# Técnicas de filtragem DLSw+ SAP/MAC

## Índice



## Introdução

Este documento fornece configurações de amostra para o ponto de acesso ao serviço do Data-Link Switching Plus (DLSw+) (SAP) e as técnicas de filtração MAC.

Filtrar pode ser usada para aumentar a escalabilidade de uma rede do DLSw+. Por exemplo, você pode usar a filtração a:

- Reduza o tráfego através de um link MACILENTO (especialmente importante muito em enlaces de velocidade baixa e nos ambientes com o NetBIOS).
- Aumente a Segurança de uma rede controlando o acesso a determinados dispositivos.
- Aumente o desempenho da CPU e a escalabilidade do Roteadores do DLSw+ do centro de dados.

O DLSw+ oferece diversas opções que podem ser usadas para executar a filtração. Filtrar pode ser feita em endereços, em SAP, ou em nomes de netbios MAC.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

## Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

## Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

# Configure as técnicas de filtragem para DLSw+ SAP

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Nota:** Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes registrados).

Usando a topologia de rede descrita na seção do diagrama da rede, a exigência é parar todo o tráfego de netbios em posições remotas de alcançar o roteador central (Sao Paulo). O DLSw+ oferece diversas opções realizar esta tarefa, que são analisadas nas seguintes seções.

**Nota:** O tráfego de NetBIOS utiliza os valores de SAP 0xF0 (para comandos) e 0xF1 (para respostas). Tipicamente, os administradores de rede usam os valores acima mencionados de SAP para filtrar (aceite ou negue) este protocolo.

**Nota:** Os clientes netbios usam o MAC address funcional de NetBIOS (C000.0000.0080) como o MAC de destino (DMAC) em seus pacotes da pergunta do nome de netbios. Como mencionado mais cedo, todos os quadros têm valores de SAP de 0xF0 ou de 0xF1.

Para este teste, o CCSpcC PC é configurado para conectar ao MAC address do FEP usando SAP 0xF0. Na realidade este tráfego olha o mesmos que NetBIOS, pelo menos de uma perspectiva de SAP. Consequentemente, você pode observar que a correspondência debuga no roteador do DLSw+ quando este tráfego chega.

## Diagrama de Rede

Esta seção usa a instalação de rede mostrada neste diagrama.

No diagrama da rede, um roteador do centro de dados (Sao Paulo) é descrito com uma conexão à unidade central. Este roteador recebe conexões de peer múltiplas do DLSw+ de todos os filiais remotas. Cada filial remota tem o Systems Network Architecture (SNA) e os clientes netbios. Não há nenhum servidor de netbios no centro de dados que precisa de obter alcançado dos escritórios remotos.

Para a simplicidade, os detalhes de configuração de somente um escritório remoto (Caracas) são mostrados. O diagrama da rede igualmente mostra o valor do MAC address do processador de front end (FEP) e do PC remoto chamados CCSpcC. Os endereços MAC são mostrados no formato canônico (Ethernet) e não-canônico (do Token Ring).

## Configurar listas de acesso de saída lsap em escritórios remotos

Usando este método, todos os escritórios remotos devem ser configurados com a opção do **lsap-output-list**. Nenhuma outra alteração de configuração é exigida no roteador central.

**O lsap-output-list** liga a SAP uma lista de acessos (SAP ACL) que atualmente permite somente que as seivas SNA (por exemplo, 0x00, 0x04, 0x08, e assim por diante) vão para o roteador central, e nega tudo mais. Refira compreendendo listas de controle de acesso do ponto de acesso ao serviço para obter mais informações sobre de como executar a filtração baseada nas seivas.

