Techniques de filtrage SAP/MAC avec DLSw+

Contenu

Introduction

Ce document fournit des configurations d'échantillon pour des techniques de point d'accès services (SAP) et de filtrage MAC de Data-Link Switching Plus (DLSw+).

Le filtrage peut être utilisé pour améliorer l'évolutivité d'un réseau DLSw+. Par exemple, vous pouvez utiliser le filtrage à :

- Réduisez le trafic à travers un lien WAN (particulièrement important sur très des liaisons à bas débit et dans les environnements avec Netbios).
- Améliorez la Sécurité d'un réseau en contrôlant l'accès à certains périphériques.
- Améliorez la performance du CPU et l'évolutivité des Routeurs du centre de données DLSw+.

DLSw+ offre plusieurs options qui peuvent être utilisées pour exécuter le filtrage. Le filtrage peut être fait sur des adresses MAC, SAP, ou des noms NetBIOS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez pour des techniques de filtrage DLSw+ SAP

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Utilisant la topologie du réseau représentée dans la section de schéma de réseau, la condition requise est d'arrêter tout le trafic de Netbios aux sites distants d'atteindre le routeur central (Sao Paulo). DLSw+ offre plusieurs options d'accomplir cette tâche, qui sont analysées dans les sections suivantes.

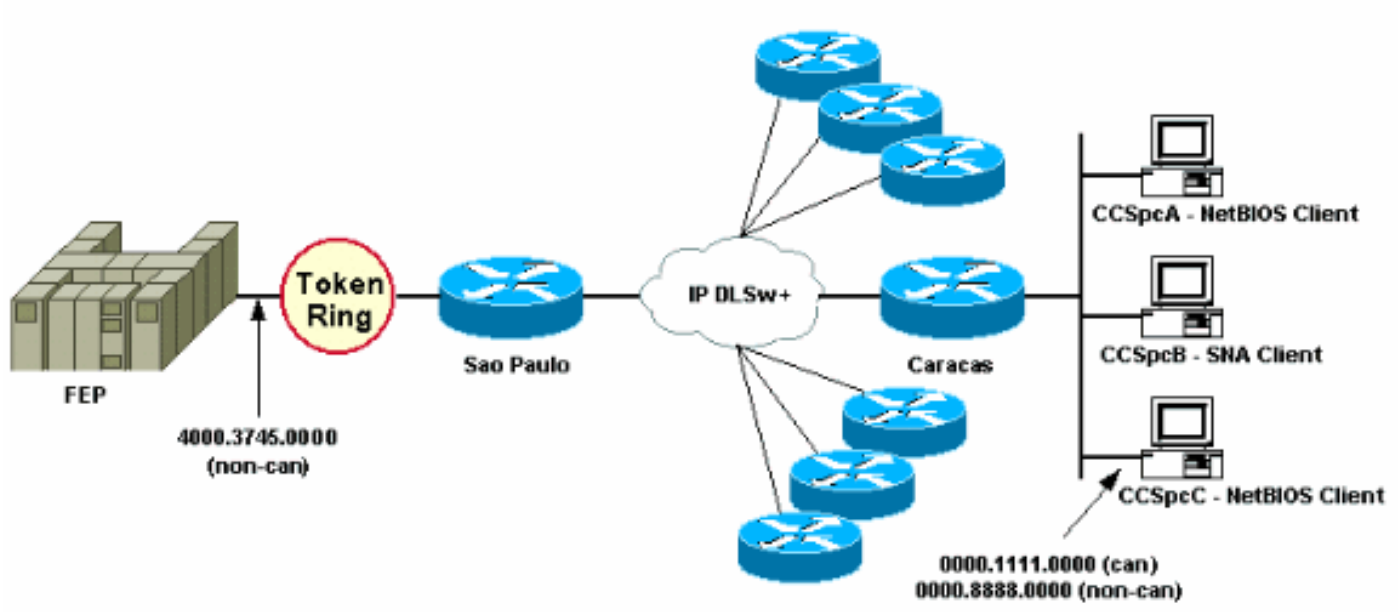
Remarque: Le trafic de Netbios utilise les valeurs de SAP 0xF0 (pour des commandes) et 0xF1 (pour des réponses). Typiquement, les administrateurs réseau emploient les valeurs mentionnées ci-dessus de SAP pour filtrer (recevez ou refusez) ce protocole.

Remarque: Les clients de Netbios utilisent l'adresse MAC fonctionnelle de Netbios (C000.0000.0080) comme MAC de destination (DMAC) sur leurs paquets de requête de nom NetBIOS. Comme cité précédemment, toutes les trames ont des valeurs de SAP de 0xF0 ou de 0xF1.

