両方があります。 データセンターには、リモート オフィスからアクセスされる必要がある NetBIOS サーバがありません。

分かりやすくするため、1 つのリモート オフィス (Caracas) のみの設定の詳細が示されています。 また、このネットワーク ダイアグラムには、front-end processor (FEP; フロントエンド プロセッサ)、および CCSpcC と呼ばれるリモート PC の MAC アドレス値も示されています。 MAC アドレスは、標準 (イーサネット) と非標準 (トークン リング) の両方の形式で示されています。

リモート オフィスでの LSAP 出力アクセス リストの設定

この方式を使用すると、すべてのリモート オフィスは **lsap-output-list** オプションを使用して設定する必要があります。 中央ルータではその他の設定変更は必要ありません。

lsap-output-list は、SAP アクセス リスト (SAP ACL) にリンクしています。このアクセス リストは現在 SNA SAP (0x00、0x04、0x08 など) が中央ルータに向かうことのみを許可し、その他すべてを拒否します。 SAP に基づいてフィルタリングを実行する方法についての詳細は、『サービス アクセス ポイントのアクセス コントロール リストについて』を参照してください。

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	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

```
no ip directed-broadcast !
access-list 200 permit 0x0000
0x0D0D access-list 200 deny
0x0000 0xFFFF ! 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
```

Caracas ルータが NetBIOS トラフィックを受信したときにどのように反応するかを確認するには、**debug dlsw** コマンドを使用します。

```
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
```

リモート オフィス ルータ（Caracas）が 4000.3745.0000 の到達可能性情報を持っておらず、また一部の「禁止された」SAP を使用してその MAC アドレスを検索する探索を行った場合、その要求はブロックされます。

```
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
```

リモート オフィス ルータ（Caracas）が 4000.3745.0000 に関する到達可能性情報を持っている場合を考えます。 たとえば、（許可された SAP を使用する）別のステーションがすでに FEP MAC アドレスを問い合せているとします。 この場合、「攻撃者」PC（CCSpcC）は NULL XID を送信しますが、ルータはそれを阻止します。

```
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
```

中央ルータでの dlsw icannotreach saps の設定

dlsw icannotreach saps コマンドを使用すると、送信が禁止されていることが判明しているプロトコルをフィルタリングできます。 明示的に拒否する必要があるものだけが判明している場合は、次の設定に示すように、中央ルータで **dlsw icannotreach saps** コマンドを使用します。

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

リモート ピアがすでにアップしている場合であっても、ただちに中央ルータを設定（**dlsw icannotreach saps** コマンドを含める）できます。 この出力にはリモート ルータの一方でのデバッグが示されており、CapExId メッセージの受信が示されています。 次のメッセージは、SAP 0xF0/F1 によるフレームを中央ルータに送信しないように、リモート オフィスに指示しています。

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 メッセージが受信されると、Caracas ルータは Sao Paulo が SAP 0xF0 をサポートしていないことを学習します。

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.

次に示す **show** コマンドの出力は中央ルータで取得されたもので、SAP 0xF0 がサポートされていない設定変更を示しています。

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.
```

次に示すのは、NetBIOS PC ステーションが接続を試みた際の Caracas ルータからの **debug** の出力です。

```
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
```

中央ルータでの dlsw icanreach saps の設定

どの種類のトラフィックが許可されているかが正確に判明していて、その他すべてのトラフィックが確実に拒否されるようにする場合は、**dlsw icanreach saps** コマンドを設定すると便利です。たとえば、**dlsw icanreach saps 4** を設定すると、0x04（および応答である 0x05）を除くすべての SAP を明示的に拒否します。

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

この **show** コマンドの出力では、Caracas ルータは、Sao Paulo が SAP 0x04 および 0x05 が宛先であるフレームのみをサポートしていることを認識しています。 他のすべての SAP はサポートされていません。

