Tecniche di filtro DLSw+ SAP/MAC

Sommario

Introduzione

In questo documento vengono fornite configurazioni di esempio per le tecniche DLSw+ (Data-Link Switching Plus), SAP (Service Access Point) e MAC Filtering.

Il filtro può essere utilizzato per migliorare la scalabilità di una rete DLSw+. È ad esempio possibile utilizzare i filtri per:

- Ridurre il traffico su un collegamento WAN (particolarmente importante su collegamenti a velocità molto bassa e in ambienti con NetBIOS).
- Migliorare la sicurezza di una rete controllando l'accesso a determinati dispositivi.
- Migliora le prestazioni della CPU e la scalabilità dei router DLSw+ per data center.

DLSw+ offre diverse opzioni che possono essere utilizzate per eseguire il filtraggio. È possibile filtrare gli indirizzi MAC, i nomi SAP o NetBIOS.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione per le tecniche di filtro DLSw+ SAP

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Utilizzando la topologia di rete illustrata nella sezione Diagramma reticolare, è necessario interrompere tutto il traffico NetBIOS nelle postazioni remote per raggiungere il router centrale (San Paolo). DLSw+ offre diverse opzioni per eseguire questa operazione, che vengono analizzate nelle sezioni seguenti.

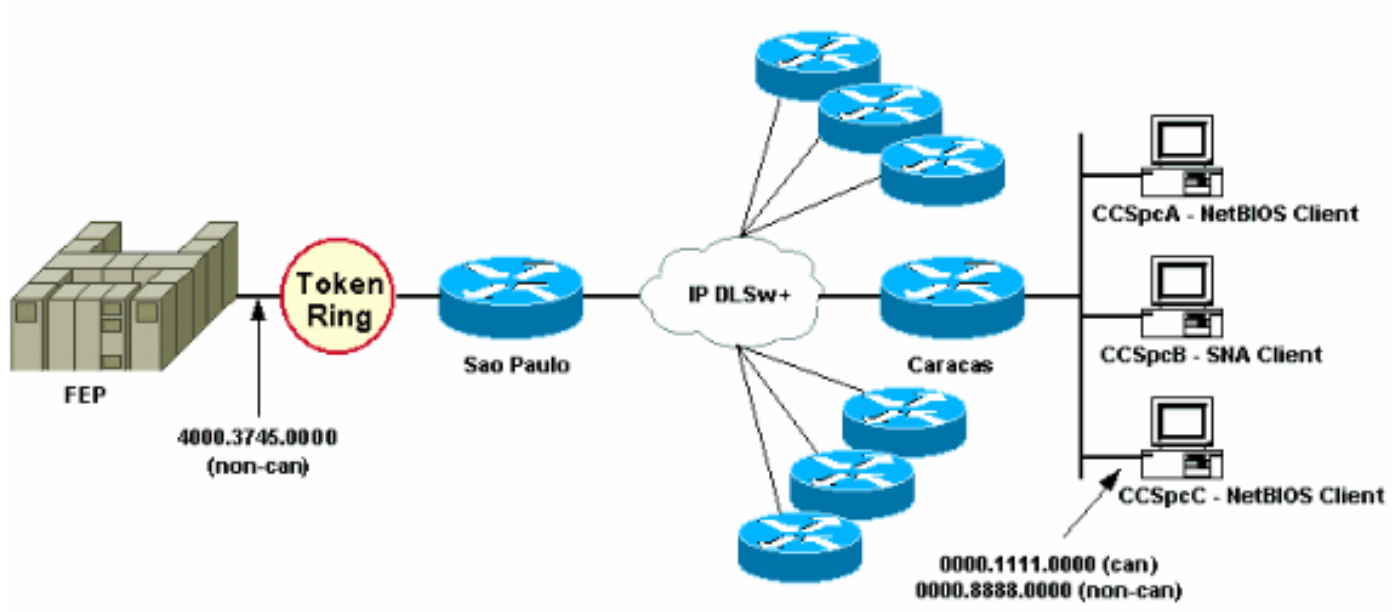
Nota: il traffico NetBIOS utilizza i valori SAP 0xF0 (per i comandi) e 0xF1 (per le risposte). In genere, gli amministratori di rete utilizzano i valori SAP sopra indicati per filtrare (accettare o negare) questo protocollo.

