

Методы фильтрации DLSw+ SAP/MAC

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка для технологий фильтрации DLSw+ SAP](#)

[Схема сети](#)

[Настройте выходные списки доступа LSAP в удаленных офисах](#)

[Настройте dlsw icannotreach saps в Центральном маршрутизаторе](#)

[Настройте соки dlsw icanreach в Центральном маршрутизаторе](#)

[Способы фильтрации DLSw+ MAC](#)

[Настройте mac-address dlsw icanreach в Центральном маршрутизаторе](#)

[Настройте монопольный Mac dlsw icanreach в Центральном маршрутизаторе](#)

[Настройте mac-address dlsw в Удаленных маршрутизаторах](#)

[Настройте монопольный Mac dlsw icanreach, удаленный в Центральном маршрутизаторе](#)

[Дополнительные сведения](#)

Введение

Этот документ предоставляет примеры конфигурации для коммутации соединения передачи данных плюс (DLSw+) способы фильтрации по MAC-адресам и Точка доступа к сервису (SAP).

Фильтрация может использоваться для улучшения масштабируемости сети DLSw+. Например, можно использовать фильтрацию для:

- Уменьшите трафик через канал WAN (особенно важный на очень низкоскоростных соединениях и в средах с NetBIOS).
- Улучшите безопасность сети путем управления доступом к определенным устройствам.
- Улучшите Производительность ЦПУ и масштабируемость маршрутизаторов DLSw+ центра обработки данных.

DLSw+ предлагает несколько опций, которые могут использоваться для выполнения фильтрации. Фильтрация может быть сделана на MAC-адресах, SAP или Именах NETBIOS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.](#)

Настройка для технологий фильтрации DLSw+ SAP

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: [Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" \(Поиск команд\) \(только для зарегистрированных клиентов\).](#)

Использование топологии сети, изображенной в разделе [Диаграммы сети](#), требование должно остановить весь Трафик NetBIOS в удаленных местоположениях от достижения Центрального маршрутизатора (Сан-Паулу). DLSw+ предлагает несколько опций для выполнения этой задачи, которые проанализированы в следующих разделах.

Примечание: Трафик NetBIOS использует значения SAP 0xF0 (для команд) и 0xF1 (для ответов). Как правило, администраторы сети используют вышеупомянутые значения SAP для фильтрации (примите или запретите), этот протокол.

Примечание: Клиенты NetBIOS используют NetBIOS функциональный MAC-адрес (C000.0000.0080) как MAC - адрес назначения (DMAC) на их Пакетах запроса Имени NETBIOS. Как отмечалось ранее, все кадры имеют значения SAP 0xF0 или 0xF1.

Для этого теста ПК CCSpсC настроен для соединения с MAC-адресом FEP с помощью SAP 0xF0. В действительности этот трафик выглядит одинаково как NetBIOS, по крайней мере с точки зрения SAP. Когда этот трафик поступает, Поэтому можно наблюдать соответствующие отладки в маршрутизаторе DLSw+.

Схема сети

Этот раздел использует сетевую установку, показанную в этой схеме.

В схеме сети маршрутизатор ЦОД (Сан-Паулу) изображен с соединением с мейнфреймом. Этот маршрутизатор получает множественные одноранговые соединения DLSw+ от всех удаленных ответвлений. Каждое удаленное ответвление имеет и Системную сетевую архитектуру (SNA) и Клиентов NetBIOS. Нет никаких Серверов NetBIOS в ЦОД, к которому нужно обратиться из удаленных офисов.

Для простоты показывают элементы конфигурации только одного удаленного офиса (Каракас). Схема сети также показывает значение MAC-адреса препроцессора (FEP) и

удаленного ПК, названного CCSpC. MAC-адреса показывают и в каноническом (Ethernet) и в неканонический (Token Ring) формат.

Настройте выходные списки доступа LSAP в удаленных офисах

Использование этого метода, все удаленные офисы должны быть настроены с опцией **lsap-output-list**. Никакие другие изменения конфигурации не требуются в центральном маршрутизаторе.

