Técnicas de filtrado DLSw+ SAP/MAC

Contenido

Introducción

Este documento proporciona las configuraciones de muestra para el punto de acceso de servicio del Data-Link Switching Plus (DLSw+) (SAP) y las técnicas de filtrado MAC.

La filtración se puede utilizar para aumentar el scalability de una red del DLSw+. Por ejemplo, usted puede utilizar la filtración a:

- Reduzca el tráfico a través de un link PÁLIDO (especialmente importante en mismo los links de baja velocidad y en los entornos con el NetBios).
- Aumente la Seguridad de una red controlando el acceso a ciertos dispositivos.
- Aumente el rendimiento de la CPU y el scalability del Routers del DLSw+ del centro de datos.

El DLSw+ ofrece varias opciones que se puedan utilizar para realizar la filtración. La filtración se puede hacer en las direcciones MAC, SAP, o los nombres de NETBIOS.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Configurar para técnicas de filtrado DLSw+ SAP

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes registrados).

Usando la topología de red representada en la sección del diagrama de la red, el requisito es parar todo el tráfico de NETBIOS en los lugares remotos de alcanzar al router central (Sao Paulo). El DLSw+ ofrece varias opciones para lograr esta tarea, que se analizan en las secciones siguientes.

Nota: El tráfico de NetBIOS usa valores SAP 0xF0 (para comandos) y 0xF1 (para respuestas). Típicamente, los administradores de la red utilizan los valores antedichos de SAP para filtrar (valide o niegue) este protocolo.

Nota: Los clientes NetBIOS utilizan la dirección MAC funcional del NetBios (C000.0000.0080) como el MAC de destino (DMAC) en sus paquetes de la interrogación del nombre de NETBIOS. Según lo mencionado anterior, todas las tramas tienen valores de SAP de 0xF0 o de 0xF1.

Para esta prueba, el CCSpcC PC se configura para conectar con la dirección MAC del FEP usando SAP 0xF0. En la realidad este tráfico mira lo mismo que el NetBios, por lo menos de una perspectiva de SAP. Por lo tanto, usted puede observar los debugs correspondientes en el router del DLSw+ cuando llega este tráfico.

Diagrama de la red

Esta sección utiliza la configuración de la red mostrada en este diagrama.

En el diagrama de la red, representan a un router de centro de datos (Sao Paulo) con una conexión a la unidad central. Este router recibe las conexiones de peer múltiples del DLSw+ de todas las sucursales remotas. Cada sucursal remota tiene la Arquitectura de red de sistemas (SNA) y los clientes NetBIOS. No hay servidores de NetBIOS en el centro de datos que necesitan conseguir accedidos de las oficinas remotas.

Para la simplicidad, los detalles de la configuración de solamente una oficina remota (Caracas) se muestran. El diagrama de la red también muestra el valor de la dirección MAC del Procesador frontal (FEP) y de la PC remota llamados CCSpcC. Las direcciones MAC se muestran en el formato canónico (los Ethernetes) y no canónico (del Token Ring).

Listas de acceso a los resultados de LSAP de la configuración en las oficinas remotas

Usando este método, todas las oficinas remotas se deben configurar con la opción del **lsap-output-list**. No se requiere ningunos otros cambios de configuración en el router central.

El lsap-output-list enlaza a SAP una lista de acceso (SAP ACL) que permite actualmente solamente que las savias SNA (por ejemplo, 0x00, 0x04, 0x08, y así sucesivamente) vayan hacia el router central, y niega todo lo demás. Refiera comprensión de las listas de control de acceso del punto de acceso de servicio para más información sobre cómo realizar la filtración basada en las savias.

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

Utilizan al **comando debug dlsw** de considerar cómo el router Caracas reacciona cuando recibe el tráfico 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
```

Si el router de oficina remota (Caracas) no tiene la información de alcance para 4000.3745.0000, y la consigue a un explorador que busque que la dirección MAC usando algo de “prohibió” las savias, después se bloquea la petición.