| CARACAS | SAO PAULO |
|---|---|
| Current configuration:<br>!<br>hostname CARACAS<br>!<br>dlsw local-peer peer-id<br>1.1.1.2<br>dlsw remote-peer 0 tcp<br>1.1.1.1<br>**lsap-output-list 200** dlsw<br>bridge-group 1 ! interface<br>Ethernet0/0 no ip directed-<br>broadcast bridge-group 1 !<br>interface Serial0/1 ip<br>address 1.1.1.2 255.255.255.0<br>no ip directed-broadcast !<br>**access-list 200 permit 0x0000**<br>**0x0D0D access-list 200 deny**<br>**0x0000 0xFFFF** ! bridge 1<br>protocol ieee ! end | Current configuration:<br>!<br>hostname SAOPAULO<br>!<br>source-bridge ring-group 3<br>dlsw local-peer peer-id<br>1.1.1.1<br>dlsw remote-peer 0 tcp<br>1.1.1.2<br>!<br>interface TokenRing0/0<br>no ip directed-broadcast<br>ring-speed 16<br>source-bridge 10 1 3<br>source-bridge spanning<br>!<br>interface Serial1/0<br>ip address 1.1.1.1<br>255.255.255.0<br>no ip directed-broadcast<br>no ip mroute-cache<br>clockrate 32000<br>!<br>end |

**O comando debug dlsw** é usado considerar como o roteador de Caracas reage quando recebe o tráfego de netbios.

```
CARACAS#debug dlsw DLSw reachability debugging is on at event level for all protocol traffic
DLSw peer debugging is on DLSw local circuit debugging is on DLSw core message debugging is on
DLSw core state debugging is on DLSw core flow control debugging is on DLSw core xid debugging
is on
```

Se o roteador da sede remoto (Caracas) não a tem a informação de alcançabilidade para 4000.3745.0000, e obtém um explorador que procure que o MAC address que usa algum do "proibiu" as seivas, a seguir o pedido é obstruído.

```
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
```

Considere o caso onde o roteador da sede remoto (Caracas) tem a informação de alcançabilidade para 4000.3745.0000. Por exemplo, uma outra estação (que usa as seivas permitidas) já pediu o endereço MAC de fep. Nesta situação o "delinquente" PC (CCSpcC) envia seu XID NULO, mas o roteador para-o.

```
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
```

## Configurar as seivas do icannotreach do dlsw no roteador central

Usar o **comando dlsw icannotreach saps** permite que você filtre aqueles protocolos que você sabe não é reservado ser enviado transversalmente. Se você conhece somente o que deve explicitamente ser negado, use o **comando dlsw icannotreach saps no** roteador central, segundo as indicações destas configurações.

| CARACAS | SAO PAULO |
|---|---|
| Current configuration:<br>!<br>hostname CARACAS<br>!<br>dlsw local-peer peer-id 1.1.1.2<br>dlsw remote-peer 0 tcp 1.1.1.1<br>dlsw bridge-group 1<br>!<br>interface Ethernet0/0<br>no ip directed-broadcast<br>bridge-group 1<br>!<br>interface Serial0/1<br>ip address 1.1.1.2 255.255.255.0<br>no ip directed-broadcast<br>!<br>bridge 1 protocol ieee<br>!<br>end | Current configuration:<br>!<br>hostname SAOPAULO<br>!<br>source-bridge ring-group 3<br>dlsw local-peer peer-id 1.1.1.1<br>dlsw remote-peer 0 tcp 1.1.1.2<br>**dlsw icannotreach sap F0** !<br>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 |

Você pode configurar o roteador central (inclua o **comando dlsw icannotreach saps**) sobre - - voa, mesmo quando os peer remotos são já acima. Esta saída mostra debugar em um dos roteadores remotos, que indica a recepção do mensagem capexid. Esta mensagem instrui os escritórios remotos para não enviar nenhuns quadros com SAP 0xF0/F1 para o roteador 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
```

Depois que o mensagem capexid é recebido, o roteador de Caracas aprende que Sao Paulo não apoia 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.
```

**O show command output (resultado do comando show)** indicado aqui, tomado no roteador central, mostra à alteração de configuração onde SAP 0xF0 não é apoiado.

```
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.
```

Este é o **resultado do debug do** roteador de Caracas quando a estação de NetBIOS PC tenta a conexão:

```
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
```