```
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 コマンドを使用すると、中央ルータでの設定変更が DLSw+ コードで表示されることを確認できます。

```
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 のフィルタリング方式

このドキュメントに示すネットワーク ダイアグラムを使用して、FEP MAC アドレス（4000.3745.0000）が宛先であるフレームのみを中央ルータが受信するようにします。

中央ルータでの dlsw icanreach mac-address の設定

dlsw icanreach mac-address コマンドを使用すると、すべてのリモート オフィスは、中央ルータの IP アドレスを指定するホスト MAC アドレスについて、DLSw+ 到達可能性テーブルにエントリを持つことになります。 このエントリは UNCONFIRM 状態で、リモート オフィス ルータがホストのローカル テストまたは XID を受信した場合、中央ルータのみに CUR_ex（Can U Reach Explorer）メッセージを送信することを示します。

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	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

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	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

ここでは、Caracas ルータは到達可能性キャッシュに永続的なエントリを作成しています。 このエントリがフレッシュでない場合、状態は UNCONFIRM です。 DLSw+ ルータが MAC アドレスと NetBIOS 名をキャッシュする方法についての詳細は、『DLSw+ トラブルシューティング ガイドの到達可能性』の章を参照してください。

```
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 ルータ上の **show dlsw capabilities** コマンドの出力により、MAC アドレス 4000.3745.0000 がピア 1.1.1.1 を介して到達可能であることがリモート オフィスで認識されていることが確認できます。 また「icanreach mac-exclusive を言う行に注意して下さい: いいえ」。これは、中央ルータはホスト以外のその他の MAC アドレスに到達できることを示しています。 そのため、リモート オフィスのいずれかが他の MAC アドレスを探す際には、要求を中央ルータに送信できます。 ただし、**icanreach mac-address 4000.3745.0000** コマンドを含めることにより、この重要なリソースのリケーションがすべてのリモート ブランチで認識されます。 中央ルータに着信するフレームをさらに制限する場合は、「中央ルータでの dlsw icanreach mac-exclusive の設定」を参照してください。

```
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.
```

mask パラメータは **dlsw icanreach mac-address 4000.3745.0000** ***mask ffff.ffff.ffff*** のように使用できます。 このパラメータを使用する場合、MAC アドレスは通常 16 進数形式（0x4000.3745.0000）で表示されることに注意してください。 そのため、バイナリ形式ですべてが 1 のマスクは 16 進数 0xFFFF.FFFF.FFFF で表現されます。

次に、特定の入力 MAC が、すでに設定されている **dlsw icanreach mac-address** コマンドの下に含まれているかどうかを判断する方法の例を示します。

1. **dlsw icanreach mac-address 4000.3745.0000 mask ffff.ffff** 0000 コマンドを使用して設定されているルータから始めます。
2. 入力 MAC アドレス 4000.3745.0009 が前述のルータ設定コマンドに含まれているかどうかを評価します。
3. まず、MAC アドレス（4000.3745.0009）および設定済みの MASK（FFFF.FFFF.0000）を 16 進数からバイナリ表現に変換します。 次の表の最初の 2 つの行にこの手順を示します。

4. 続いて、これら 2 つのバイナリ数値の間で論理 AND 演算を実行し、結果を 16 進数表現（4000.3745.0000）に変換します。 この演算の結果を、次の表の 3 行目に示します。
5. AND 演算の結果が **dlsw icanreach mac-address** コマンドの MAC アドレス（この例では 4000.3745.0000）に一致する場合、入力 MAC アドレス（4000.3745.0009）は **dlsw icanreach mac-address** コマンドにより許可されます。 この例では、4000.3745.0000 ~ 4000.3745.FFFF の範囲内のすべての入力 MAC アドレスは **dlsw icanreach mac-address** コマンドに含まれます。 この範囲のすべての MAC アドレスに対して同じ手順を繰り返すことで、このことを確認できます。

さらに例を示します。

- **dlsw icanreach mac-address 4000.3745.0000 マスク ffff.ffff.ffff —このコマンドは** MAC アドレス 4000.3745.0000 だけが含まれています。 その他の MAC アドレスはこのマスクをパスします。
- **dlsw icanreach mac-address 4000.0000.3745 マスク ffff.0000.ffff** —このコマンドはが 0x0000-0xFFFF である範囲ですべての MAC アドレスが含まれています。

