DLSw+ SAP/MAC-filtering

Inhoud

Inleiding

Dit document bevat voorbeeldconfiguraties voor datalink-switching plus (DLSw+) Service access point (SAP) en MAC-filtertechnieken.

Filtering kan worden gebruikt om de schaalbaarheid van een DLSw+-netwerk te verbeteren. U kunt bijvoorbeeld filtering gebruiken om:

- Verminder het verkeer via een WAN-link (met name belangrijk voor zeer snelle links en in omgevingen met NetInstall).
- Vergroot de beveiliging van een netwerk door de toegang tot bepaalde apparaten te controleren.
- Vergroot de CPU-prestaties en schaalbaarheid van DLSw+-routers voor datacenters.

DLSw+ biedt verschillende opties die kunnen worden gebruikt voor het filteren. Filtering kan worden uitgevoerd op MAC-adressen, SAP- of NetConfiguration-namen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configureren voor DLSw+ SAP-filtering

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Als u aanvullende informatie wilt vinden over de opdrachten in dit document, gebruikt u het Opdrachtplanningprogramma (alleen geregistreerd klanten).

Gebruik van de netwerktopologie die in het gedeelte Netwerkdiagram wordt afgebeeld, om al het Netparticuliere verkeer op afgelegen locaties te stoppen met het bereiken van de Central-router (Sao Paulo). DLSw+ biedt verschillende opties om deze taak te volbrengen, die in de volgende secties worden geanalyseerd.

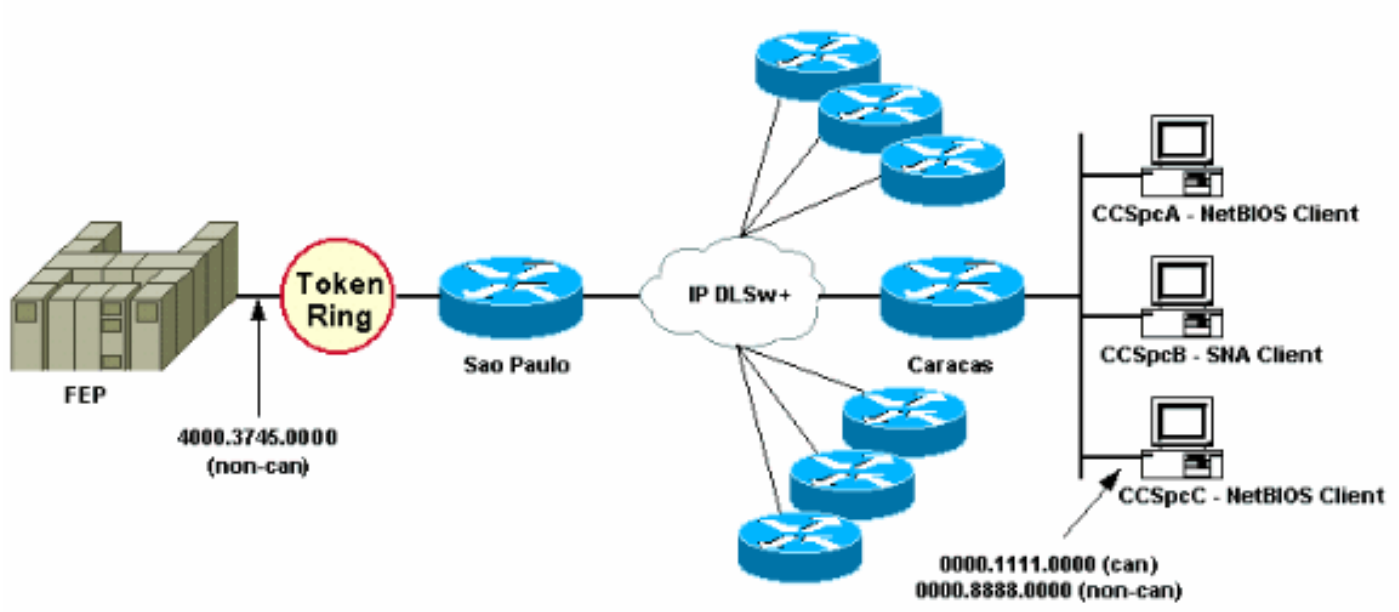
N.B.: Netoverheid gebruikt SAP-waarden 0xF0 (voor opdrachten) en 0xF1 (voor antwoorden). Meestal gebruiken netwerkbeheerders de bovengenoemde SAP-waarden om dit protocol te filteren (aanvaarden of ontkennen).