## Configurar as seivas do icanreach do dlsw no roteador central

Configurar o **comando dlsw icanreach saps** é útil quando você conhece que exatamente o que o tipo de tráfego é permitido e você quer se certificar de que todo tráfego restante está negado. Por exemplo, quando você configura o **dlsw icanreach saps 4**, você nega explicitamente todas as seivas exceto 0x04 (e 0x05, a resposta).

| CARACAS | SAO PAULO |
|---|---|
| Current configuration:<br>!<br>hostname CARACAS<br>!<br>dlsw local-peer peer-id<br>1.1.1.2 | Current configuration:<br>!<br>hostname SAOPAULO<br>!<br>source-bridge ring-group 3<br>dlsw local-peer peer-id 1.1.1.1 |

| | |
|---|---|
| dlsw remote-peer 0 tcp 1.1.1.1<br>dlsw bridge-group 1<br>!<br>interface Ethernet0/0<br> no ip directed-broadcast<br> bridge-group 1<br>!<br>interface Serial0/1<br> ip address 1.1.1.2 255.255.255.0<br> no ip directed-broadcast<br>!<br>bridge 1 protocol ieee<br>!<br>end | dlsw remote-peer 0 tcp 1.1.1.2<br>**dlsw icanreach sap 0 4** !<br>interface TokenRing0/0 no ip directed-broadcast ring-speed 16 source-bridge 10 1 3 source-bridge spanning ! interface Serial1/0 ip address 1.1.1.1 255.255.255.0 no ip directed-broadcast no ip mroute-cache clockrate 32000 ! end |

Note neste **show command output (resultado do comando show)** que o roteador de Caracas reconhece que Sao Paulo apoia somente os quadros destinados às seivas 0x04 e 0x05. Todas seivas restantes são unsupported.

```
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.
```

Você pode usar o **comando show dlsw capabilities local** verificar que as alterações de configuração no roteador central aparecem no código do 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.
```

## Técnicas de filtragem de DLSw+ MAC

Usando o diagrama da rede mostrado neste documento, faça o roteador central receber os quadros destinados ao endereço MAC de fep (4000.3745.0000) somente.

## Configurar o endereço MAC do icanreach do dlsw no roteador central

Usando o **comando dlsw icanreach mac-address**, todos os escritórios remotos têm uma entrada em sua tabela de alcançabilidade do DLSw+ para o MAC address do host esses pontos ao endereço IP de Um ou Mais Servidores Cisco ICM NT do roteador central. Esta entrada está no estado UNCONFIRM, que indica que se o roteador da sede remoto recebe um teste local ou um XID para o host, ele envia uma mensagem de CUR_ex (pode o explorador do alcance U) ao roteador central somente.

| CARACAS | SAO PAULO |
|---|---|
| Current configuration:<br>!<br>hostname CARACAS<br>!<br>dlsw local-peer peer-id 1.1.1.2<br>dlsw remote-peer 0 tcp 1.1.1.1<br>dlsw bridge-group 1<br>!<br>interface Ethernet0/0<br>no ip directed-broadcast<br>bridge-group 1<br>!<br>interface Serial0/1<br>ip address 1.1.1.2 255.255.255.0<br>no ip directed-broadcast<br>!<br>bridge 1 protocol ieee<br>!<br>end | Current configuration:<br>!<br>hostname SAOPAULO<br>!<br>source-bridge ring-group 3<br>dlsw local-peer peer-id 1.1.1.1<br>dlsw remote-peer 0 tcp 1.1.1.2<br>**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 !<br>end |

Aqui, o roteador de Caracas criou uma entrada permanente em seu cache de alcançabilidade. Se a entrada não é fresca, o estado é UNCONFIRM. Refira o capítulo de alcançabilidade do guia de Troubleshooting do DLSw+ para obter mais informações sobre de como o Roteadores do DLSw+ põe em esconderijo endereços e nomes de netbios MAC.