Nota: i client NetBIOS utilizzano l'indirizzo MAC funzionale NetBIOS (C000.0000.0080) come indirizzo MAC di destinazione (DMAC) sui pacchetti di query del nome NetBIOS. Come accennato in precedenza, tutti i frame hanno valori SAP di 0xF0 o 0xF1.

Per questo test, il PC CCSpcC è configurato per la connessione all'indirizzo MAC del FEP utilizzando SAP 0xF0. In realtà questo traffico ha lo stesso aspetto di NetBIOS, almeno dal punto di vista SAP. Pertanto, è possibile osservare i debug corrispondenti nel router DLSw+ quando questo traffico arriva.

Esempio di rete

Questa sezione utilizza la configurazione di rete illustrata nel diagramma.



Nel diagramma di rete è raffigurato un router per centro dati (San Paolo) con una connessione al mainframe. Questo router riceve più connessioni peer DLSw+ da tutte le succursali remote. Ogni filiale remota dispone sia di SNA (Systems Network Architecture) che di client NetBIOS. Nel centro dati non sono presenti server NetBIOS a cui è necessario accedere dagli uffici remoti.

Per semplicità, vengono mostrati i dettagli di configurazione di un solo ufficio remoto (Caracas). Il diagramma di rete mostra anche il valore dell'indirizzo MAC del processore front-end (FEP) e del PC remoto chiamato CCSpcC. Gli indirizzi MAC sono mostrati in formato canonico (Ethernet) e non canonico (Token Ring).

Configurazione degli elenchi degli accessi all'output LSAP negli uffici remoti

Con questo metodo, tutti gli uffici remoti devono essere configurati con l'opzione **lsap-output-list**. Non sono necessarie altre modifiche alla configurazione nel router centrale.

L'**lsap-output-list** si collega a un elenco degli accessi SAP (ACL SAP) che attualmente consente solo ai SAP SNA (ad esempio, 0x00, 0x04, 0x08 e così via) di dirigersi verso il router centrale e nega tutto il resto. Per ulteriori informazioni su come eseguire i filtri basati sugli Access Point, fare riferimento a Descrizione degli Access Control List dei punti di accesso al servizio.

CARACAS	SAN PAOLO
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	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 !

```
 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
```

Il comando **debug dlsw** viene usato per verificare la reazione del router Caracas quando riceve il traffico 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
```

Se il router della sede remota (Caracas) non dispone di informazioni sulla raggiungibilità per 4000.3745.0000 e ottiene un elenco di cartelle che cerca l'indirizzo MAC utilizzando alcuni SAP "vietati", la richiesta viene bloccata.

```
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
```

Si consideri il caso in cui il router dell'ufficio remoto (Caracas) non dispone di informazioni sulla raggiungibilità per 4000.3745.0000. Ad esempio, un'altra stazione (che utilizza gli SAP consentiti) ha già richiesto l'indirizzo MAC FEP. In questa situazione, il PC "offensivo" (CCSpcC) invia il proprio XID NULL, ma il router lo ferma.

```
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
```

Configurazione di dlsw icannotreach saps sul router centrale

Il comando **dlsw icannotreach saps** permette di filtrare i protocolli per i quali non è consentito l'invio. Se si conosce solo ciò che deve essere negato esplicitamente, usare il comando **dlsw icannotreach saps** sui router centrali, come mostrato in queste configurazioni.

CARACAS	SAN PAOLO
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

Èpossibile configurare il router centrale (includendo il comando **dlsw icannotreach saps**) al volo, anche quando i peer remoti sono già attivi. Questo output mostra il debug su uno dei router remoti, ossia la ricezione del messaggio CapExId. Questo messaggio indica agli uffici remoti di non inviare alcun frame con SAP 0xF0/F1 verso il router centrale.

```
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
```

Dopo aver ricevuto il messaggio CapExId, il router Caracas viene a sapere che San Paolo non supporta 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.
```

L'output del comando **show** qui visualizzato, restituito dal router centrale, mostra la modifica della configurazione dove SAP 0xF0 non è supportato.

```
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.
```

Questo è l'output del comando **debug** restituito dal router Caracas quando la stazione PC NetBIOS tenta la connessione:

```
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
```

Configurare il server DHCP dlsw icanreach sul router centrale

Configurare il comando **dlsw icanreach saps** è utile quando si conosce esattamente il tipo di traffico consentito e si desidera essere certi che venga rifiutato tutto il resto del traffico. Ad esempio, quando si configura **dlsw icanreach saps 4**, si negano esplicitamente tutti gli saps ad eccezione di 0x04 (e 0x05, la risposta).

