

Configuración y solución de problemas de IP MLS en switches Catalyst 6500/6000 con MSFC

Contenido

[Introducción](#)

[Antes de comenzar](#)

[Convenciones](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Información general de MLS en MSFC](#)

[Ejemplo 1: Ruteo de MSFC entre dos VLAN](#)

[Lectura de entradas show mls y verificación básica](#)

[Lectura de tablas de resultados del comando show mls](#)

[Solución de problemas en una conexión específica](#)

[Ejemplo 2: Dos MSFC en el mismo chasis configurado para HSRP](#)

[Activación de comandos show mls](#)

[Ejecución de comandos de entrada show mls](#)

[Consejos de Troubleshooting](#)

[Creación de flujos](#)

[La contabilidad IP excluye el tráfico MLS](#)

[No se puede configurar la máscara de flujo completa de la interfaz](#)

[Información Relacionada](#)

Introducción

Este documento es una guía para la verificación y lectura de comandos de Multilayer Switching (MLS) en el Catalyst 6500/6000. El documento contiene un estudio muy breve sobre qué es MLS, y también ofrece ejemplos de cómo utilizar MLS. Basándose en estos ejemplos, este documento muestra cómo verificar el funcionamiento de MLS y proporciona breves consejos de troubleshooting para configurar MLS.

Este documento se aplica solamente al switch Catalyst 6500/6000 Series equipado con el siguiente hardware:

- Supervisor Engine 1A que ejecuta el software Catalyst OS (CatOS)
- Tarjeta de función de política (PFC)
- Tarjeta de función de switch multicapa (MSFC)

Nota: Este documento no es válido cuando se utiliza cualquier otra configuración de hardware, como Supervisor Engine 2 o Multilayer Switch Module (MSM). Tampoco es válido cuando se ejecuta Cisco IOS® Software tanto en Supervisor Engine 1A como en MSFC.

Para obtener información similar con respecto a la resolución de problemas del ruteo unicast en un Catalyst 6500/6000 Series Switch con Supervisor Engine 2 y que ejecuta el software CatOS, consulte [Solución de Problemas del Ruteo IP Unicast que Involucra CEF en Catalyst 6500/6000 Series Switches con Supervisor Engine 2 y que Ejecuta CatOS System Software](#).

Para una descripción más completa de la terminología y el funcionamiento MLS, consulte la sección Información Relacionada.

Antes de comenzar

Convenciones

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

Prerequisites

No hay requisitos previos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las versiones de software y hardware indicadas a continuación.