Lsap-output-list связывается со списком доступа SAP (ACL SAP), который в настоящее время только позволяет, что SNA SAP (например, 0x00, 0x04, 0x08, и так далее) для движения к центральному маршрутизатору, и запрещает все остальное. См. [Понимание Списков контроля доступа Точки доступа к сервису](#) для получения дополнительной информации о то, как выполнить фильтрацию на основе, SAP.

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

Команда debug dlsw используется, чтобы видеть, как Маршрутизатор Caracas реагирует, когда это получает Трафик 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
          
```

Если удаленный офисный маршрутизатор (Каракас) не имеет информации о доступности для 4000.3745.0000, и это получает проводник, который ищет тот MAC-адрес с помощью некоторых "запрещенных", SAP, то запрос заблокирован.

```

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

Рассмотрите случай, где удаленный офисный маршрутизатор (Каракас) действительно имеет информацию о доступности для 4000.3745.0000. Например, другая станция (использующий позволенный SAP), уже попросивший MAC - адреса коммуникационного процессора (FEP). В этой ситуации ПК "преступника" (CCSpC) передает свой ПУСТОЙ ПАКЕТ XID, но маршрутизатор останавливает его.

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.Reg 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
```

[Настройте dlsw icannotreach saps в Центральном маршрутизаторе](#)

Использование команды **dlsw icannotreach saps** позволяет вам фильтровать те протоколы, которые вы знаете, не позволены быть переданным через. Если вы знаете только, что должно быть явно запрещено, использовать команду **dlsw icannotreach saps** на центральном маршрутизаторе (маршрутизаторах), как показано в этих конфигурациях.

КАРАКАС	Сан-Паулу
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

Можно настроить центральный маршрутизатор (включайте команду **dlsw icannotreach saps**),

на лету, даже когда удаленные узлы подключены уже. Эти выходные данные показывают отладку на одном из удаленных маршрутизаторов, который указывает на прием Сообщения saraxid. Это сообщение дает удаленным офисам команду не передавать любые кадры с SAP 0xF0/F1 к центральному маршрутизатору.

```
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
```

После того, как Сообщение saraxid получено, Маршрутизатор Caracas узнает, что Сан-Паулу не поддерживает 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-JK203S-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2) Copyright (c) 1986-1999 by cisco Systems, Inc.
```

Выходные данные команды show, отображенные здесь, взяты в центральном маршрутизаторе, показывают изменение конфигурации, где не поддерживается SAP 0xF0.

```
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-JK203S-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2) Copyright (c) 1986-1999 by cisco Systems, Inc.
```

Когда станция ПК NetBIOS делает попытку соединения, это - выходные данные отладки от Маршрутизатора Caracas:

```
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
```

[Настройте соки dlsw icanreach в Центральном маршрутизаторе](#)

Настройка команда dlsw icanreach saps полезна, когда вы знаете точно, какой трафик позволен и вы хотите удостовериться, что запрещен весь другой трафик. Например, при

настройке **dlsw icanreach saps 4** вы явно запрещаете все соки кроме 0x04 (и 0x05, ответ).

КАРАКАС	Сан-Паулу
<pre>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</pre>	<pre>Current configuration: ! hostname SAOPAULO ! source-bridge ring-group 3 dlsw local-peer peer-id 1.1.1.1 dlsw remote-peer 0 tcp 1.1.1.2 dlsw icanreach sap 0 4 ! interface TokenRing0/0 no ip directed-broadcast ring-speed 16 source-bridge 10 1 3 source- bridge spanning ! interface Serial1/0 ip address 1.1.1.1 255.255.255.0 no ip directed- broadcast no ip mroute-cache clockrate 32000 ! end</pre>

Обратите внимание в этих **выходных данных команды show**, что Маршрутизатор Caracas распознает, что Сан-Паулу только поддерживает кадры, предназначенные к сокам 0x04 и 0x05. Все другие соки являются неподдерживаемыми.

```
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.
```