```
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 el caso donde el router de oficina remota (Caracas) tiene información de alcance para 4000.3745.0000. Por ejemplo, otra estación (usando las savias permitidas) pidió ya el FEP MAC

Address. En esta situación que el “delincuente” PC (CCSpcC) envía su XID NULO, pero al router lo para.

```
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
```

Savias del icannotreach del dlsw de la configuración en el router central

Usando el **comando dlsw icannotreach saps** permite que usted filtre esos protocolos que usted sabe no se permite ser enviado a través. Si usted conoce solamente qué debe ser negada explícitamente, utilice el **comando dlsw icannotreach saps** en el router central, tal y como se muestra en de estas configuraciones.

CARACAS	SAO PAULO
Current configuration: ! hostname CARACAS ! dlsw local-peer peer-id 1.1.1.2 dlsw remote-peer 0 tcp 1.1.1.1 dlsw bridge-group 1 ! interface Ethernet0/0 no ip directed-broadcast bridge-group 1 ! interface Serial0/1 ip address 1.1.1.2 255.255.255.0 no ip directed-broadcast ! bridge 1 protocol ieee ! end	Current configuration: ! hostname SAOPAULO ! source-bridge ring-group 3 dlsw local-peer peer-id 1.1.1.1 dlsw remote-peer 0 tcp 1.1.1.2 **dlsw icannotreach sap F0** ! interface TokenRing0/0 no ip directed-broadcast ring-speed 16 source-bridge 10 1 3 source-bridge spanning ! interface Serial1/0 ip address 1.1.1.1 255.255.255.0 no ip directed-broadcast no ip mroute-cache clockrate 32000 ! end

Usted puede configurar al router central (incluya el **comando dlsw icannotreach saps**) simultáneamente, incluso cuando los peeres remotos están ya para arriba. Esta salida muestra el debug en uno de los routeres remotos, que indica la recepción del mensaje CapExId. Este mensaje da instrucciones las oficinas remotas para no enviar ningunas tramas con SAP 0xF0/F1 hacia el router 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
```

Después de que mensaje CapExId se reciba, el router Caracas aprende que Sao Paulo no soporta SAP 0xF0.

```
CARACAS#show dlsw capabilities DLSw: Capabilities for peer 1.1.1.1(2065) vendor id (OUI) : '00C'
(cisco) version number : 2 release number : 0 init pacing window : 20 unsupported saps : F0 num
of tcp sessions : 1 loop prevent support : no icanreach mac-exclusive : no icanreach netbios-
excl. : no reachable mac addresses : none reachable netbios names : none V2 multicast capable :
yes DLSw multicast address : none cisco version number : 1 peer group number : 0 peer cluster
support : no border peer capable : no peer cost : 3 biu-segment configured : no UDP Unicast
support : yes Fast-switched HPR supp : no NetBIOS Namecache length : 15 local-ack configured :
yes priority configured : no cisco RSVP support : no configured ip address : 1.1.1.1 peer type :
conf version string : Cisco Internetwork Operating System Software IOS (tm) C2600 Software
(C2600-JK2O3S-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2) Copyright (c) 1986-1999 by cisco
Systems, Inc.
```

La salida del comando show visualizada aquí, tomado en el router central, muestra a cambio de configuración donde SAP 0xF0 no se soporta.

```
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.
```

Ésta es la **salida de los debugs del** router Caracas cuando la estación del NetBios PC intenta la conexión:

```
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
```

Savias del icanreach del dlsw de la configuración en el router central

Configurar el **comando dlsw icanreach saps** es útil cuando usted conoce que exactamente lo que no prohiben el tipo de tráfico y usted quiere aseegurarse que el resto del tráfico está negado. Por ejemplo, cuando usted configura el **dlsw icanreach saps 4**, usted niega explícitamente todas las savias excepto 0x04 (y 0x05, la respuesta).

CARACAS	SAO PAULO
Current configuration:	Current configuration:

```
!
hostname CARACAS
!
dlsw local-peer peer-id
1.1.1.2
dlsw remote-peer 0 tcp
1.1.1.1
dlsw 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
```

```
!
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
```

Observe en esta **salida del comando show** que el router Caracas reconoce que Sao Paulo soporta solamente las tramas destinadas a las savias 0x04 y 0x05. El resto de las savias están sin apoyo.