- Catalyst 6500/6000 con MSFC

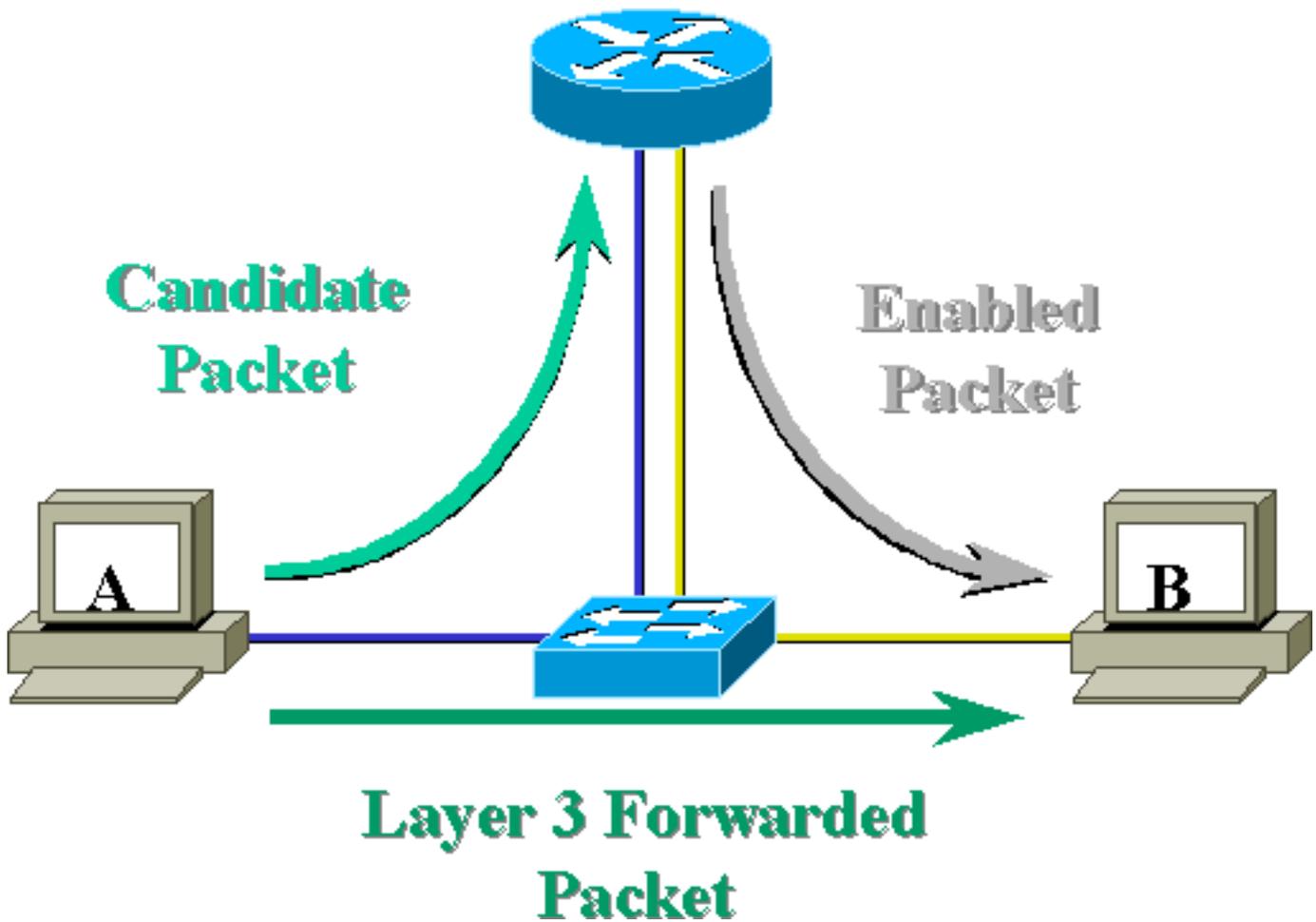
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Información general de MLS en MSFC

El MSFC es el motor de ruteo de segunda generación para el switch Catalyst de la serie 6500/6000 que puede rutear 15 millones de paquetes por segundo. La MSFC sólo funciona con Supervisor Engines que tienen la PFC. La MSFC realiza un MLS interno con la PFC, que actúa de manera similar a la Tarjeta de Función de NetFlow (NFFC) en el Catalyst 5000. Este MLS interno no es visible y se limita exclusivamente al switch: no tiene nada que configurar para que funcione y admite accesos directos de hardware para IP, IPX y multidifusión IP. La configuración de la MSFC es similar a la configuración de un RSM o una RSFC mediante interfaces de VLAN. Puede acceder mediante el uso de la sesión 15 (para MSFC en el Supervisor Engine en la ranura 1) o la sesión 16 (para MSFC en el Supervisor Engine en la ranura 2).

El principio es similar al protocolo de switching multicapa (MLSP) en el Catalyst 5000. El primer paquete es ruteado por la MSFC y la PFC crea un acceso directo que es utilizado por todos los paquetes subsiguientes del mismo flujo. A diferencia de MLSP en el Catalyst 5000, que requiere comunicación IP entre el MLS-SE y el MLS-RP, MLS en el Catalyst 6500/6000 funciona mediante la comunicación entre el MSFC y el PFC a través de un canal serial (SCP).

El PFC no puede ser el MLS-SE para un entorno MLS de Catalyst 5000; sin embargo, la MSFC puede ser MLS-RP para otros Catalyst 5000 en la red. En ese caso, debe configurar la MSFC usando el mismo comando `mls rp ip` que lo haría para cualquier router Cisco IOS utilizado como el RP MLS.



