Techniques de filtrage SAP/MAC avec DLSw+

Contenu

Introduction

Ce document fournit des exemples de configuration pour la commutation de liaison de données plus (DLSw+) le point d'accès au service (SAP) et les techniques de filtrage MAC.

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

- Réduire le trafic sur une liaison WAN (particulièrement important sur les liaisons à très faible débit et dans les environnements avec NetBIOS).
- Améliorez la sécurité d'un réseau en contrôlant l'accès à certains périphériques.
- Améliorez les performances du processeur et l'évolutivité des routeurs DLSw+ du data center.

DLSw+ offre plusieurs options qui peuvent être utilisées pour effectuer le filtrage. Le filtrage peut être effectué sur les adresses MAC, les noms SAP ou NetBIOS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

Conventions

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

Configuration pour les techniques de filtrage SAP DLSw+

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

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez l'outil de recherche de commandes (clients inscrits seulement).

Àl'aide de la topologie du réseau décrite dans la section Schéma du réseau, vous devez empêcher tout trafic NetBIOS sur des sites distants d'atteindre le routeur central (Sao Paulo). DLSw+ offre plusieurs options pour accomplir cette tâche, qui sont analysées dans les sections suivantes.

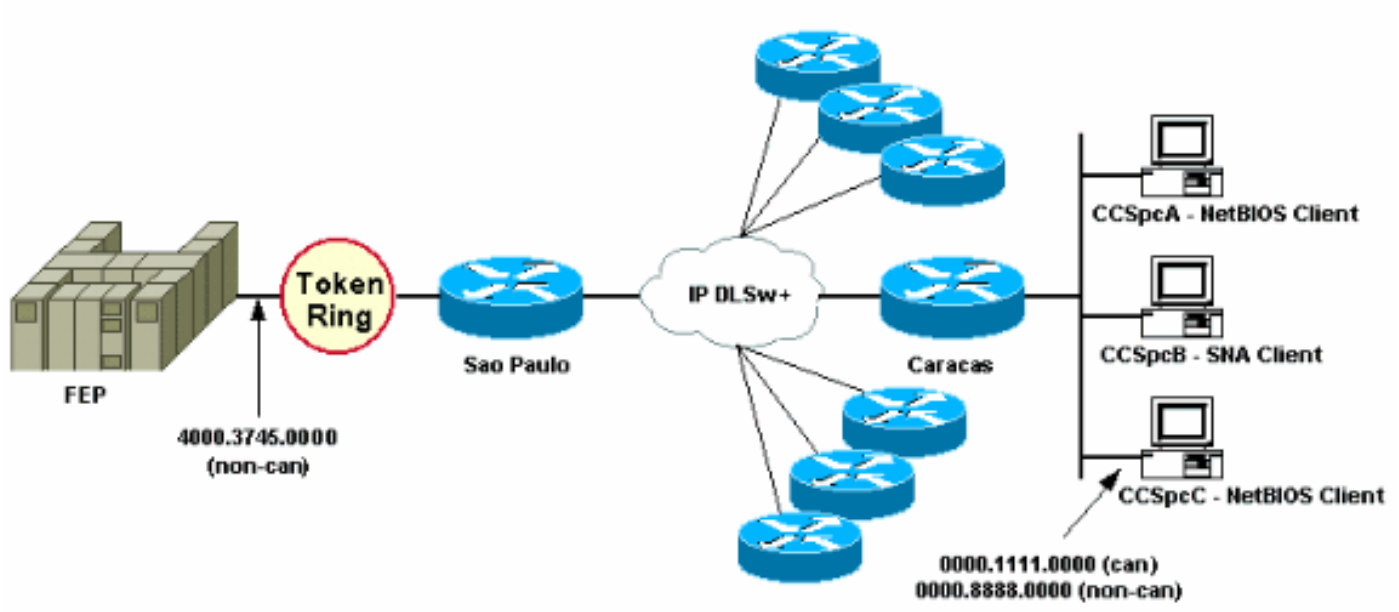
Remarque : le trafic NetBIOS utilise les valeurs SAP 0xF0 (pour les commandes) et 0xF1 (pour les réponses). En règle générale, les administrateurs réseau utilisent les valeurs SAP mentionnées ci-dessus pour filtrer (accepter ou refuser) ce protocole.