Pour ce test, le PC de CCSpcC est configuré pour se connecter à l'adresse MAC du FEP utilisant SAP 0xF0. En réalité ce trafic regarde les mêmes que Netbios, au moins d'un point de vue de SAP. Par conséquent, vous pouvez observer que la correspondance met au point dans le routeur DLSw+ quand ce trafic arrive.

Diagramme du réseau

Cette section utilise la configuration réseau affichée dans ce diagramme.



Dans le schéma de réseau, un routeur du centre de calcul (Sao Paulo) est dépeint avec une connexion au mainframe. Ce routeur reçoit de plusieurs connexions homologues DLSw+ de toutes les filiales distantes. Chaque filiale distante a des clients du Systems Network Architecture (SNA) et du Netbios. Il n'y a aucun serveur de Netbios au centre de traitement des données qui doit obtenir accédé à des bureaux distants.

Pour la simplicité, les détails de configuration de seulement un bureau distant (Caracas) sont affichés. Le schéma de réseau affiche également la valeur d'adresse MAC du processeur frontal (FEP) et de l'ordinateur distant appelé CCSpcC. Des adresses MAC sont affichées dans le format canonique (des Ethernets) et non-canonique (d'Anneau à jeton).

Configurez les listes d'accès de sortie de LSAP aux bureaux distants

Suivre cette méthode, tous les bureaux distants doivent être configurés avec l'option de lsap-sortie-**liste**. Aucun autre changement de configuration n'est exigé du routeur central.

La lsap-sortie-liste lie à SAP une liste d'accès (ACL de SAP) qui permet actuellement seulement à des sèves SNA (par exemple, 0x00, 0x04, 0x08, et ainsi de suite) pour aller vers le routeur central, et refuse tout autrement. Référez-vous compréhension derrière des listes de contrôle d'accès de point d'accès services pour plus d'informations sur la façon exécuter le filtrage basé sur des sèves.

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 !	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

access-list 200 permit 0x0000 0x0D0D access-list 200 deny 0x0000 0xFFFF ! bridge 1 protocol ieee ! end	! interface Serial1/0 ip address 1.1.1.1 255.255.255.0 no ip directed-broadcast no ip mroute-cache clockrate 32000 ! end

La commande de **debug dlsw** est utilisée de voir comment le routeur Caracas réagit quand elle reçoit le trafic de Netbios.

```
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
```

Si le routeur du bureau distant (Caracas) n'a pas les informations d'accessibilité pour 4000.3745.0000, et elles obtient un explorateur qui recherche que l'adresse MAC utilisant une partie de « a interdit » des sèves, alors la demande est bloquée.

```
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
```

Considérez le cas où le routeur du bureau distant (Caracas) a les informations d'accessibilité pour 4000.3745.0000. Par exemple, une autre station (utilisant les sèves permises) a déjà demandé l'adresse MAC FEP. Dans cette situation que le PC de « contrevenant » (CCSpcC) envoie son XID NULL, mais le routeur l'arrête.

```
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
```

Configurez le dlsw icannotreach saps au routeur central

Utilisant le **dlsw icannotreach saps la** commande te permet pour filtrer ces protocoles on ne vous laisse pas que savez être envoyé à travers. Si vous connaissez seulement ce qui doit être explicitement refusé, utilisez la commande de **dlsw icannotreach saps** sur les routeurs centraux, suivant les indications de ces 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

Vous pouvez configurer le routeur central (incluez la commande de **dlsw icannotreach saps**) à la volée, même lorsque les pairs distants sont déjà. Cette sortie affiche le débogage sur un des Routeurs distants, qui indique la réception du message de CapExId. Ce message demande aux bureaux distants pour n'envoyer aucune trame avec SAP 0xF0/F1 vers le routeur central.

```
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
```

Après que le message de CapExId soit reçu, le routeur Caracas apprend que Sao Paulo ne prend en charge pas 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.
```

La sortie de commande show affichée ici, pris au routeur central, affiche à la modification de configuration où SAP 0xF0 n'est pas pris en charge.

```
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.
```

C'est la **sortie de débogage du** routeur Caracas quand la station PC de Netbios tente la connexion :

```
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
```

Configurez les sèves de dlsw icanreach au routeur central

Configurer la commande de **sèves de dlsw icanreach** est utile quand vous connaissez qu'exactement ce que le type de trafic est permis et vous voulez s'assurer que tout autre trafic est refusé. Par exemple, quand vous configurez les **sèves 4 de dlsw icanreach**, vous refusez explicitement toutes les sèves excepté 0x04 (et 0x05, la réponse).

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 dans cette **sortie de commande show** que le routeur Caracas identifie que Sao Paulo prend en charge seulement des trames destinées aux sèves 0x04 et 0x05. Toutes autres sèves sont sans support.