Ejemplo 1: Ruteo de MSFC entre dos VLAN

El MLS en el Catalyst 6500/6000 para IP de unidifusión es plug and play. No es necesario configurarlo. A continuación se muestra una configuración de ejemplo donde **tamer** es un Catalyst 6500/6000, que tiene una MSFC llamada **tamer-msfc**. El ruteo entre VLAN 11 y 12 se configura en la MSFC sin un sólo comando relacionado con MLS. Tenga en cuenta que el Supervisor Engine no tendrá ninguna configuración específica de MLS.

```
tamer-msfc#wr t
Building configuration...

Current configuration:
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname tamer-msfc
!
boot system flash bootflash:c6msfc-ds-mz.121-1.E2.bin
!
ip subnet-zero
ip cef
!
interface Vlan11
 ip address 11.1.1.2 255.255.255.0
```

```

!
interface Vlan12
 ip address 12.1.1.2 255.255.255.0
!
router eigrp 1
 network 11.0.0.0
 network 12.0.0.0
 no auto-summary
!
ip classless
no ip http server
!
!
line con 0
 transport input none
line vty 0 4
 login
!
end

```

Lectura de entradas show mls y verificación básica

A continuación se muestra el resultado que debe obtener al ejecutar el comando **show mls** en el Supervisor Engine.

```

tamer (enable) show mls
Total packets switched = 8
!--- Number of packet shortcut by MLS. Total Active MLS entries = 0 !--- Number of flows
currently existing. MSFC 11.1.1.2 (Module 15) entries = 0 IP Multilayer switching aging time =
256 seconds IP Multilayer switching fast aging time = 0 seconds, packet threshold = 0 IP Current
flow mask is Destination flow Active IP MLS entries = 0 Netflow Data Export version: 7 Netflow
Data Export disabled Netflow Data Export port/host is not configured. Total packets exported = 0
IP MSFC ID Module XTAG MAC Vlans -----
11.1.1.2 15 1 00-d0-d3-9c-9e-3c 12,11 !--- MSFC recognized by the switch.

```

La salida del comando **show mls** siempre debe tener una ID de MSFC IP. Si no ve el ID de MSFC IP cuando ejecuta el comando **show mls**, verifique lo siguiente:

- MSFC está en funcionamiento (por ejemplo, no se bloquea en el modo ROMmon).
- MLS todavía está habilitado en la MSFC.

Puede verificarlo mediante la ejecución de los siguientes comandos en la MSFC:

```

tamer-msfc#show mls status
MLS global configuration status:
global mls ip: enabled
!--- Should be enabled for unicast IP. global mls ipx: enabled global mls ip multicast: disabled
current ip flowmask for unicast: destination only current ipx flowmask for unicast: destination
only

```

Mediante la ejecución del comando **show mls status**, puede determinar si el MLS está habilitado para IP, IPX y multidifusión IP. Estas funciones siempre se deben habilitar de forma predeterminada; sin embargo, pueden inhabilitarse si se ejecuta el siguiente comando en el modo configuración:

```
no mls ip
```

El comando `no mls ip` sólo se debe usar para propósitos de depuración. El comando también está disponible como un comando oculto en el modo de configuración global. También puede inhabilitar MLS en una interfaz por VLAN ejecutando el comando `no mls ip` en el modo de configuración de la interfaz

Nota: No ejecute el comando `show mls rp` en la MSFC. Este resultado del comando indica que MLS está inhabilitado. Sin embargo, el resultado del comando `show mls` ejecutado en el Supervisor Engine arriba indicado indicó que MLS funcionaba correctamente. Esta discrepancia ocurre porque el comando `show mls rp` se debe utilizar cuando se hace MLS-rp junto con un switch Catalyst 5000.

```
tamer-msfc#show mls rp
ip multilayer switching is globally disabled
ipx multilayer switching is globally disabled
ipx mls inbound acl override is globally disabled
mls id is 00d0.d39c.9e04
mls ip address 0.0.0.0
mls ip flow mask is unknown
mls ipx flow mask is unknown
number of domains configured for mls 0
```