Remarque : les clients NetBIOS utilisent l'adresse MAC fonctionnelle NetBIOS (C000.000.0080) comme adresse MAC de destination (DMAC) sur leurs paquets de requête de nom NetBIOS. Comme mentionné précédemment, toutes les trames ont des valeurs SAP de 0xF0 ou 0xF1.

Pour ce test, le PC CCSpcC est configuré pour se connecter à l'adresse MAC du FEP à l'aide de SAP 0xF0. En réalité, ce trafic ressemble à NetBIOS, du moins du point de vue de SAP. Par conséquent, vous pouvez observer les débogages correspondants dans le routeur DLSw+ lorsque ce trafic arrive.

Diagramme du réseau

Cette section utilise la configuration réseau illustrée dans ce schéma.



Dans le schéma de réseau, un routeur de centre de données (Sao Paulo) est représenté avec une connexion au mainframe. Ce routeur reçoit plusieurs connexions homologues DLSw+ de toutes les filiales distantes. Chaque succursale distante a des clients SNA (Systems Network Architecture) et NetBIOS. Aucun serveur NetBIOS dans le data center n'a besoin d'être accessible depuis les bureaux distants.

Par souci de simplicité, les détails de configuration d'un seul bureau distant (Caracas) sont affichés. Le schéma de réseau indique également la valeur d'adresse MAC du processeur frontal (FEP) et du PC distant appelé CCSpcC. Les adresses MAC sont affichées au format canonique (Ethernet) et non canonique (Token Ring).

Configurer les listes d'accès aux sorties LSAP sur les bureaux distants

Avec cette méthode, tous les bureaux distants doivent être configurés avec l'option **lsap-output-list**. Aucune autre modification de configuration n'est requise dans le routeur central.

La **lsap-output-list** se connecte à une liste de contrôle d'accès SAP (SAP ACL) qui autorise actuellement uniquement les SAP SNA (par exemple, 0x00, 0x04, 0x08, etc.) à se diriger vers le routeur central et refuse tout le reste. Référez-vous à Comprendre les listes de contrôle d'accès aux points d'accès de service pour plus d'informations sur la façon d'effectuer le filtrage basé sur les SAP.

CARACAS	SAO PAULO
Current configuration: ! hostname CARACAS ! dlsw local-peer peer-id 1.1.1.2 dlsw remote-peer 0 tcp 1.1.1.1 **lsap-output-list 200** dlsw bridge-group 1 ! interface Ethernet0/0 no ip directed-broadcast bridge-group 1	Current configuration: ! hostname SAOPAULO ! source-bridge ring-group 3 dlsw local-peer peer-id 1.1.1.1 dlsw remote-peer 0 tcp 1.1.1.2 ! interface TokenRing0/0 no ip directed-broadcast ring-speed 16 source-bridge 10 1 3

```
!
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
```

```
 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
```

La commande **debug dlsw** permet de voir comment le routeur Caracas réagit lorsqu'il reçoit le trafic 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 de bureau distant (Caracas) ne dispose pas d'informations d'accessibilité pour 4000.3745.0000 et qu'il obtient un explorateur qui recherche cette adresse MAC à l'aide de certains SAP « interdits », 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 de bureau distant (Caracas) possède des informations d'accessibilité pour 4000.3745.0000. Par exemple, une autre station (utilisant les SAP autorisés) a déjà demandé l'adresse MAC FEP. Dans ce cas, le PC « délinquant » (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
```

configuration de dlsw icannotreach saps au niveau du routeur central

L'utilisation de la commande **dlsw icannotreach saps** vous permet de filtrer les protocoles que vous savez ne pas être autorisés à traverser. Si vous ne savez que ce qui doit être explicitement refusé, utilisez la commande **dlsw icannotreach saps** sur le ou les routeurs centraux, comme indiqué dans 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 (inclure la commande **dlsw icannotreach saps**) à la volée, même lorsque les homologues distants sont déjà actifs. Ce résultat montre le débogage sur l'un des routeurs distants, qui indique la réception du message CapExId. Ce message indique aux bureaux distants de ne pas envoyer de trames 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
```