CARACAS	SAN PAOLO
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	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

! bridge 1 protocol ieee ! end	clockrate 32000 ! end

In questo output del comando **show** il router Caracas riconosce che San Paolo supporta solo i frame destinati agli sap 0x04 e 0x05. Tutti gli altri sap non sono supportati.

```
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.
```

Èpossibile utilizzare il comando **show dlsw capabilities local** per verificare che le modifiche della configurazione sul router centrale vengano visualizzate nel codice 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.
```

Tecniche di filtro DLSw+ MAC

Utilizzando il diagramma di rete mostrato in questo documento, fare in modo che il router centrale riceva solo i frame destinati all'indirizzo MAC FEP (4000.3745.0000).

Configurazione di dlsw icanreach mac-address sul router centrale

Usando il comando **dlsw icanreach mac-address**, tutti gli uffici remoti hanno una voce nella tabella DLSw+ reachability per l'indirizzo MAC dell'host che punta all'indirizzo IP del router centrale. Questa voce si trova nello stato UNCONFIRM, che indica che se il router della sede remota riceve un test locale o un XID per l'host, invia un messaggio CUR_ex (Can U Reach Explorer) solo al router centrale.

CARACAS	SAN PAOLO
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 !	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 address 1.1.1.1 255.255.255.0 no ip directed-broadcast

bridge 1 protocol ieee ! end	no ip mroute-cache clockrate 32000 ! end

In questo caso, il router Caracas ha creato una voce permanente nella cache di raggiungibilità. Se la voce non è nuova, lo stato è UNCONFIRM. Per ulteriori informazioni su come i router DLSw+ memorizzano nella cache gli indirizzi MAC e i nomi NetBIOS, consultare il capitolo Raggiungibilità della guida alla risoluzione dei problemi DLSw+.

```
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
```

L'output del comando **show dlsw capabilities** sul router Caracas conferma che l'ufficio remoto è a conoscenza del fatto che l'indirizzo MAC 4000.3745.0000 è raggiungibile tramite il peer 1.1.1.1. Si noti anche la riga "icanreach mac-unique: no". Indica che il router centrale è in grado di raggiungere altri indirizzi MAC oltre all'host. Pertanto, se uno degli uffici remoti cerca un altro indirizzo MAC, può inviare le proprie richieste al router centrale. Tuttavia, con l'inclusione del comando **icanreach mac-address 4000.3745.0000**, tutte le filiali remote sono a conoscenza della posizione di questa importante risorsa. Per ulteriori restrizioni sui frame che arrivano al router centrale, consultare il documento sulla configurazione della funzione dlsw icanreach mac-unique sul router centrale.