```
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
```

A saída do **comando show dlsw capabilities no** roteador de Caracas confirma que este escritório remoto sabe que o MAC address 4000.3745.0000 é alcançável através do par 1.1.1.1. Igualmente note a linha que diz o “icanreach MAC-exclusivo: não”. Indica que o roteador central é capaz de alcançar o outro MAC endereça além do host. Consequentemente, se alguns dos escritórios remotos procuram o outro MAC address, podem enviar seus pedidos ao roteador central. Contudo, com a inclusão do **comando icanreach mac-address 4000 3745 0000**, todos os filiais remotas estão cientes do lugar deste recurso importante. Se você quer colocar umas limitações mais adicionais em que quadros chegam no roteador central, consulte para configurar o icanreach do dlsw MAC-exclusivo no roteador central.

```
CARACAS#show dlsw capabilities DLSw: Capabilities for peer 1.1.1.1(2065) vendor id (OUI) : '00C'
(cisco) version number : 2 release number : 0 init pacing window : 20 unsupported saps : none
```

```
num of tcp sessions : 1 loop prevent support : no icanreach mac-exclusive : no icanreach
netbios-excl. : no reachable mac addresses : 4000.3745.0000 <mask ffff.ffff.ffff> reachable
netbios names : none V2 multicast capable : yes DLSw multicast address : none cisco version
number : 1 peer group number : 0 peer cluster support : no border peer capable : no peer cost :
3 biu-segment configured : no UDP Unicast support : yes Fast-switched HPR supp. : no NetBIOS
Namecache length : 15 local-ack configured : yes priority configured : no cisco RSVP support :
no configured ip address : 1.1.1.1 peer type : conf version string : Cisco Internetwork
Operating System Software IOS (tm) C2600 Software (C2600-JK2O3S-M), Version 12.0(7)T, RELEASE
SOFTWARE (fc2) Copyright (c) 1986-1999 by cisco Systems, Inc.
```

Você pode usar o parâmetro da **máscara** como a *máscara ffff.ffff.ffff do* **endereço MAC 4000.3745.0000 do icanreach do dlsw**. *Quando você usa* este parâmetro, note que os endereços MAC estão apresentados tipicamente no formato hexadecimal (0x4000.3745.0000). Consequentemente uma máscara todas em uma (no binário) é representada pelo número hexadecimal 0xFFFF.FFFF.FFFF.

Está aqui um exemplo de como determinar se um MAC de entrada particular é incluído sob um **comando dlsw icanreach mac-address** já configurado:

1. Comece com um roteador configurado com o comando da **máscara ffff.ffff 0000 do endereço MAC 4000.3745.0000 do icanreach do dlsw**.
2. Avalie mesmo se o MAC address 4000.3745.0009 da entrada está incluído pelo comando router configuration precedente.
3. Primeiramente, converta o MAC address (4000.3745.0009) e a MÁSCARA configurada (FFFF.FFFF.0000) do hexadecimal à representação binária. As primeiras duas fileiras nesta tabela mostram esta etapa.
4. Então, execute um lógico E uma operação entre aqueles dois números binários, e converta o resultado à representação hexadecimal (4000.3745.0000). O resultado desta operação é descrito na terceira fileira desta tabela.
5. Se o resultado do E da operação combina o MAC address no **comando dlsw icanreach mac-address** (em nosso exemplo, 4000.3745.0000), a seguir o MAC address da entrada (4000.3745.0009) está permitido pelo **comando dlsw icanreach mac-address**. Em nosso exemplo, todo o MAC address da entrada dentro da escala 4000.3745.0000 a 4000.3745.FFFF é incluído pelo **comando dlsw icanreach mac-address**. Você pode verificar este repetindo as mesmas etapas para todos os endereços MAC nesta escala.

Estes são alguns mais exemplos:

- **máscara ffff.ffff.ffff do endereço MAC 4000.3745.0000 do icanreach do dlsw — Este comando** inclui somente o MAC address 4000.3745.0000. Nenhum outro endereço MAC passa esta máscara.
- **máscara ffff.0000.ffff do endereço MAC 4000.0000.3745 do icanreach do dlsw** — Este comando inclui todos os endereços MAC na escala onde o é 0x0000-0xFFFF.