中央ルータでの dlsw icanreach mac-exclusive の設定

中央ルータで **dlsw icanreach mac-exclusive** コマンドを設定すると、前もって定義済みの MAC アドレス（この場合は 4000.3745.0000）が宛先になっているパケットのみがセントラル ロケーションで許可されるようになります。

このフィルタリング情報は、CapExId メッセージを使用してすべての DLSw+ ピア間で交換されることに注意してください。 WAN 帯域幅を節約するには、リモート ルータ自体で（フレームのブロックなどの）アクションが発生する場合であっても、セントラル ロケーションでフィルタリング情報を設定します。

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 mac-exclusive dlsw icanreach mac-address 4000.3745.0000 mask ffff.ffff.ffff**f ! 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

この出力では、Caracas ルータは、MAC アドレス 4000.3745.0000 がピア 1.1.1.1 を介して到達可能であることを認識していることが観察されます。 この例と上記のシナリオの違いはここに「icanreach mac-exclusive を示すことです: リモートオフィスがそれら以外 4000.3745.0000 に向かうセントラルルータの方に帯を送信 しないことをはい」、つまり意味します。

```
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.
```

ここで **debug** 出力には、4000.3745.0000 以外の任意の MAC アドレス (ここでは 4000.3745.0080 を使用) が宛先である着信トラフィックに対して、Caracas ルータがどのように反応しているかが示されています。 Caracas では、ホスト (4000.3745.0000) が宛先ではないフレームに関しては Sao Paulo が使用されません。 この場合、Sao Paulo は Caracas で設定されている唯一のリモート ピアであるため、このルータにはフレームを送信先するその他のピアはありません。

```
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 コマンドを使用して MAC アドレスを定義することなく、**dlsw icanreach mac-exclusive** コマンドを使用してルータを設定した場合、ルータからピアに、到達できる MAC アドレスがまったくないことがアドバタイズされます。 そのため、そのピアを介した通信が失われることになります。

注: ここでの設定例は例としてのみ示されています。 これには誤りがあるため、**使用しないでください**。

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
```

debug の出力には、4000.3745.0000 が宛先であるフレームを Caracas ルータが受信した際に Caracas ルータで何が起こるかが示されています。 Caracas の DLSw リモートピアは 1 つ (Sao Paulo) だけですが、前述の設定では Sao Paulo からピアにどの MAC アドレスにも到達できないことが示されていたことに注意してください。

```
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
```

リモート ルータでの dlsw mac-address の設定

この例では、各リモート オフィス ルータは手動で設定され、特定の MAC アドレスを検索する際には目的の中央ルータにダイレクトされます。 これにより、正しくないピアに向かう不必要なトラフィックが減ります。 リモート オフィスで 1 つのリモート ピアのみが設定されている場合、この設定に利点はありません。 ただし、複数のリモート ピアが設定されている場合、この設定は WAN 帯域幅を浪費することなく、リモート サイト ルータを正しい場所に導きます。

新しい 1 つの DLSw+ リモート ピア (2.2.2.1) が Caracas ルータで設定されています。

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

Caracas ルータの空の到達可能性テーブルから始めて、FEP のエントリが UNCONFIRM 状態であることに注意してください。

```
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
```