N.B.: Netoverheid-clients gebruiken het Netoverheid-functionele MAC-adres (C000.000.0080) als de bestemming MAC (DMAC) op hun NetReset-applicaties. Zoals eerder vermeld, hebben alle frames SAP-waarden van 0xF0 of 0xF1.

Voor deze test wordt de CCSpcC PC geconfigureerd om met behulp van SAP 0xF0 aan te sluiten op het MAC-adres van de FEP. In werkelijkheid ziet dit verkeer er hetzelfde uit als NetMeeting, ten minste vanuit een SAP-perspectief. Daarom kunt u de bijbehorende debugs in de DLSw+ router observeren wanneer dit verkeer arriveert.

Netwerkdiagram

Deze sectie gebruikt de netwerkinstellingen die in dit diagram worden weergegeven.



In het netwerkdiagram wordt een datacenterrouter (Sao Paulo) afgebeeld met een verbinding naar het mainframe. Deze router ontvangt meerdere DLSw+ peer verbindingen van alle externe takken. Elke externe tak heeft zowel Systems Network Architecture (SNA) als NetConfiguration-clients. In het datacenter zijn er geen Netoverheid-servers die toegang moeten krijgen van de externe kantoren.

Voor de eenvoud worden de configuratiegegevens van slechts één extern kantoor (Caracas) weergegeven. Het netwerkdiagram toont ook de MAC-adreswaarde van de front-end processor (FEP) en de externe PC die CCSpcC wordt genoemd. De adressen van MAC worden getoond in zowel canonical (Ethernet) als niet-kanonisch (Token Ring) formaat.

LSAP-toegangslijsten op externe vestigingen configureren

Met deze methode moeten alle externe vestigingen zijn geconfigureerd met de optie **lsap-output-lijst**. Er worden geen andere configuratiewijzigingen in de centrale router vereist.

De **lsap-uitvoer-lijst** links naar een SAP-toegangslijst (SAP ACL's) die momenteel alleen SNA SAP's (bijvoorbeeld 0x00, 0x04, 0x08 enzovoort) toestaat om naar de centrale router te gaan en ontkent alles wat anders is. Raadpleeg de begrijpelijke toegangscontrolelijsten voor servicepunt voor meer informatie over het uitvoeren van filtering op basis van SAP's.

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

```
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
```

```
!
interface Serial1/0
 ip address 1.1.1.1
255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 clockrate 32000
!
end
```

De opdracht **debug dlsw** wordt gebruikt om te zien hoe de Caracas-router reageert wanneer de router het NetReset-verkeer ontvangt.

```
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
```

Als de router op afstand (Caracas) geen bereikbaarheidsinformatie heeft voor 4000.3745.0000, en er een verkenner wordt die op dat MAC-adres let met behulp van een aantal van de "verboden" SAP's, is het verzoek geblokkeerd.

```
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
```

Neem het geval waarin de router op afstand van kantoor (Caracas) bereikbaarheidsinformatie heeft voor 4000.3745.0000. Bijvoorbeeld, een ander station (met de toegestane SAP's) vroeg al om het FEP MAC-adres. In deze situatie stuurt de "overtreder" PC (CCSpcC) zijn NULL XID, maar de router stopt deze.

```
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
```

DLSw-ijsbestrijdingskaarten configureren op de centrale router

Met de opdracht **dlsw icannotreach** kunt u de protocollen filteren waarvan u weet dat ze niet overheen mogen worden verzonden. Als u alleen weet wat expliciet moet worden ontkend, gebruikt u de opdracht **dlsw icannotreach** op de centrale router(s), zoals getoond in deze configuraties.