```
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.
```

Vous pouvez utiliser la commande **locale de show dlsw capabilities** de vérifier que les modifications de configuration au routeur central apparaissent dans le code DLSw+.

```
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.
```

Techniques de filtrage MAC DLSw+

Utilisant le schéma de réseau affiché dans ce document, incitez le routeur central à recevoir des trames destinées à l'adresse MAC FEP (4000.3745.0000) seulement.

Configurez le mac-address de dlsw icanreach au routeur central

Utilisant la commande de **mac-address de dlsw icanreach**, tous les bureaux distants ont une entrée sur leur table d'accessibilité DLSw+ pour l'adresse MAC d'hôte ces points à l'adresse IP du routeur centrale. Cette entrée est dans l'état UNCONFIRM, qui indique que si le routeur du bureau distant reçoit un test local ou un XID pour l'hôte, il envoie un message de CUR_ex (peut l'explorateur de portée U) au routeur central seulement.

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.fff**f ! interface TokenRing0/0 no ip directed-broadcast ring-speed 16 source-bridge 10 1 3 source-bridge spanning ! interface Serial1/0 ip

! interface Serial0/1 ip address 1.1.1.2 255.255.255.0 no ip directed- broadcast ! bridge 1 protocol ieee ! end	address 1.1.1.1 255.255.255.0 no ip directed-broadcast no ip mroute-cache clockrate 32000 ! end

Ici, le routeur Caracas a créé une entrée permanente dans son cache d'accessibilité. Si l'entrée n'est pas fraîche, l'état est UNCONFIRM. Référez-vous au chapitre Accessibilité de guide de dépannage DLSw+ pour plus d'informations sur la façon dont les Routeurs DLSw+ cachent des adresses MAC et des noms NetBIOS.

```
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
```

La sortie de la commande de **show dlsw capabilities** sur le routeur Caracas confirme que ce bureau distant sait que l'adresse MAC 4000.3745.0000 est accessible par l'intermédiaire du pair 1.1.1.1. Notez également la ligne qui indique la « MAC-exclusivité d'icanreach : non ». Il indique que le routeur central est capable d'atteindre d'autres adresses MAC sans compter que l'hôte. Par conséquent, si les bureaux distants l'uns des recherchent l'autre adresse MAC, ils peuvent envoyer leurs demandes au routeur central. Cependant, avec l'intégration de la commande du **mac-address 4000.3745.0000 d'icanreach**, toutes les filiales distantes se rendent compte de l'emplacement de cette importante ressource. Si vous voulez imposer d'autres restrictions à quelles trames arrivent au routeur central, référez-vous configurent la MAC-exclusivité de dlsw icanreach au routeur central.