```
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.
```

Èpossibile utilizzare il parametro **mask** come **dlsw icanreach mac-address 4000.3745.0000** ***mask ffff.ffff.ffff***. Quando si utilizza questo parametro, gli indirizzi MAC sono in genere presentati in formato esadecimale (0x4000.3745.0000). Pertanto, una maschera all-one (in formato binario) è rappresentata dal numero esadecimale 0xFFFF.FFFF.

Di seguito è riportato un esempio di come determinare se un particolare MAC di input è incluso in un comando **dlsw icanreach mac-address** già configurato:

1. Iniziare con un router configurato con il comando **dlsw icanreach mac-address 4000.3745.0000 mask ffff.ffff** 0000.
2. Valutare se l'indirizzo MAC di input 4000.3745.0009 è incluso o meno con il precedente comando di configurazione del router.
3. Convertire innanzitutto l'indirizzo MAC (4000.3745.0009) e la maschera configurata (FFFF.FFFF.0000) dalla rappresentazione esadecimale a quella binaria. Nelle prime due righe della tabella viene illustrato questo passaggio.
4. Eseguire quindi un'operazione AND logica tra i due numeri binari e convertire il risultato in rappresentazione esadecimale (4000.3745.0000). Il risultato di questa operazione è illustrato nella terza riga della tabella.
5. Se il risultato dell'operazione AND corrisponde all'indirizzo MAC nel comando **dlsw icanreach mac-address** (nell'esempio riportato, 4000.3745.0000), l'indirizzo MAC di input (4000.3745.0009) viene autorizzato dal comando **dlsw icanreach mac-address**. Nell'esempio, gli indirizzi MAC di input compresi nell'intervallo da 4000.3745.0000 a 4000.3745.FFFF vengono inclusi dal comando **dlsw icanreach mac-address**. È possibile verificare questa condizione ripetendo gli stessi passaggi per qualsiasi indirizzo MAC incluso nell'intervallo.

Ecco alcuni esempi:

- **dlsw icanreach mac-address 4000.3745.0000 mask ffff.ffff.ffff**—Questo comando include solo l'indirizzo MAC 4000.3745.0000. Nessun altro indirizzo MAC supera questa maschera.
- **dlsw icanreach mac-address 4000.0000.3745 mask ffff.0000.ffff** - Questo comando include tutti gli indirizzi MAC nell'intervallo 4000.XXXX.3745 dove XXXX è 0x0000-0xFFFF.

Configurazione di dlsw icanreach mac-unique sul router centrale

Con il comando **dlsw icanreach mac-unique** configurato sul router centrale, solo i pacchetti destinati agli indirizzi MAC precedentemente definiti (in questo caso 4000.3745.000) sono autorizzati sulla postazione centrale.

Si noti che queste informazioni di filtro vengono scambiate tra tutti i peer DLSw+ che utilizzano

messaggi CapExId. La larghezza di banda della WAN viene risparmiata configurando le informazioni di filtro nella posizione centrale, anche se le azioni (come il blocco dei frame) si verificano sui router remoti stessi.

CARACAS	SAN PAOLO
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

In questo output, il router Caracas è consapevole che l'indirizzo MAC 4000.3745.0000 è raggiungibile tramite il peer 1.1.1.1. La differenza tra questo esempio e lo scenario precedente è che qui viene mostrato "icanreach mac-unique: yes", ossia gli uffici remoti non inviano frame al router centrale diversi da quelli destinati a 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.
```

L'output del comando **debug** qui mostra come il router Caracas reagisce al traffico in entrata destinato a qualsiasi indirizzo MAC diverso da 4000.3745.0000 (in questo caso, viene utilizzato 4000.3745.0080). Caracas non usa San Paolo per i frame non destinati all'host (4000.3745.0000). In questo caso, San Paolo è l'unico peer remoto configurato in Caracas, quindi questo router non ha altri peer a cui inviarlo.

```
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
```

Se si configura un router con il comando **dlsw icanreach mac-unique** senza definire alcun indirizzo MAC con il comando **dlsw icanreach mac-address**, il router annuncia ai propri peer di non poter raggiungere alcun indirizzo MAC. Quindi perderete la comunicazione attraverso quel peer.

Nota: la configurazione di esempio è illustrata solo come esempio. È un errore e **non dovrebbe essere utilizzato**.

SAN PAOLO
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
```

Questo output di **debug** indica cosa succede al router Caracas quando riceve un frame destinato a 4000.3745.0000. Si noti che Caracas ha solo un peer remoto DLSw (San Paolo), ma nella configurazione precedente , San Paolo ha indicato ai peer che non può raggiungere alcun indirizzo 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
```

Configurazione dell'indirizzo dlsw mac sui router remoti

In questo esempio, quando si cercano indirizzi MAC specifici, ogni router di una sede remota viene configurato manualmente e indirizzato al router centrale desiderato. Ciò riduce il traffico non necessario diretto al peer sbagliato. Se per l'ufficio remoto è configurato un solo peer remoto, questa configurazione non è utile. Tuttavia, se sono configurati più peer remoti, questa configurazione indirizza il router del sito remoto al posto giusto senza sprecare la larghezza di banda della WAN.

Un nuovo peer remoto DLSw+ (2.2.2.1) è configurato sul router Caracas.

CARACAS	SAN PAOLO
Current configuration: ! hostname CARACAS ! dlsw local-peer peer-id 1.1.1.2 dlsw remote-peer 0 tcp 1.1.1.1	Current configuration: ! hostname SAOPAULO ! source-bridge ring- group 3

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	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