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

U kunt de centrale router (inclusief de opdracht **dlsw icannotreach**) tijdens de vlucht configureren, zelfs wanneer de afstandsbediening al actief is. Deze uitvoer toont het debug op een van de afstandsrouters, die de ontvangst van het CapExID-bericht aangeeft. Dit bericht geeft de externe kantoren op om geen frames met SAP 0xF0/F1 naar de centrale router te verzenden.

```
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
```

Nadat het CapExID-bericht is ontvangen, leert de router Caracas dat Sao Paulo geen SAP 0xF0

ondersteunt.

```
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.
```

De hier weergegeven opdrachtoutput, die op de centrale router is genomen, toont de configuratiewijziging in de gebieden waarop SAP 0xF0 niet wordt ondersteund.

```
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.
```

Dit is de **debug**-uitvoer van de Caracas-router wanneer het Netoverheid PC-station probeert de verbinding te maken:

```
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
```

DLSw-contentbereik configureren op de centrale router

Het configureren van het **dlsw icanreach saps**-opdracht is handig wanneer u precies weet welk type verkeer is toegestaan en u wilt ervoor zorgen dat al het andere verkeer wordt ontkend. Bijvoorbeeld, wanneer u **dlsw icanreach saps 4** configureren, ontkent u expliciet alle saps behalve 0x04 (en 0x05, de respons).

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

Opmerking in deze opdrachtoutput van **show** dat de Caracas router erkent dat Sao Paulo alleen frames ondersteunt die bestemd zijn voor saps 0x04 en 0x05. Alle andere kaarten worden niet ondersteund.

```
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.
```

U kunt de **lokale** opdracht van de **show dlsw-functies** gebruiken om te verifiëren dat de configuratieveranderingen in de centrale router in de DLSw+-code verschijnen.

```
SAOPAULO#show dlsw capabilities local
 DLSw: Capabilities for local peer 1.1.1.1
   vendor id (OUI)          : '00C' (cisco)
   version number           : 2
   release number           : 0
   init pacing window       : 20
   unsupported saps  : 0 2 6 8 A C E 10 12 14 16 18 1A 1C 1E 20 22 24 26 28
```

```
 2A 2C 2E 30 32 34 36 38 3A 3C 3E 40 42 44 46 48 4A 4C 4E 50 52 54 56 58 5A 5C 5E
 60 62 64 66 68 6A 6C 6E 70 72 74 76 78 7A 7C 7E 80 82 84 86 88 8A 8C 8E 90 92 94
 96 98 9A 9C 9E A0 A2 A4 A6 A8 AA AC AE B0 B2 B4 B6 B8 BA BC BE C0 C2 C4 C6 C8 CA
 CC CE D0 D2 D4 D6 D8 DA DC DE E0 E2 E4 E6 E8 EA EC EE F0 F2 F4 F6 F8 FA FC FE
  num of tcp sessions      : 1
  loop prevent support     : no
  icanreach mac-exclusive  : no
  icanreach netbios-excl.  : no
  reachable mac addresses  : none
  reachable netbios names  : none
  V2 multicast capable     : yes
  DLSw multicast address   : none
  cisco version number     : 1
  peer group number        : 0
  peer cluster support     : yes
  border peer capable      : no
  peer cost                : 3
  biu-segment configured   : no
  UDP Unicast support      : yes
  Fast-switched HPR supp.  : no
  NetBIOS Namecache length : 15
  cisco RSVP support       : no
  current border peer      : none
  version string           :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JK2O3S-M), Version 12.0(7)T,  RELEASE SOFTWARE (fc2)
Copyright (c) 1986-1999 by cisco Systems, Inc.
```

DLSw+ MAC-filtering

Gebruik van het netwerkdiagram dat in dit document wordt getoond, om de centrale router frames te maken die bestemd zijn voor het FEP MAC-adres (4000.3745.000).

DLSw-icanreach-hoofdadres in de centrale router configureren

Met het **dlsw icanreach mac-address** opdracht, hebben alle externe kantoren een ingang op hun DLSw+ bereikbaarheidslijst voor het MAC-adres van de host dat naar het IP-adres van de centrale router wijst. Deze ingang is in de staat UNCONFIRM, die erop wijst dat als de verre kantoorrouter een lokale test of XID voor de host ontvangt, het een bericht CUR_ex (Can U Reach Explorer) alleen naar de centrale router stuurt.