Une fois le message CapExId reçu, le routeur Caracas apprend que Sao Paulo ne prend pas en charge 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 la commande **show** affichée ici, prise au niveau du routeur central, montre 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.
```

Voici la sortie **debug** du routeur Caracas lorsque la station PC 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
```

Configurer dlsw icanreach saps au niveau du routeur central

La configuration de la commande **dlsw icanreach saps** est utile lorsque vous savez exactement quel type de trafic est autorisé et que vous voulez vous assurer que tout autre trafic est refusé. Par exemple, lorsque vous configurez **dlsw icanreach saps 4**, vous refusez explicitement tous les sap sauf 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	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 ! bridge 1 protocol ieee ! end	no ip directed-broadcast no ip mroute-cache clockrate 32000 ! end

Notez dans cette sortie de commande **show** que le routeur Caracas reconnaît que Sao Paulo ne prend en charge que les trames destinées aux sap 0x04 et 0x05. Tous les autres sap ne sont pas pris en charge.

```
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 **show dlsw Features local** pour vérifier que les modifications de configuration au niveau du 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+

À l'aide du schéma de réseau présenté dans ce document, faites en sorte que le routeur central reçoive des trames destinées à l'adresse MAC FEP (4000.3745.0000) uniquement.

configuration de dlsw icanreach mac-address au niveau du routeur central

À l'aide de la commande **dlsw icanreach mac-address**, tous les bureaux distants ont une entrée dans leur table d'accessibilité DLSw+ pour l'adresse MAC hôte qui pointe vers l'adresse IP du routeur central. Cette entrée est dans l'état UNCONFIRM, ce qui indique que si le routeur du bureau distant reçoit un test local ou un XID pour l'hôte, il envoie un message CUR_ex (Can U Reach Explorer) au routeur central uniquement.

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	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 !