Un paquete candidato es un paquete que potencialmente puede iniciar la configuración de un acceso directo MLS. Su dirección MAC de destino es igual a la dirección MAC de un router que ejecuta MLS. En este caso, la dirección MAC del MSFC es 00-d0-d3-9c-9e-3c (se obtiene ejecutando el comando `show mls`). Para verificar que el switch sabe que esta dirección MAC es una dirección MAC del router, ejecute el comando `show cam mac_address`, como se muestra a continuación.

```
tamer (enable) show cam 00-d0-d3-9c-9e-3c
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry
VLAN  Dest MAC/Route Des      [CoS]  Destination Ports or VCs / [Protocol Type]
----  -
11     00-d0-d3-9c-9e-3c R#           15/1
12     00-d0-d3-9c-9e-3c R#           15/1
Total Matching CAM Entries Displayed = 2
```

Esta salida confirma que el switch sabe que esta dirección MAC es una entrada de router vinculada al puerto 15/1 (puerto MSFC en la ranura 1).

Si todavía no ve la MSFC cuando ejecuta el comando `show mls` en el Supervisor Engine del switch, ejecute el siguiente comando:

```
tamer (enable) show mls rlog 12
SWLOG at 815d0c50: magic 1008, size 51200, cur 815d4170, end 815dd460
Current time is: 08/08/00,17:13:25

118 08/08/00,17:13:16:(RouterConfig)Router_cfg: router_add_MAC_to_earl 00-d0-d3-
9c-9e-3c added for mod 15/1 Vlan 12 Earl AL =0
```

```

117 08/08/00,17:13:16:(RouterConfig)Router_Cfg: Process add mls entry for mod 15
/1 vlan 12, i/f 1, proto 0, LC 3
116 08/08/00,17:13:16:(RouterConfig)Router_cfg: router_add_MAC_to_earl 00-d0-d3-
9c-9e-3c added for mod 15/1 Vlan 11 Earl AL =0
115 08/08/00,17:13:16:(RouterConfig)Router_Cfg: Process add mls entry for mod 15
/1 vlan 11, i/f 1, proto 0, LC 3

```

Este comando le muestra los mensajes que el switch recibe de la MSFC y que se agregan las entradas del router.

Lectura de tablas de resultados del comando show mls

Ejecute el comando show mls entry para visualizar la tabla MLS entera con todos los accesos directos. La siguiente salida muestra todos los flujos recibidos.

```

tamer (enable) show mls entry
Destination-IP  Source-IP          Prot  DstPrt SrcPrt Destination-MAC  Vlan EDst
-----
MSFC 11.1.1.2 (Module 15):
10.68.5.1      -                    -    -      -      00-d0-00-3f-a3-ff 8    ARPA
12.1.1.1      -                    -    -      -      00-00-0c-8c-70-88 12   ARPA
11.1.1.1      -                    -    -      -      00-00-0c-09-50-66 11   ARPA
ESrc DPort  SPort  Stat-Pkts  Stat-Bytes  Uptime  Age
-----
ARPA 1/3    7/3    4          400         00:00:02 00:00:02
ARPA 7/4    7/3    4          400         00:00:08 00:00:08
ARPA 7/3    7/4    9          900         00:00:08 00:00:08

Destination-IPX          Destination-MAC  Vlan EDst ESrc  Port  Stat-Pkts
-----
Stat-Bytes  Uptime  Age
-----

MSFC 11.1.1.2 (Module 15):

Total entries displayed: 2
tamer (enable)

```

Nota: Se crea un flujo por destino. Un ping de 12.1.1.1 a 11.1.1.1 creará dos flujos (uno para cada dirección), como indican las dos últimas líneas en el resultado que se muestra arriba.