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	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

```
 ip address 1.1.1.2
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
```

Hier heeft de Caracas router een permanente ingang in zijn bereikbaarheidscache gecreëerd. Als er geen nieuw nummer komt, wordt de staat NIET BEVESTIGD. Raadpleeg het leesbaarheidshoofdstuk van de DLSw+-probleemoplossing voor meer informatie over de manier waarop DLSw+ routers MAC-adressen en NetOS-namen maken.

```
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
```

De output van het bevel van de **show dlsw** op de router van Caracas bevestigt dat dit afstandskantoor weet dat het MAC-adres 4000.3745.000 bereikbaar is via peer 1.1.1. Let ook op de lijn die "icanreach mac-exclusieve: ". Het wijst erop dat de centrale router andere MAC adressen behalve de gastheer kan bereiken. Daarom, als om het even welke verre bureaus andere MAC adres zoeken, kunnen zij hun verzoeken naar de centrale router sturen. Met de opname van het **icanreach mac-adres 4000.3745.0000** commando zijn alle verafgelegen filialen zich echter bewust van de locatie van deze belangrijke hulpbron. Als u verdere beperkingen wilt plaatsen op welke frames bij de centrale router aankomen, raadpleeg dan Configure dlsw icanreach mac-only bij Central Router.

```
CARACAS#show dlsw capabilities
 DLSw: Capabilities for peer 1.1.1.1(2065)
   vendor id (OUI)          : '00C' (cisco)
   version number           : 2
   release number           : 0
   init pacing window       : 20
   unsupported saps         : none
   num of tcp sessions      : 1
   loop prevent support     : no
   icanreach mac-exclusive  : no
   icanreach netbios-excl.  : no
   reachable mac addresses  : 4000.3745.0000




   reachable netbios names  : none
   V2 multicast capable     : yes
```

```
   DLSw multicast address   : none
   cisco version number     : 1
   peer group number        : 0
   peer cluster support     : no
   border peer capable      : no
   peer cost                : 3
   biu-segment configured   : no
   UDP Unicast support      : yes
   Fast-switched HPR supp. : no
   NetBIOS Namecache length : 15
   local-ack configured     : yes
   priority configured      : no
   cisco RSVP support      : no
   configured ip address    : 1.1.1.1
   peer type                : conf
   version string           :
 Cisco Internetwork Operating System Software
 IOS (tm) C2600 Software (C2600-JK2O3S-M), Version 12.0(7)T,  RELEASE SOFTWARE (fc2)
 Copyright (c) 1986-1999 by cisco Systems, Inc.
```

U kunt de **masker** parameter gebruiken als **dlsw icanreach mac-adres 4000.3745.0000** ***mask ffff.ffff.ffff.*** Wanneer u deze parameter gebruikt, let op dat de MAC-adressen doorgaans in hexadecimale indeling (0x4000.3745.000) worden weergegeven. Daarom wordt een all-ones masker (in binair getal) weergegeven door het hexadecimale getal 0xFFFF.FFFF.FFFF.

Hier is een voorbeeld van hoe te bepalen of een bepaalde input MAC onder een reeds gevormd **dlsw icanreach mac-adres** opdracht is opgenomen:

1. Begin met een router die met het **dlsw icanreach mac-adres 4000.3745.0000 mask fff.ffff.** 0000 opdracht **wordt** geconfigureerd.
2. Evalueer of het input-MAC-adres 4000.3745.0009 al dan niet is opgenomen door de vorige opdracht voor routerconfiguratie.
3. Converteer eerst het MAC-adres (4000.3745.0009) en de geconfigureerde MASK (FFFF.FFFF.0000) van hexadecimale naar binaire representatie. De eerste twee rijen in deze tabel tonen deze stap.
4. Voer vervolgens een logische EN handeling uit tussen deze twee binaire getallen en converteer het resultaat naar hexadecimale weergave (4000.3745.000). Het resultaat van deze operatie wordt in de derde rij van deze tabel weergegeven.
5. Als het resultaat van de AND-bewerking overeenkomt met het MAC-adres in de opdracht **dlsw icanreach mac-adres** (in ons voorbeeld 4000.3745.0000) wordt het MAC-adres (4000.3745.0009) toegestaan door het **dlsicw een** opdracht voor een hoofdadres. In ons voorbeeld wordt elk MAC-adres dat binnen het bereik van 4000.3745.000 tot 4000.3745.FFFF valt, opgenomen door de opdracht **dlsw icanreach mac-adres**. U kunt dit controleren door de zelfde stappen voor om het even welke MAC adressen in dit bereik te herhalen.