Можно использовать команду **show dlsw capabilities local**, чтобы проверить, что изменения конфигурации в центральном маршрутизаторе появляются в коде 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
```

Способы фильтрации DLSw+ MAC

Использование [схемы сети](#), показанной в этом документе, заставьте центральный маршрутизатор принять кадры, предназначенные к MAC - адресу коммуникационного процессора (FEP) (4000.3745.0000) только.

Настройте mac-address dlsw icanreach в Центральном маршрутизаторе

Использование команды **dlsw icanreach mac-address**, все удаленные офисы имеют запись на своей таблице достижимости DLSw+ для MAC-адреса узла, который указывает к IP-адресу центрального маршрутизатора. Эта запись находится в состоянии UNCONFIRM, которое указывает, что, если удаленный офисный маршрутизатор получает локальный тест или XID для хоста, это передает CUR_ex (Может У Достигать Проводника), сообщение к центральному маршрутизатору только.

КАРАКАС	Сан-Паулу
<pre>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</pre>	<pre>Current configuration: ! hostname SAOPAULO ! source-bridge ring-group 3 dlsw local-peer peer-id 1.1.1.1 dlsw remote-peer 0 tcp 1.1.1.2 dlsw icanreach mac-address 4000.3745.0000 mask ffff.ffff.ffff ! interface TokenRing0/0 no ip directed-broadcast ring-speed 16 source-bridge 10 1 3 source-bridge spanning ! interface Serial1/0 ip address 1.1.1.1 255.255.255.0 no ip directed-broadcast no ip mroute-cache clockrate 32000 ! end</pre>

Здесь, Маршрутизатор Caracas создал постоянное значение в своем кэше доступности. Если запись не нова, состояние является UNCONFIRM. См. [Раздел Достижимость Руководства по поиску и устранению проблем DLSw+](#), для получения дополнительной информации о как MAC-адреса кэша маршрутизаторов DLSw+ и Имена NETBIOS.

```
CARACAS#show dlsw reachability DLSw Local MAC address reachability cache list Mac Addr status
Loc. port rif 0000.8888.0000 FOUND LOCAL TBridge-001 --no rif-- DLSw Remote MAC address
reachability cache list Mac Addr status Loc. peer 4000.3745.0000 UNCONFIRM REMOTE 1.1.1.1(2065)
DLSw Local NetBIOS Name reachability cache list NetBIOS Name status Loc. port rif DLSw Remote
NetBIOS Name reachability cache list NetBIOS Name status Loc. peer
```

Выходные данные команды **show dlsw capabilities** на Маршрутизаторе Caracas подтверждают, что этот удаленный офис знает, что MAC-адрес 4000.3745.0000 достижим через узел 1.1.1.1. Также обратите внимание на линию, которая говорит "icanreach

монопольный Mac: нет. это указывает, что центральный маршрутизатор способен к достижению других MAC-адресов помимо хоста. Поэтому, если какой-либо из удаленных офисов ищет другой MAC-адрес, они могут отправить свои запросы к центральному маршрутизатору. Однако с включением команды **icanreach mac-address 4000.3745.0000**, все удаленные ответвления знают о местоположении этого важного ресурса. Если вы хотите установить дальнейшие ограничения для того, какие кадры поступают в центральный маршрутизатор, обратитесь для [Настройки монопольного Mac dlsw icanreach в Центральном маршрутизаторе](#).