```
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.
```

Usted puede utilizar el **comando show dlsw capabilities local** de verificar que los cambios de configuración en el router central aparecen en el código del 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 filtrado DLSw+ MAC

Usando el diagrama de la red mostrado en este documento, haga que el router central recibe las tramas destinadas al FEP MAC Address (4000.3745.0000) solamente.

Configure el MAC address del icanreach del dlsw en el router central

Usando el **comando dlsw icanreach mac-address**, todas las oficinas remotas tienen una entrada en su tabla de alcance del DLSw+ para la dirección MAC del host esas puntas a la dirección IP del router central. Esta entrada está en el estado UNCONFIRM, que indica que si el router de oficina remota recibe una prueba local o un XID para el host, él envía un mensaje de CUR_ex (puede el explorador del alcance U) al router central solamente.

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

Aquí, el router Caracas ha creado una Entrada permanente en su memoria caché de alcance. Si la entrada no está fresca, el estado es UNCONFIRM. Refiera al capítulo de alcance del guía de Troubleshooting del DLSw+ para más información sobre cómo el Routers del DLSw+ oculta las direcciones MAC y los nombres de NETBIOS.

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

La salida del **comando show dlsw capabilities** en el router Caracas confirma que esta oficina remota sabe que la dirección MAC 4000.3745.0000 es accesible vía el par 1.1.1.1. También observe la línea que dice el “icanreach mac-exclusivo: no”. Indica que el router central es capaz de alcanzar otras direcciones MAC además del host. Por lo tanto, si las oficinas remotas unas de los buscan la otra dirección MAC, pueden enviar sus peticiones al router central. Sin embargo, con la inclusión del **comando icanreach mac-address 4000 3745 0000**, todas las sucursales remotas son conscientes de la ubicación de este recurso importante. Si usted quiere poner otras restricciones en qué tramas llegan el router central, refiera al icanreach del dlsw de la configuración mac-exclusivo en el router 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.
```

Usted puede utilizar el parámetro de la **máscara** como *máscara ffff.ffff.ffff del* **MAC address 4000.3745.0000 del icanreach del dlsw**. *Cuando usted utiliza* este parámetro, observe que las direcciones MAC están presentadas típicamente en el formato hexadecimal (0x4000.3745.0000). Por lo tanto una máscara del todo uno (en el binario) es representada por el número hexadecimal 0xFFFF.FFFF.FFFF.

Aquí está un ejemplo de cómo determinar si un MAC de entrada determinado es incluido bajo **comando dlsw icanreach mac-address** ya configurado:

1. Comience con un router configurado con el comando de la **máscara ffff.ffff 0000 del MAC address 4000.3745.0000 del icanreach del dlsw**.
2. Evalúe independientemente de si la dirección MAC 4000.3745.0009 de la entrada es incluida por el comando router configuration anterior.
3. Primero, convierta la dirección MAC (4000.3745.0009) y la MÁSCARA configurada (FFFF.FFFF.0000) del hexadecimal a la representación binaria. Las primeras dos filas en esta tabla muestran este paso.
4. Entonces, realice un lógico Y una operación entre esos dos números binarios, y convierta el resultado a la representación hexadecimal (4000.3745.0000). El resultado de esta operación se representa en la tercera fila de esta tabla.
5. Si el resultado del Y de la operación hace juego la dirección MAC en el **comando dlsw icanreach mac-address** (en nuestro ejemplo, 4000.3745.0000), después la dirección MAC de la entrada (4000.3745.0009) es permitida por el **comando dlsw icanreach mac-address**. En nuestro ejemplo, cualquier dirección MAC de la entrada dentro del rango 4000.3745.0000 a 4000.3745.FFFF es incluida por el **comando dlsw icanreach mac-address**. Usted puede verificar esto relanzando los mismos pasos para cualquier dirección MAC en este rango.