Dit zijn nog een paar voorbeelden:

- **dlsw icanreach mac-adres 4000.3745.000 mask ffff.ffff.ffff**-Deze opdracht bevat alleen het MAC-adres 4000.3745.000. Geen andere MAC-adressen geven dit masker door.
- **dlsw icanreach mac-adres 4000.0000.3745 mask fff.0000.ffff**-Deze opdracht bevat alle MAC-adressen in het bereik 4000.XXXX.3745 waarin XXXX 0x000FF-0xFFF is .

Het configureren van dlsw icanreach mac-exclusief bij de centrale router

Met de **dlsw icanreach mac-exclusieve** opdracht die bij de centrale router is ingesteld, zorgt u ervoor dat alleen pakketten die bestemd zijn voor de MAC-adressen die eerder zijn gedefinieerd (in dit geval 4000.3745.000) op de centrale locatie zijn toegestaan.

Let op dat deze filterinformatie tussen alle DLSw+-peers wordt uitgewisseld via CapExID-berichten. U slaat WAN-bandbreedte op door de filterinformatie op de centrale locatie te configureren, zelfs als de handelingen (zoals blokkerende frames) zich op de afstandsrouters zelf voordoen.

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.fffff** ! interface TokenRing0/0 no ip directed-broadcast ring-speed 16 source-bridge 10 1 3 source-bridge spanning ! interface Serial1/0 ip address 1.1.1.1 255.255.255.0 no ip directed-broadcast no ip mroute-cache clockrate 32000 ! end

Let erop dat de Caracas-router weet dat het MAC-adres 4000.3745.0000 bereikbaar is via peer 1.1.1. Het verschil tussen dit voorbeeld en het vorige scenario is dat we hier "icanreach mac-exclusiviteit tonen: ja", wat betekent dat de afgelegen kantoren geen andere frames naar de centrale router sturen dan die welke bestemd zijn voor 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.
```

De **debug-**uitvoer hier toont hoe de Caracas-router reageert op inkomend verkeer dat bestemd is voor een ander MAC-adres dan 4000.3745.000 (4000.3745.0080 wordt hier gebruikt). Caracas gebruikt Sao Paulo niet voor frames die niet bestemd zijn voor de host (4000.3745.0000). In dit geval is Sao Paulo de enige externe peer die in Caracas is geconfigureerd, dus deze router heeft geen ander peer om het te verzenden.

```
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
```

Als u een router met het **dlsw icanreach mac-exclusieve** opdracht configureren zonder een MAC-adres te definiëren met behulp van het opdracht **dlsw icanreach mac-adres**, geeft de router aan zijn peers aan dat deze geen MAC-adressen kan bereiken. Daarom verlies je de communicatie via die peer.

Opmerking: de voorbeeldconfiguratie hier wordt alleen als voorbeeld weergegeven. Het is een vergissing en **mag niet worden gebruikt**.

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
```

Deze **debug**-uitvoer geeft aan wat er gebeurt op de Caracas-router wanneer er een frame wordt ontvangen dat bestemd is voor 400.3745.000. Merk op dat Caracas alleen één DLSw Remote-peer (Sao Paulo) heeft, maar in de vorige configuratie heeft Sao Paulo aan zijn peers aangegeven dat het geen MAC-adressen kan bereiken.

```
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
```

DLSw-hoofdadres configureren op de afstandsrouters

In dit voorbeeld wordt elke externe kantoorrouter handmatig ingesteld en op de gewenste centrale router gericht wanneer u op specifieke MAC-adressen zoekt. Dit vermindert onnodig verkeer dat naar de verkeerde peer gaat. Als het externe kantoor maar één externe peer heeft geconfigureerd, is deze configuratie niet voordelig. Als echter meerdere externe peers worden geconfigureerd, richt deze configuratie de router op de juiste plaats zonder WAN-bandbreedte te verspillen.

Eén nieuwe DLSw+ externe peer (2.2.2.1) wordt ingesteld op de Caracas-router.