```
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.
```

Vous pouvez utiliser le paramètre de **masque** en tant que *masque ffff.ffff.ffff du* **mac-address 4000.3745.0000 de dlsw icanreach**. *Quand vous utilisez* ce paramètre, notez que des adresses MAC sont typiquement présentées dans le format hexadécimal (0x4000.3745.0000). Par conséquent des tout-ceux masquent (dans la binaire) est représentés par le nombre hexadécimal 0xFFFF.FFFF.FFFF.

Voici un exemple de la façon déterminer si un MAC particulier d'entrée est inclus sous une commande déjà configurée de **mac-address de dlsw icanreach** :

1. Début avec un routeur configuré avec la commande du **masque ffff.ffff 0000 du mac-address 4000.3745.0000 de dlsw icanreach**.
2. Évaluez si l'adresse MAC 4000.3745.0009 d'entrée est incluse par la commande de configuration de routeur précédente.

3. D'abord, convertissez l'adresse MAC (4000.3745.0009) et le MASQUE configuré (FFFF.FFFF.0000) de l'hexadécimal à la représentation binaire. Les deux premières lignes dans cette table affichent cette étape.
4. Puis, exécutez un logique ET une exécution entre ces deux nombres binaire, et convertissez le résultat en représentation hexadécimale (4000.3745.0000). Le résultat de cette exécution est dépeint dans la troisième ligne de cette table.
5. Si le résultat du ET de l'exécution apparie l'adresse MAC dans la commande de **mac-address de dlsw icanreach** (dans notre exemple, 4000.3745.0000), alors on permet l'adresse MAC d'entrée (4000.3745.0009) par la commande de **mac-address de dlsw icanreach**. Dans notre exemple, n'importe quelle adresse MAC d'entrée dans la marge 4000.3745.0000 à 4000.3745.FFFF est incluse par la commande de **mac-address de dlsw icanreach**. Vous pouvez vérifier ceci en répétant les mêmes étapes pour toutes les adresses MAC dans cette plage.

Ce sont quelques plus d'exemples :

- **masque ffff.ffff.ffff du mac-address 4000.3745.0000 de dlsw icanreach — Cette commande** inclut seulement l'adresse MAC 4000.3745.0000. Autre adresse MAC ne passe pas ce masque.
- **masque ffff.0000.ffff du mac-address 4000.0000.3745 de dlsw icanreach** — Cette commande inclut toutes les adresses MAC dans la plage où est 0x0000-0xFFFF.

Configurez la MAC-exclusivité de dlsw icanreach au routeur central

La commande de MAC-**exclusivité de dlsw icanreach** étant configuré au routeur central, vous vous assurez qu'on permet seulement des paquets destinés aux adresses MAC précédemment définies (dans ce cas 4000.3745.0000) au site central.

Notez que ces informations de filtrage sont permutées entre tous les pairs DLSw+ utilisant des messages de CapExId. Vous sauvegardez la bande passante BLÊME en configurant les informations de filtrage au site central, quoique les actions (telles que bloquer des trames) se produisent aux Routeurs distants eux-mêmes.

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-	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

broadcast ! bridge 1 protocol ieee ! end	

Observez dans cette sortie que le routeur Caracas sait que l'adresse MAC 4000.3745.0000 est accessible par l'intermédiaire du pair 1.1.1.1. La différence entre cet exemple et le scénario précédent est qu'ici nous affichons la « MAC-exclusivité d'icanreach : oui », ainsi il signifie que les bureaux distants n'envoient pas des trames vers le routeur central autre que ceux destiné pour 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.
```

La sortie de débogage ici affiche comment le routeur Caracas réagit au trafic entrant destiné à n'importe quelle adresse MAC autre que 4000.3745.0000 (4000.3745.0080 est utilisés ici). Caracas n'utilise pas Sao Paulo des trames non destinées à l'hôte (4000.3745.0000). Dans ce cas, Sao Paulo est le seul pair distant configuré à Caracas, ainsi ce routeur n'a aucun autre pair auquel pour l'envoyer.

```
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
```

Si vous configurez un routeur avec la commande de MAC-exclusivité de dlsw icanreach sans définir n'importe quelle adresse MAC utilisant la commande de mac-address de dlsw icanreach, le routeur annonce à ses pairs qu'elle peut n'atteindre aucune adresse MAC du tout. Par conséquent vous perdrez la transmission par ce pair.

Remarque: La configuration d'échantillon ici est affichée seulement comme exemple. C'est une erreur et ne devrait pas être utilisé.

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
```

Cette **sortie de débogage** indique ce qui se produit au routeur Caracas quand il reçoit une trame destinée à 4000.3745.0000. Notez que Caracas a seulement un distant-pair de DLSw (Sao Paulo), mais dans la configuration précédente, Sao Paulo a indiqué à ses pairs qu'il ne peut atteindre aucune adresses MAC.