```
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.
```

Можно использовать параметр маски в качестве **mac-address dlsw icanreach 4000.3745.0000 масок ffff.ffff.ffff**. При использовании этого параметра обратите внимание, что MAC-адреса, как правило, представляются в шестнадцатеричном формате (0x4000.3745.0000). Поэтому маска "все единицы" (в двоичных файлах) представлена шестнадцатеричным числом 0xFFFF.FFFF.FFFF.

Вот пример того, как определить, включен ли определенный указанный MAC - адрес при уже настроенной команде **dlsw icanreach mac-address**:

1. Запустите с маршрутизатора, настроенного с **mac-address dlsw icanreach 4000.3745.0000 масок ffff.ffff 0000** команд.
2. Оцените, включен ли адрес указанного MAC - адреса 4000.3745.0009 предыдущей командой конфигурации маршрутизатора.
3. Во-первых, преобразуйте MAC-адрес (4000.3745.0009) и настроенную МАСКУ (FFFF.FFFF.0000) от шестнадцатеричного до двоичного отображения. Первые две строки в этой таблице показывают этот шаг.
4. Затем выполните логическую операцию И между теми двумя двоичными числами и преобразуйте результат в шестнадцатеричное представление (4000.3745.0000). Результат этой операции изображен в третьей строке этой таблицы.
5. Если результат операции И совпадает с MAC-адресом в команде **dlsw icanreach mac-address** (в нашем примере, 4000.3745.0000), то адрес указанного MAC - адреса (4000.3745.0009) **позволен командой dlsw icanreach mac-address**. В нашем примере, любом адресе указанного MAC - адреса в диапазоне 4000.3745.0000 к 4000.3745. FFFF включен **командой dlsw icanreach mac-address**. Можно проверить это путем повторения тех же шагов для любых MAC-адресов в этом диапазоне.

Это еще несколько примеров:

- **mac-address dlsw icanreach 4000.3745.0000 масок ffff.ffff.ffff** — Эта команда только включает MAC-адрес 4000.3745.0000. Никакие другие MAC-адреса не передают эту маску.
- **mac-address dlsw icanreach 4000.0000.3745 маски ffff.0000.ffff** — Эта команда включает все MAC-адреса в диапазон 4000. XXXX.3745, где XXXX 0x0000-0xFFFF.

Настройте монопольный Mac dlsw icanreach в Центральном маршрутизаторе

С командой `dlsw icanreach mac-exclusive`, настроенной в центральном маршрутизаторе, вы гарантируете, что только пакеты, предназначенные к MAC-адресам, ранее определенным (в этом случае 4000.3745.0000), позволены в центральном месте расположения.

Обратите внимание на то, что этой отфильтрованной информацией обмениваются между всеми узлами DLSw+ с помощью Сообщений sarxid. Вы сохраняете полосу пропускания глобальной сети (WAN) путем настройки отфильтрованной информации в центральном месте расположения, даже при том, что действия (такие как блокирование кадров) происходят в самих удаленных маршрутизаторах.

КАРАКАС	Сан-Паулу
<pre>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</pre>	<pre>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 ! 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</pre>

Заметьте в этих выходных данных, что Маршрутизатор Caracas знает, что MAC-адрес 4000.3745.0000 достижим через узел 1.1.1.1. Различие между данным примером и предыдущим сценарием - то, что здесь мы показываем "icanreach монопольный Mac: да", что означает, что удаленные офисы не передают кадры к центральному маршрутизатору кроме предназначенных для 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.
```

Выходные данные отладки здесь показывают, как Маршрутизатор Caracas реагирует на

входящий трафик, предназначенный к любому MAC-адресу кроме 4000.3745.0000 (4000.3745.0080, используется здесь). Каракас не использует Сан-Паулу для кадров, не предназначенных к хосту (4000.3745.0000). В этом случае Сан-Паулу является единственным удаленным узлом, настроенным в Каракасе, таким образом, этот маршрутизатор не имеет никакого другого узла, к которому можно передать его.

```
CARACAS#debug dls w 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
```

При настройке маршрутизатора с командой **dls w icanreach mac-exclusive**, не определяя MAC-адреса с помощью команды **dls w icanreach mac-address** маршрутизатор дает объявление к его узлам, что это не может достигнуть никаких MAC-адресов вообще. Поэтому вы потеряете связь через тот узел.

Примечание: Пример конфигурации здесь показывают только как пример. Это - ошибка и не должно использоваться.