## Configurar o icanreach do dlsw MAC-exclusivo no roteador central

Com o **comando dlsw icanreach mac-exclusive** configurado no roteador central, você assegura-se de que somente os pacotes destinados aos endereços MAC definidos previamente (neste caso 4000.3745.0000) estejam permitidos no local central.

Note que esta informação de filtragem está trocada entre todos os pares do DLSw+ que usam mensagens capexid. Você salvar a largura de banda de WAN configurando a informação de filtragem no local central, mesmo que as ações (tais como a obstrução de quadros) ocorram nos

roteadores remotos eles mesmos.

| CARACAS | SAO PAULO |
|---|---|
| Current configuration:<br>!<br>hostname CARACAS<br>!<br>dlsw local-peer peer-id 1.1.1.2<br>dlsw remote-peer 0 tcp 1.1.1.1<br>dlsw bridge-group 1<br>!<br>interface Ethernet0/0<br>no ip directed-broadcast<br>bridge-group 1<br>!<br>interface Serial0/1<br>ip address 1.1.1.2 255.255.255.0<br>no ip directed-broadcast<br>!<br>bridge 1 protocol ieee<br>!<br>end | Current configuration:<br>!<br>hostname SAOPAULO<br>!<br>source-bridge ring-group 3<br>dlsw local-peer peer-id 1.1.1.1<br>dlsw remote-peer 0 tcp 1.1.1.2<br>**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 |

Observe nesta saída que o roteador de Caracas sabe que o MAC address 4000.3745.0000 é alcançável através do par 1.1.1.1. A diferença entre este exemplo e o cenário anterior é que aqui nós mostramos o “icanreach MAC-exclusivo: sim”, assim que significa que os escritórios remotos não enviam quadros para o roteador central a não ser aqueles destinado para 4000.3745.0000.

CARACAS#**show dlsw capabilities** DLSw: Capabilities for peer 1.1.1.1(2065) vendor id (OUI) : '00C' (cisco) version number : 2 release number : 0 init pacing window : 20 unsupported saps : none num of tcp sessions : 1 loop prevent support : no **icanreach mac-exclusive : yes** icanreach netbios-excl. : no **reachable mac addresses : 4000.3745.0000 <mask ffff.ffff.ffff>** reachable netbios names : none V2 multicast capable : yes DLSw multicast address : none cisco version number : 1 peer group number : 0 peer cluster support : no border peer capable : no peer cost : 3 biu-segment configured : no UDP Unicast support : yes Fast-switched HPR supp. : no NetBIOS Namecache length : 15 local-ack configured : yes priority configured : no cisco RSVP support : no configured ip address : 1.1.1.1 peer type : conf version string : Cisco Internetwork Operating System Software IOS (tm) C2600 Software (C2600-JK2O3S-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2) Copyright (c) 1986-1999 by cisco Systems, Inc.

O resultado do debug aqui mostra como o roteador de Caracas reage ao tráfego de entrada destinado a todo o MAC address a não ser 4000.3745.0000 (4000.3745.0080 são usados aqui). Caracas não usa Sao Paulo para os quadros não destinados ao host (4000.3745.0000). Neste caso, Sao Paulo é o único peer remoto configurado em Caracas, assim que este roteador não tem nenhum outro par a que para o enviar.

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 você configura um roteador com o **comando dlsw icanreach mac-exclusive** sem definir nenhum MAC address usando o **comando dlsw icanreach mac-address**, o roteador anuncia a seus pares que pode não alcançar nenhum endereço MAC de todo. Consequentemente você perderá uma comunicação através desse par.

**Nota:** A configuração de exemplo aqui é mostrada somente como um exemplo. É um erro e **não deve ser usado**.

| SAO PAULO |
| --- |
| Current configuration:<br>!<br>hostname SAOPAULO<br>!<br>source-bridge ring-group 3<br>dlsw local-peer peer-id 1.1.1.1<br>dlsw remote-peer 0 tcp 1.1.1.2<br>**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 |

Este **resultado do debug** indica o que acontece no roteador de Caracas quando recebe um quadro destinado a 4000.3745.0000. Note que Caracas tem somente um remoto-par de DLSw (Sao Paulo), mas na configuração precedente, Sao Paulo indicou a seus pares que não pode alcançar nenhuns endereços 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
```