Éstos son algunos más ejemplos:

- **máscara ffff.ffff.ffff del MAC address 4000.3745.0000 del icanreach del dlsw — Este comando** incluye solamente la dirección MAC 4000.3745.0000. Ningunas otras direcciones MAC pasan esta máscara.
- **máscara ffff.0000.ffff del MAC address 4000.0000.3745 del icanreach del dlsw** — Este comando incluye todas las direcciones MAC en el rango donde está 0x0000-0xFFFF el.

Icanreach del dlsw de la configuración mac-exclusivo en el router central

Con el **comando dlsw icanreach mac-exclusive** configurado en el router central, usted se asegura de que solamente los paquetes destinados a las direcciones MAC definidas previamente (en este caso 4000.3745.0000) están permitidos en la ubicación central.

Observe que este filtrado de información está intercambiado entre todos los pares del DLSw+ que usan los mensajes de CapExId. Usted salva el ancho de banda WAN configurando el filtrado de

información en la ubicación central, aunque las acciones (tales como bloqueo de las tramas) ocurren en los routeres remotos ellos mismos.

CARACAS	SAO PAULO
Current configuration: ! hostname CARACAS ! dlsw local-peer peer-id 1.1.1.2 dlsw remote-peer 0 tcp 1.1.1.1 dlsw bridge-group 1 ! interface Ethernet0/0 no ip directed-broadcast bridge-group 1 ! interface Serial0/1 ip address 1.1.1.2 255.255.255.0 no ip directed-broadcast ! bridge 1 protocol ieee ! end	Current configuration: ! hostname SAOPAULO ! source-bridge ring-group 3 dlsw local-peer peer-id 1.1.1.1 dlsw remote-peer 0 tcp 1.1.1.2 **dlsw icanreach mac-exclusive dlsw icanreach mac-address 4000.3745.0000 mask ffff.ffff.ffff**f ! interface TokenRing0/0 no ip directed-broadcast ring-speed 16 source-bridge 10 1 3 source-bridge spanning ! interface Serial1/0 ip address 1.1.1.1 255.255.255.0 no ip directed-broadcast no ip mroute-cache clockrate 32000 ! end

Observe en esta salida que el router Caracas sabe que la dirección MAC 4000.3745.0000 es accesible vía el par 1.1.1.1. La diferencia entre este ejemplo y el escenario previó es que aquí mostramos el “icanreach mac-exclusivo: sí”, así que significa que las oficinas remotas no envían las tramas hacia el router central con excepción de ésas 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.

La salida de los debugs aquí muestra cómo el router Caracas reacciona al tráfico entrante destinado a cualquier dirección MAC con excepción de 4000.3745.0000 (4000.3745.0080 se utiliza aquí). Caracas no utiliza Sao Paulo para las tramas no destinadas al host (4000.3745.0000). En este caso, Sao Paulo es el único peer remoto configurado en Caracas, así que este router no tiene ningún otro par a quien enviarla.

CARACAS#**debug dlsw** DLSw reachability debugging is on at event level for all protocol traffic DLSw peer debugging is on DLSw local circuit debugging is on DLSw core message debugging is on DLSw core state debugging is on DLSw core flow control debugging is on DLSw core xid debugging is on *Mar 1 22:41:33.200: DLSW Received-ctlQ : CLSI Msg : TEST_STN.Ind dlen: 40 *Mar 1 22:41:33.204: CSM: Received CLSI Msg : TEST_STN.Ind dlen: 40 from DLSw Port0 *Mar 1 22:41:33.204: CSM: smac 0000.8888.0000, **dmac 4000.3745.0080**, ssap 4 , dsap 0 *Mar 1 22:41:33.204: **broadcast filter failed mac check** *Mar 1 22:41:33.204: **CSM: Write to all peers not**

ok - PEER_NO_CONNECTIONS

Si usted configura a un router con el **comando dlsw icanreach mac-exclusive** sin la definición de ninguna dirección MAC usando el **comando dlsw icanreach mac-address**, el router hace publicidad a sus pares que no puede alcanzar ninguna dirección MAC en absoluto. Por lo tanto usted perderá la comunicación a través de ese par.