Сан-Паулу
Current configuration: ! hostname SAOPAULO ! source-bridge ring-group 3 dls w local-peer peer-id 1.1.1.1 dls w remote-peer 0 tcp 1.1.1.2 dls w 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

Эти выходные данные отладки указывают на то, что происходит в Маршрутизаторе Caracas, когда это принимает кадр, предназначенный к 4000.3745.0000. Обратите внимание на то, что Каракас только имеет один Удаленный узел dls w (Сан-Паулу), но в предыдущей конфигурации, Сан-Паулу указал к его узлам, что это не может достигнуть никаких MAC-адресов.

```
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
```

[Настройте mac-address dls w в Удаленных маршрутизаторах](#)

В данном примере каждый удаленный офисный маршрутизатор вручную настроен и направлен к желаемому центральному маршрутизатору при поиске определенных MAC-адресов. Это уменьшает трафик, в котором нет необходимости, который переходит к

неверному одноранговому узлу. Если удаленному офису только настроили один удаленный узел, то эта конфигурация не выгодна. Однако, если несколько удаленных одноранговых узлов настроены, эта конфигурация направляет маршрутизатор удаленного сайта к правильному месту, не тратя впустую полосу пропускания глобальной сети (WAN).

Один новый удаленный узел DLSw+ (2.2.2.1) настроен в Маршрутизаторе Caracas.

КАРАКАС	Сан-Паулу
<pre> 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 </pre>	<pre> Current configuration: ! hostname SAOPAULO ! source-bridge ring- group 3 dlsw local-peer peer-id 1.1.1.1 dlsw remote-peer 0 tcp 1.1.1.2 ! interface TokenRing0/0 no ip directed- broadcast ring-speed 16 source-bridge 10 1 3 source-bridge spanning ! interface Serial1/0 ip address 1.1.1.1 255.255.255.0 no ip directed- broadcast no ip mroute-cache clockrate 32000 ! end </pre>

При начале с пустой таблицы достижимости в Маршрутизаторе Caracas обратите внимание, что запись для FEP находится в статусе 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
          
```

Когда первый пакет поступает, ища FEP, только пакеты для пиринга 1.1.1.1 (Сан-Паулу) переданы а не к 2.2.2.1. Поэтому вы сохраняете полосу пропускания глобальной сети (WAN) и ресурсы ЦПУ на других узлах.

```

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
          
```

[Настройте монопольный Mac dlsw canreach, удаленный в Центральном маршрутизаторе](#)

На этом этапе схема сети и требования к проектированию изменены. Это - новый пример сети:

В данном примере новое устройство SNA (4000.3746.0000) добавлено в местоположении Сан-Паулу. Эта машина должна установить связь с устройством в другом местоположении (взаимодействуйте 3.3.3.1). Маршрутизатор Сан-Паулу выполняет эту конфигурацию.

```
Сан-Паулу
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
```

С этой конфигурацией Сан-Паулу маршрутизатор Сан-Паулу сообщает всем своим узлам, что, из-за **команды mac-exclusive**, это может только достигнуть MAC-адреса 4000.3745.0000. Как показано в этих **выходных данных отладки**, это также предотвращает новое устройство SNA (4000.3746.0000) от установления связи через 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
```

Для решения проблемы этого внесите эти изменения в конфигурацию Сан-Паулу.

```
Сан-Паулу
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
```

С **удаленным** ключевым словом другие устройства в центральном маршрутизаторе **позволены** (которые не заданы в **команде dlsw icanreach mac-address**) сделать исходящие соединения. Когда устройство 4000.3746.0000 запустило свое соединение, это - **выходные данные отладки** на Сан-Паулу.

```
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

[Дополнительные сведения](#)

- [Страница технической поддержки DLSw](#)
- [Руководство по дизайну DLSw+](#)
- [Руководство по поиску и устранению проблем DLSw+](#)
- [Общие сведения о списках управления доступом для точек доступа к службам](#)