```
255.255.255.0
 no ip directed-
broadcast
!
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
```

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. Reportez-vous au chapitre Accessibilité du guide de dépannage DLSw+ pour plus d'informations sur la manière dont les routeurs DLSw+ mettent en cache les adresses MAC et les 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 **show dlsw Features** sur le routeur Caracas confirme que ce bureau distant connaît l'adresse MAC 4000.3745.0000 est accessible via l'homologue 1.1.1.1. Notez également la ligne qui dit « icanreach mac-exclusive : non ». Il indique que le routeur central est capable d'atteindre d'autres adresses MAC en dehors de l'hôte. Par conséquent, si un bureau distant recherche une autre adresse MAC, il peut envoyer ses requêtes au routeur central. Cependant, avec l'inclusion de la commande **icanreach mac-address 4000.3745.0000**, toutes les filiales distantes connaissent l'emplacement de cette ressource importante. Si vous voulez imposer des restrictions supplémentaires sur les trames arrivant sur le routeur central, référez-vous à Configurer dlsw icanreach mac-exclusive sur le 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




   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 **mask** en tant que **dlsw icanreach mac-address 4000.3745.0000 *mask ffff.ffff.ffff*** . Lorsque vous utilisez ce paramètre, notez que les adresses MAC sont généralement présentées au format hexadécimal (0x4000.3745.0000). Par conséquent, un masque 1 (en binaire) est représenté par le nombre hexadécimal 0xFFFF.FFFF.FFFF.

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

1. Commencez par un routeur configuré avec la commande **dlsw icanreach mac-address 4000.3745.000 mask ffff.ffff** 0000.
2. Déterminez si l'adresse MAC d'entrée 4000.3745.0009 est incluse dans la commande de configuration précédente du routeur.
3. Tout d'abord, convertissez l'adresse MAC (4000.3745.0009) et le MASK configuré (FFFF.FFFF.0000) de la représentation hexadécimale en représentation binaire. Les deux premières lignes de ce tableau indiquent cette étape.
4. Ensuite, exécutez une opération AND logique entre ces deux nombres binaires et convertissez le résultat en représentation hexadécimale (4000.3745.0000). Le résultat de cette opération est représenté dans la troisième ligne de ce tableau.
5. Si le résultat de l'opération AND correspond à l'adresse MAC dans la commande **dlsw icanreach mac-address** (dans notre exemple, 4000.3745.0000), alors l'adresse MAC d'entrée (4000.3745.0009) est autorisée par le **dsdldsdsldsdsdsdsdsc w icanreach mac-address**. Dans notre exemple, toute adresse MAC d'entrée comprise entre 4000.3745.000 et 4000.3745.FFFF est incluse par la commande **dlsw icanreach mac-address**. Vous pouvez le vérifier en répétant les mêmes étapes pour toutes les adresses MAC de cette plage.

Voici quelques exemples supplémentaires :

- **dlsw icanreach mac-address 4000.3745.000 mask ffff.ffff.ffff** : cette commande inclut uniquement l'adresse MAC 4000.3745.0000. Aucune autre adresse MAC ne transmet ce masque.
- **dlsw icanreach mac-address 4000.000.3745 mask ffff.0000.ffff** : cette commande inclut toutes les adresses MAC de la plage 4000.XXXX.3745 où XXXX est 0x0000-0xFX FFF.

Configurez dlsw icanreach mac-exclusive sur le routeur central

Avec la commande **dlsw icanreach mac-exclusive** configurée sur le routeur central, vous assurez

que seuls les paquets destinés aux adresses MAC précédemment définies (dans ce cas 4000.3745.0000) sont autorisés à l'emplacement central.

Notez que ces informations de filtrage sont échangées entre tous les homologues DLSw+ à l'aide de messages CapExId. Vous économisez de la bande passante WAN en configurant les informations de filtrage à l'emplacement central, même si les actions (telles que le blocage des trames) se produisent sur les 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-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

Observez dans ce résultat que le routeur Caracas connaît l’adresse MAC 4000.3745.0000 accessible via l’homologue 1.1.1.1. La différence entre cet exemple et le scénario précédent est que ici nous montrons « icanreach mac-Exclusive : yes », ce qui signifie que les bureaux distants n'envoient pas de trames vers le routeur central, sauf celles destinées à 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
```

```
   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 montre comment le routeur Caracas réagit au trafic entrant destiné à toute adresse MAC autre que 4000.3745.0000 (4000.3745.0080 est utilisé ici). Caracas n'utilise pas Sao Paulo pour les trames non destinées à l'hôte (4000.3745.000). Dans ce cas, Sao Paulo est le seul homologue distant configuré à Caracas, de sorte que ce routeur n'a aucun autre homologue auquel 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 **dlsw icanreach mac-exclusive** sans définir d'adresse MAC à l'aide de la commande **dlsw icanreach mac-address**, le routeur annonce à ses homologues qu'il ne peut atteindre aucune adresse MAC. Par conséquent, vous perdrez la communication via cet homologue.

Remarque : L'exemple de configuration ici n'est présenté qu'à titre d'exemple. C'est une erreur et **ne doit pas être utilisée**.

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 passe au niveau du routeur Caracas lorsqu'il reçoit une trame destinée à 4000.3745.0000. Notez que Caracas n'a qu'un seul homologue DLSw distant (Sao Paulo), mais dans la configuration précédente, Sao Paulo a indiqué à ses homologues qu'il ne peut pas atteindre d'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
```

Configurer dlsw mac-address au niveau des routeurs distants

Dans cet exemple, chaque routeur de bureau distant est configuré manuellement et dirigé vers le routeur central souhaité lors de la recherche d'adresses MAC spécifiques. Cela réduit le trafic inutile qui va au mauvais homologue. Si le bureau distant n'a qu'un homologue distant configuré, cette configuration n'est pas utile. Cependant, si plusieurs homologues distants sont configurés, cette configuration dirige le routeur du site distant vers le bon emplacement sans gaspiller la bande passante WAN.

Un nouvel homologue distant DLSw+ (2.2.2.1) est configuré sur le routeur Caracas.

CARACAS	SAO PAULO
Current configuration:	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
```

```
!
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
```

Àpartir d'une table d'accessibilité vide au niveau du routeur Caracas, notez que l'entrée du 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
```

Lorsque le premier paquet arrive à la recherche de FEP, seuls les paquets vers l'homologue 1.1.1.1 (Sao Paulo) sont envoyés et non vers 2.2.2.1. Par conséquent, vous économisez de la bande passante WAN et des ressources CPU sur les autres homologues.