## Configurar o endereço MAC do dlsw nos roteadores remotos

Neste exemplo, cada roteador da sede remoto manualmente é configurado e dirigido ao roteador central desejado ao procurar endereços específicos MAC. Isto reduz o tráfego desnecessário que vai ao peer errado. Se o escritório remoto tem somente um peer remoto configurado, a seguir esta configuração não é benéfica. Contudo, se os peeres remotos múltiplos são configurados, esta configuração dirige o roteador de site remoto ao local correto sem desperdiçar a largura de banda de WAN.

Um peer remoto novo do DLSw+ (2.2.2.1) é configurado no roteador de Caracas.

| CARACAS | SAO PAULO |
| --- | --- |
| Current configuration:<br>!<br>hostname CARACAS<br>!<br>dlsw local-peer peer-id 1.1.1.2<br>dlsw remote-peer 0 tcp 1.1.1.1<br>**dlsw remote-peer 0 tcp 2.2.2.1**<br>**dlsw mac-addr 4000.3745.0000** | Current configuration:<br>!<br>hostname SAOPAULO<br>!<br>source-bridge ring-group 3<br>dlsw local-peer peer-id 1.1.1.1 |

| | |
|---|---|
| **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 remote-peer 0 tcp 1.1.1.2<br>!<br>interface TokenRing0/0<br> no ip directed-broadcast<br> ring-speed 16<br> source-bridge 10 1 3<br> source-bridge spanning<br>!<br>interface Serial1/0<br> ip address 1.1.1.1 255.255.255.0<br> no ip directed-broadcast<br> no ip mroute-cache<br> clockrate 32000<br>!<br>end |

Começando com uma tabela de alcançabilidade vazia no roteador de Caracas, note que a entrada para o FEP está no status 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 o primeiro pacote chegar procurando o FEP, simplesmente os pacotes a espreitar 1.1.1.1 (Sao Paulo) estão enviados e não a 2.2.2.1. Consequentemente, você salvar a largura de banda de WAN e os recursos do CPU nos outros pares.

```
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
```

## Configurar o telecontrole MAC-exclusivo do icanreach do dlsw no roteador central

Neste momento, o diagrama da rede e os requisitos de projeto são mudados. Este é o exemplo de rede novo:

Neste exemplo, um dispositivo novo SNA (4000.3746.0000) é adicionado no lugar de Sao Paulo. Esta máquina precisa de estabelecer uma comunicação com um dispositivo em um outro lugar (par 3.3.3.1). O roteador de Sao Paulo executa esta configuração.

| SAO PAULO |
|---|
| Current configuration:<br>!<br>hostname SAOPAULO<br>!<br>source-bridge ring-group 3<br>dlsw local-peer peer-id 1.1.1.1<br>dlsw remote-peer 0 tcp 1.1.1.2<br>**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
```

Com esta configuração de Sao Paulo, o roteador de Sao Paulo informa todos seus pares que, devido ao **comando mac-exclusive**, pode somente alcançar o MAC address 4000.3745.0000. Segundo as indicações deste **resultado do debug**, isto igualmente impede que o dispositivo novo SNA (4000.3746.0000) estabeleça uma comunicação com o 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
```

Para fixar isto, faça estas mudanças à configuração 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
```

Com a palavra-chave **remota**, os outros dispositivos no roteador central são permitidos (que não são especificados no **comando dlsw icanreach mac-address**) fazer conexões de saída. Este é o **resultado do debug em** Sao Paulo quando o dispositivo 4000.3746.0000 começou sua conexão.

```
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
```

# Informações Relacionadas

- Página de suporte de DLSw
- Guia de design DLSw+
- Guia de Troubleshooting do DLSw+
- Entendendo as listas de controle de acesso ao ponto de acesso de serviço