Iniziando con una tabella di raggiungibilità vuota sul router Caracas, notare che la voce per il FEP è in stato 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
```

Quando arriva il primo pacchetto in cerca di FEP, vengono inviati solo i pacchetti al peer 1.1.1.1 (San Paolo) e non alla 2.2.2.1. Pertanto, si risparmiano larghezza di banda WAN e risorse CPU sugli altri peer.

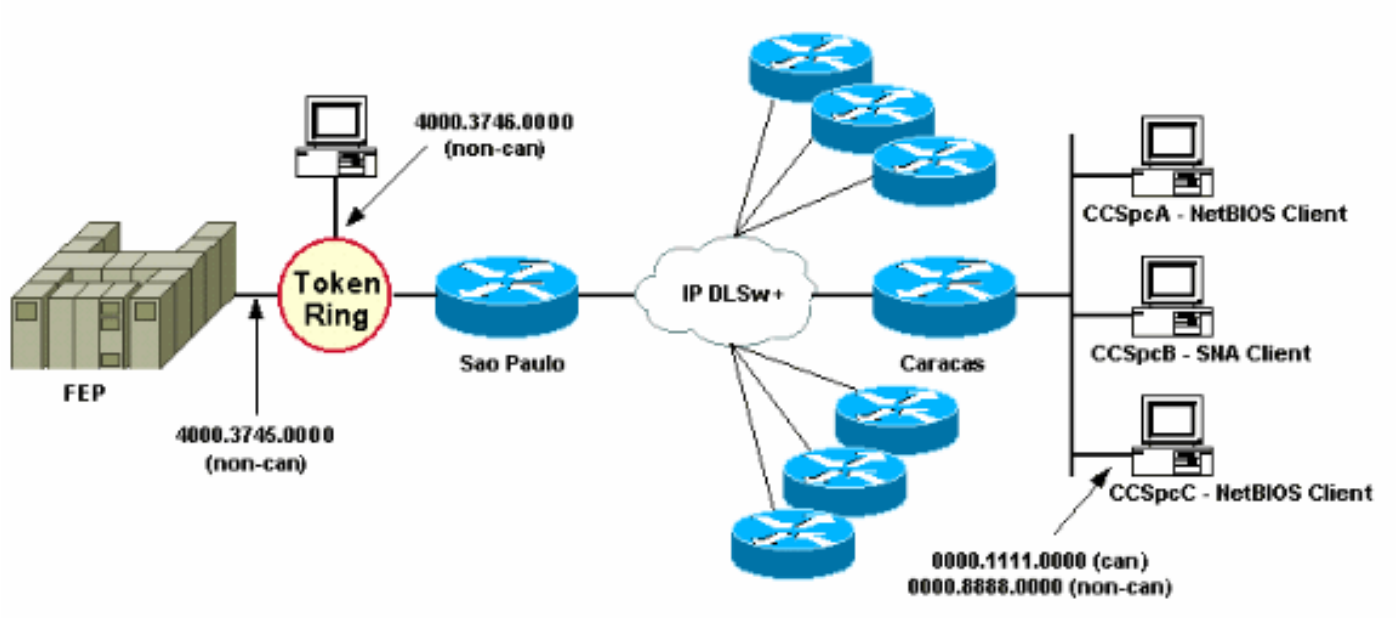
```
CARACAS#debug dlsw reachability verbose sna
 DLSw reachability debugging is on at verbose level for SNA traffic

 *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
```

Configurazione del telecomando dlsw icanreach mac-only sul router centrale

A questo punto, il diagramma di rete e i requisiti di progettazione vengono modificati. Questo è il

nuovo esempio di rete:



Nell'esempio, viene aggiunto un nuovo dispositivo SNA (4000.3746.0000) nella posizione di Sao Paulo. Questo computer deve stabilire la comunicazione con un dispositivo in un'altra posizione (peer 3.3.3.1). Il router di San Paolo esegue questa configurazione.

SAN PAOLO

```
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
```

Con questa configurazione per San Paolo, il router comunica a tutti i suoi peer che, a causa del comando **mac-exclusive**, può raggiungere solo l'indirizzo MAC 4000.3745.0000. Come mostrato in questo output di **debug**, ciò impedisce anche al nuovo dispositivo SNA (4000.3746.0000) di stabilire la comunicazione tramite 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
```

Per risolvere il problema, apportare le modifiche desiderate alla configurazione di San Paolo.

SAN PAOLO

```
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
```

Con la parola chiave **remote**, sono consentite altre periferiche sul router centrale (non specificate nel comando **dlsw icanreach mac-address**) per effettuare connessioni in uscita. Questo è l'output del comando **debug** su San Paolo quando il dispositivo 4000.3746.000 ha avviato la connessione.

```
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
```

Informazioni correlate

- Pagina di supporto DLSw

- Guida alla progettazione di DLSw+
- Guida alla risoluzione dei problemi DLSw+
- Informazioni sugli Access Control List dei punti di accesso al servizio