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
```

Beginnend met een lege bereikbaarheidstabel op de Caracas router, merk op dat de ingang voor de FEP in niet-BEVESTIGINGSstatus is:

```
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
```

Wanneer het eerste pakket arriveert op zoek naar FEP, worden alleen de pakketten naar peer 1.1.1 (Sao Paulo) verzonden en niet naar 2.2.2.1. Daarom slaat u WAN-bandbreedte en CPU-bronnen op de andere peers op.

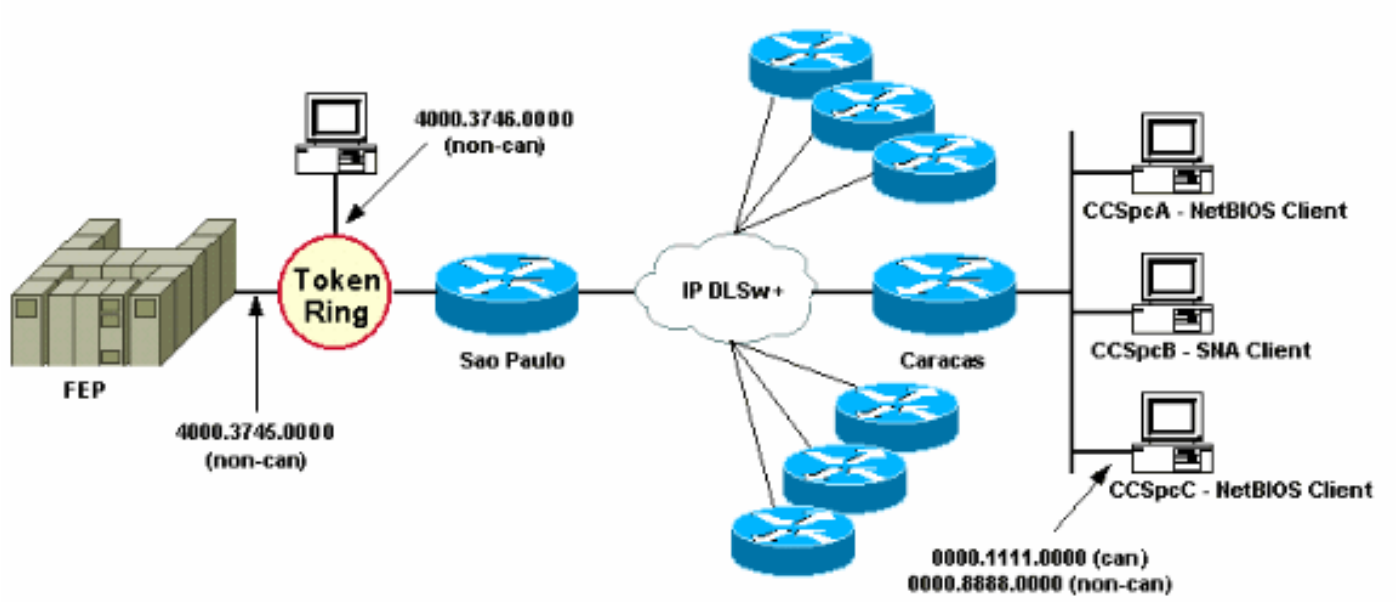
```
CARACAS#debug dlsw reachability verbose sna
 DLSw reachability debugging is on at verbose level for SNA traffic

 *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
```

Het configureren van dlsw icanreach mac-exclusieve afstandsbediening op de centrale router

Op dit punt worden het netwerkdiagram en de ontwerpvereisten gewijzigd. Dit is het nieuwe netwerkvoorbeeld:



In dit voorbeeld wordt een nieuw SNA-apparaat (4000.3746.0000) toegevoegd op de locatie van Sao Paulo. Deze machine moet communicatie met een apparaat op een andere locatie tot stand brengen (peer 3.3.3.1). De router van Sao Paulo voert deze configuratie uit.

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
```

Met deze configuratie van Sao Paulo, informeert de router van Sao Paulo al zijn peers dat, door het **mac-exclusieve** commando, het alleen het MAC-adres 4000.3745.000 kan bereiken. Zoals wordt getoond in deze **debug** uitvoer, voorkomt dit ook het nieuwe SNA apparaat (4000.37) 46.0000) van het opzetten van communicatie 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
```

Om dit te repareren, veranderen deze in de configuratie van 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
```

Met het **verre** sleutelwoord, zijn andere apparaten bij de centrale router toegestaan (die niet in de **dlsw icanreach mac-adres** opdracht worden gespecificeerd) om uitgaande verbindingen te maken. Dit is de **debug** output op Sao Paulo toen het apparaat 4000.3746.0000 zijn verbinding begon.

```
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
```

Gerelateerde informatie

- DLSw-ondersteuningspagina
- DLSw+ ontwerpgids
- Handleiding voor DLSw+ probleemoplossing
- De betekenis van Service Access Point-toegangscontrolelijsten