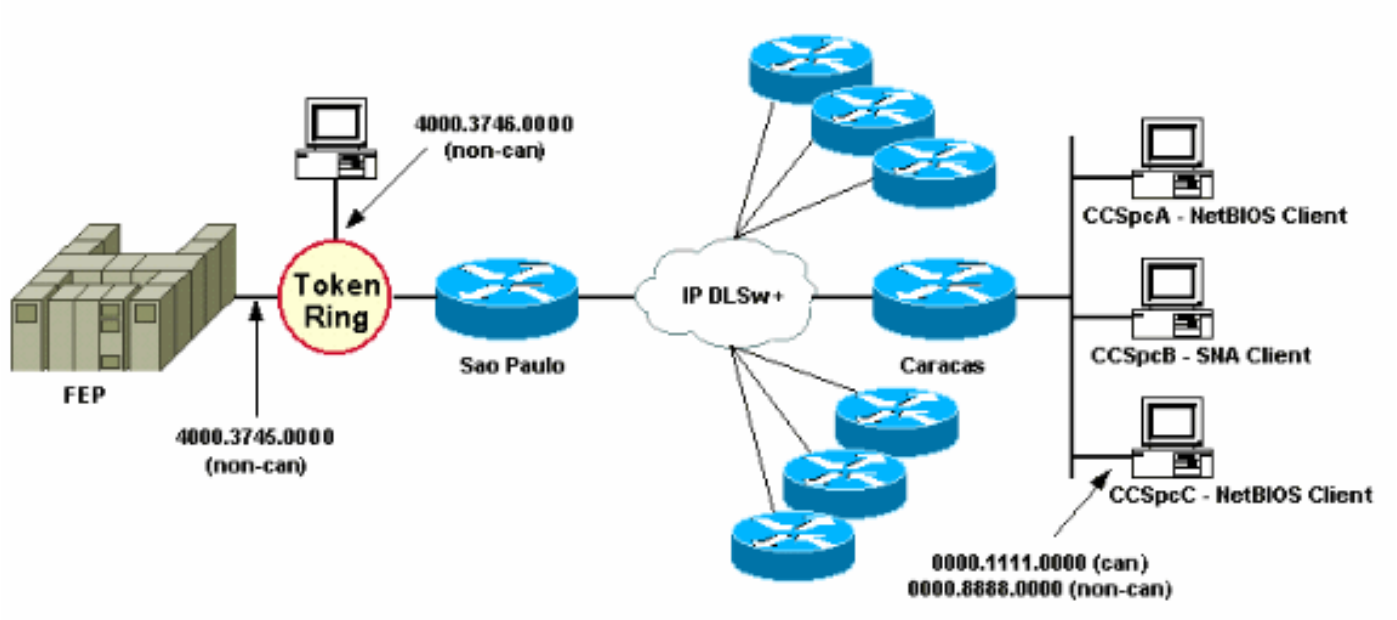
FEP を探して最初のパケットが着信すると、2.2.2.1 ではなくピア 1.1.1.1 (Sao Paulo) へのパケットのみが送信されます。 そのため、その他のピアでの WAN 帯域幅と CPU リソースが節約さ

れます。

```
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
```

中央ルータでの dlsw icanreach mac-exclusive remote の設定

ここでは、ネットワーク ダイアグラムと設計要件が変更されます。 次に新しいネットワークの例を示します。



この例では、新しい SNA デバイス (4000.3746.0000) が Sao Paulo ロケーションに追加されています。 このマシンは、別の ロケーションにあるデバイス (ピア 3.3.3.1) と通信を確立する必要があります。 Sao Paulo ルータでは、次の設定が実行されます。

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

この Sao Paulo の設定では、**mac-exclusive** コマンドにより MAC アドレス 4000.3745.0000 のみに到達できることが、Sao Paulo ルータからすべてのピアに通知されます。 次の **debug** 出力に示されているように、このことにより新しい SNA デバイス (4000.3746.0000) は DLSw+ を介して通信を確立することもできなくなります。

```
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
```

これを修正するには、Sao Paulo の設定に次の変更を加えます。

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
```

remote キーワードを使用すると、中央ルータのその他のデバイスは発信接続を行うことができます（これは dlsw icanreach mac-address コマンドでは指定されていません）。 次は、デバイス 4000.3746.0000 が接続を開始した時点での Sao Paulo の debug 出力です。

```
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
```

関連情報

- DLSw に関するサポート ページ
- DLSw+ 設計ガイド
- DLSw+ トラブルシューティング ガイド
- サービス アクセス ポイントのアクセス コントロール リストについて