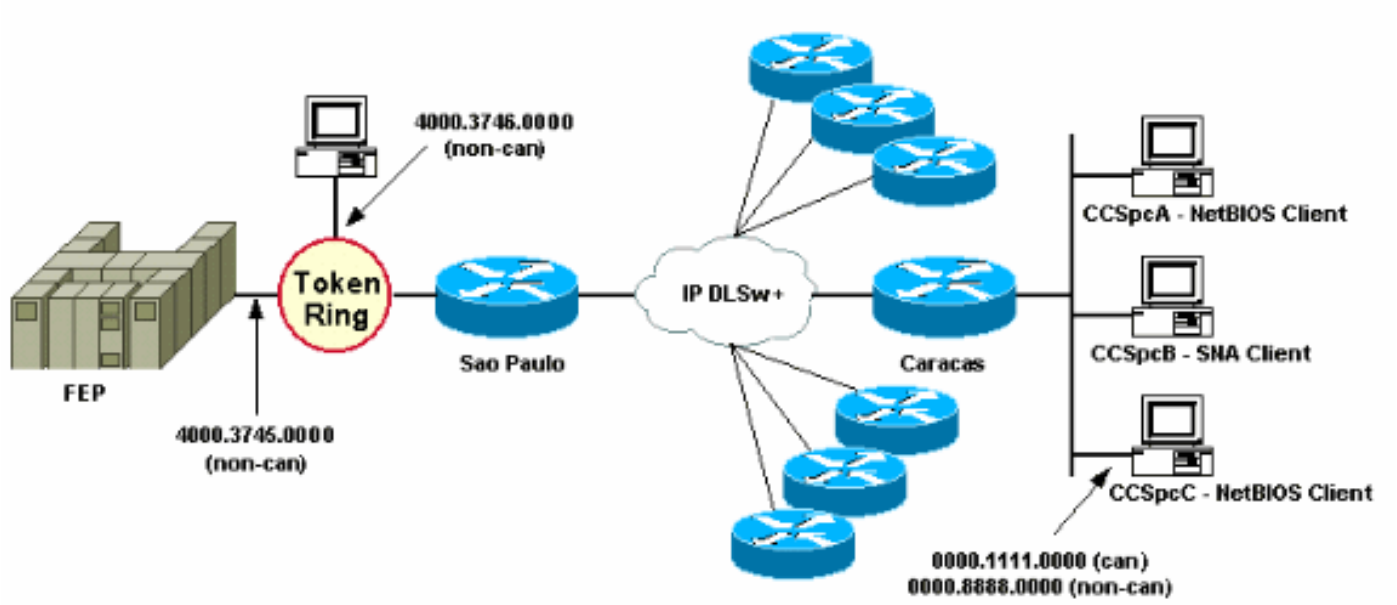
```
CARACAS#debug dlsw reachability verbose sna
 DLSw reachability debugging is on at verbose level for SNA traffic

 *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
```

configuration de dlsw icanreach mac-exclusif remote au niveau du routeur central

Àce stade, le schéma du réseau et les exigences de conception sont modifiés. Voici le nouvel exemple de réseau :



Dans cet exemple, un nouveau périphérique SNA (4000.3746.0000) est ajouté à l'emplacement Sao Paulo. Cette machine doit établir une communication avec un périphérique à un autre emplacement (homologue 3.3.3.1). Le routeur 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 Sao Paulo, le routeur Sao Paulo informe tous ses homologues qu'en

raison de la commande **mac-exclusive**, il ne peut atteindre que l'adresse MAC 4000.3745.000. Comme indiqué dans cette sortie de **débogage**, cela empêche également le nouveau périphérique SNA (4000.3746.0000) d'établir la communication via 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 corriger cela, 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 **remote**, d'autres périphériques du routeur central sont autorisés (qui ne sont pas spécifiés dans la commande **dlsw icanreach mac-address**) à établir des connexions sortantes. Il s'agit de la sortie de **débogage** sur Sao Paulo lorsque le périphérique 4000.3746.000 a démarré 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 DLSw
- Guide de conception DLSw+
- Guide de dépannage DLSw+
- Présentation des listes de contrôle d'accès SAP (Service Access Point)