Nota: La configuración de muestra aquí se muestra solamente como un ejemplo. Es un error y **no debe ser utilizado**.

SAO PAULO
Current configuration: ! hostname SAOPAULO ! source-bridge ring-group 3 dlsw local-peer peer-id 1.1.1.1 dlsw remote-peer 0 tcp 1.1.1.2 **dlsw icanreach mac-exclusive** ! interface TokenRing0/0 no ip directed-broadcast ring-speed 16 source-bridge 10 1 3 source-bridge spanning ! interface Serial1/0 ip address 1.1.1.1 255.255.255.0 no ip directed-broadcast no ip mroute-cache clockrate 32000 ! end

Esta **salida de los debugs** indica qué sucede en el router Caracas cuando recibe una trama destinada a 4000.3745.0000. Observe que Caracas tiene solamente un telecontrol-par de DLSw (Sao Paulo), pero en la configuración previa, Sao Paulo indicó a sus pares que no puede alcanzar ninguna direcciones 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

MAC address del dlsw de la configuración en los routeres remotos

En este ejemplo, configuran y se dirigen a cada router de oficina remota manualmente al router central deseado al buscar las direcciones MAC específicas. Esto reduce el tráfico innecesario que va al peer incorrecto. Si la oficina remota tiene solamente un peer remoto configurado, después esta configuración no es beneficiosa. Sin embargo, si configuran a los peeres remotos múltiples, esta configuración dirige al router de sitio remoto al lugar correcto sin perder el ancho de banda WAN.

Configuran a un nuevo peer remoto del DLSw+ (2.2.2.1) en el router Caracas.

CARACAS	SAO PAULO
Current configuration: ! hostname CARACAS ! dlsw local-peer peer-id 1.1.1.2 dlsw remote-peer 0 tcp 1.1.1.1	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

Empezando por una tabla de alcance vacía en el router Caracas, observe que la entrada para el FEP está en el estado 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
```

Cuando llega el primer paquete buscando el FEP, sólo los paquetes a mirar 1.1.1.1 (Sao Paulo) se envían y no a 2.2.2.1. Por lo tanto, usted salva el ancho de banda WAN y a los recursos de la CPU en los otros 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
```

Configure el telecontrol mac-exclusivo del icanreach del dlsw en el router central

En este momento, se cambian el diagrama de la red y los requisitos de diseño. Éste es el nuevo ejemplo de red:

En este ejemplo, un nuevo dispositivo SNA (4000.3746.0000) se agrega en la ubicación de Sao Paulo. Esta máquina necesita establecer la comunicación con un dispositivo en otra ubicación (par 3.3.3.1). El router de Sao Paulo funciona con esta configuración.

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

```
dlsw remote-peer 0 tcp 3.3.3.1 dlsw icanreach mac-
exclusive dlsw icanreach mac-address 4000.3745.0000 mask
ffff.ffff.ffff ! interface TokenRing0/0 no ip directed-
broadcast ring-speed 16 source-bridge 10 1 3 source-
bridge spanning ! interface Serial1/0 ip address 1.1.1.1
255.255.255.0 no ip directed-broadcast no ip mroute-
cache clockrate 32000 ! end
```

Con esta configuración de Sao Paulo, el router de Sao Paulo informa a todos sus pares que, debido al **comando mac-exclusive**, pueda solamente alcanzar la dirección MAC 4000.3745.0000. Tal y como se muestra en de esta **salida de los debugs**, esto también evita que el nuevo dispositivo SNA (4000.3746.0000) establezca la comunicación con el 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 reparar esto, realice estos cambios a la configuración 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
```

Con la **palabra clave remota**, los otros dispositivos en el router central se permiten (que no se especifican en el **comando dlsw icanreach mac-address**) hacer las conexiones salientes. Ésta es la **salida de los debugs** en Sao Paulo cuando el dispositivo 4000.3746.0000 comenzó su conexión.

```
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
```

Información Relacionada

- Página de soporte de DLSw
- Guía de diseño de DLSw
- Guía de Troubleshooting del DLSw+
- Cómo funcionan las listas de control de acceso a los puntos de acceso al servicio