```
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
```

Configurez le dlsw mac-address aux Routeurs distants

Dans cet exemple, chaque routeur du bureau distant est manuellement configuré et dirigé vers le routeur central désiré en recherchant les adresses MAC spécifiques. Ceci réduit le trafic inutile qui va au pair faux. Si le bureau distant a seulement un pair distant configuré, alors cette configuration n'est pas salutaire. Cependant, si des plusieurs homologues distants sont configurés, cette configuration dirige le routeur du site distant vers le bon endroit sans gaspiller la bande passante BLÊME.

Un nouveau pair distant DLSw+ (2.2.2.1) est configuré au routeur Caracas.

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

En commençant par une table d'accessibilité vide au routeur Caracas, notez que l'entrée pour le

FEP est dans l'état UNCONFIRM :

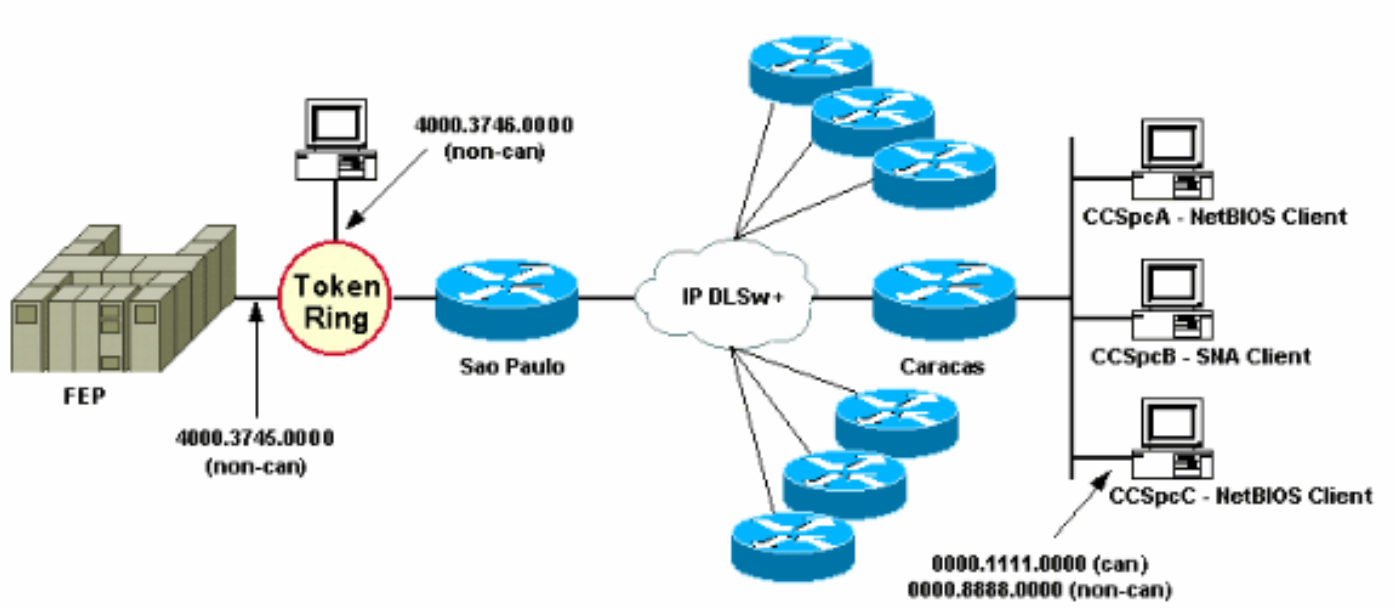
```
CARACAS#show dlsw reachability DLSw Local MAC address reachability cache list Mac Addr status
Loc. port rif DLSw Remote MAC address reachability cache list Mac Addr status Loc. peer
4000.3745.0000 UNCONFIRM REMOTE 1.1.1.1(2065) max-lf(4472) DLSw Local NetBIOS Name reachability
cache list NetBIOS Name status Loc. port rif DLSw Remote NetBIOS Name reachability cache list
NetBIOS Name status Loc. peer
```

Quand le premier paquet arrive recherchant le FEP, seulement les paquets à scruter 1.1.1.1 (Sao Paulo) sont envoyés et pas à 2.2.2.1. Par conséquent, vous économisez la bande passante BLÊME et les ressources CPU sur les autres pairs.

```
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
```

Configurez le distant de MAC-exclusivité de dlsw icanreach au routeur central

En ce moment, le schéma de réseau et les conditions requises de conception sont changés. C'est le nouvel exemple de réseau :



Dans cet exemple, une nouvelle unité SNA (4000.3746.0000) est ajoutée à l'emplacement de Sao Paulo. Cet ordinateur doit établir la transmission avec un périphérique à un autre emplacement (pair 3.3.3.1). Le routeur de Sao Paulo exécute cette 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
```

Avec cette configuration de Sao Paulo, le routeur de Sao Paulo informe tous ses pairs que, dus à la commande de MAC-**exclusivité**, elle peut seulement atteindre l'adresse MAC 4000.3745.0000. Suivant les indications de cette **sortie de débogage**, ceci empêche également la nouvelle unité SNA (4000.3746.0000) d'établir la transmission par 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
```

Pour réparer ceci, apportez ces modifications à la configuration de Sao Paulo.

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
```

Avec le mot clé **distant**, on permet à d'autres périphériques au routeur central (qui ne sont pas spécifiés dans la commande de **mac-address de dlsw icanreach**) pour établir les rapports sortants. C'est la **sortie de débogage** sur Sao Paulo quand le périphérique 4000.3746.0000 a commencé sa connexion.

```
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
```

Informations connexes

- Page de support de DLSw
- Guide de conception DLSw+
- Guide de dépannage DLSw+
- Présentation des listes de contrôle d'accès SAP (Service Access Point)