A continuación se describen algunos datos de la información que se encuentra en la tabla:

- Destination IP (IP de destino), source IP (IP de origen), Prot, DstPrt y SrcPrt son los campos que se utilizan para crear accesos directos. En este caso, sólo se utiliza el flujo de destino. Sólo se almacena en memoria caché la dirección IP de destino de un flujo. Esto se puede cambiar modificando la máscara de flujo, que se describe más adelante en este documento.
- El destino MAC es una dirección MAC que se usará para volver a escribir el destino MAC de un paquete. La dirección MAC de origen se reescribe con la dirección MAC de la MSFC.
- VLAN indica la VLAN de destino necesaria para alcanzar esa dirección IP. La VLAN de destino es importante, por ejemplo, si el paquete necesita ser enviado en un trunk.
- DPort y SPort son el destino y el puerto de origen del flujo.
- Stat-Pkts y Stat-Bytes proporcionan estadísticas sobre la cantidad de paquetes que ha

utilizado este acceso directo desde la creación del flujo.

- El tiempo de actividad es el tiempo transcurrido desde que se creó el flujo.
- La edad es el tiempo transcurrido desde que se utilizó el flujo por última vez.

Cambie el flujo a destination-source. El resultado del comando **show mls entry** muestra tanto la dirección IP de origen como la dirección IP de destino en el almacenamiento en caché. Ahora se crea un flujo diferente para cada dirección IP de origen que se comunica con la misma dirección IP de destino, como se muestra a continuación.

```
tamer (enable) set mls flow destination-source
Configured IP flowmask is set to destination-source flow.
Warning: Configuring more specific flow mask may increase the number of MLS
entries dramatically.
tamer (enable) 2000 Aug 09 17:05:12 %MLS-5-FLOWMASKCHANGE:IP flowmask changed
from DEST to DEST-SRC
```

```
tamer (enable) show mls entry
Destination-IP  Source-IP          Prot  DstPrt  SrcPrt  Destination-MAC  Vlan  EDst
-----
MSFC 11.1.1.2 (Module 15):
11.1.1.1      12.1.1.1             -    -      -      00-00-0c-09-50-66 11    ARPA
11.1.1.1      10.68.5.1            -    -      -      00-00-0c-09-50-66 11    ARPA
10.68.5.1     11.1.1.1             -    -      -      00-d0-00-3f-a3-ff 8     ARPA
12.1.1.1     11.1.1.1             -    -      -      00-00-0c-8c-70-88 12    ARPA
MSFC 0.0.0.0 (Module 16):
```

ESrc	DPort	Sport	Stat-Pkts	Stat-Bytes	Uptime	Age
ARPA	7/3	7/4	4	400	00:00:02	00:00:02
ARPA	7/3	1/3	4	400	00:00:32	00:00:32
ARPA	1/3	7/3	4	400	00:00:32	00:00:32
ARPA	7/4	7/3	4	400	00:00:02	00:00:02

```
Destination-IPX          Destination-MAC  Vlan  EDst  ESrc  Port
-----
Stat-Pkts  Stat-Bytes  Uptime  Age
-----
```

```
MSFC 11.1.1.2 (Module 15):
MSFC 0.0.0.0 (Module 16):
```

```
Total entries displayed: 4
tamer (enable)
```

La tercera opción es fijar MLS a flujo completo. Realice algunos pings y sesiones Telnet para ver cómo se crean los diferentes flujos para cada puerto TCP. A continuación se muestra cómo debe verse la tabla MLS luego de realizar algunas sesiones ping y Telnet. Al utilizar este flujo, la cantidad de flujos creados aumenta muy rápidamente. La información del puerto TCP se almacena en caché y aparece en la tabla MLS.

```
tamer (enable) set mls flow full
Configured IP flowmask is set to full flow.
Warning: Configuring more specific flow mask may increase the number of MLS
entries dramatically.
```

Tamer (enable) 2000 Aug 09 17:30:01 %MLS-5-FLOWMASKCHANGE:IP flowmask changed from DEST to FULL

tamer (enable)

tamer (enable) **show mls entry**

Destination-IP	Source-IP	Prot	DstPrt	SrcPrt	Destination-MAC	Vlan	EDst
MSFC 11.1.1.2 (Module 15):							
12.1.1.1	11.1.1.1	ICMP	-	-	00-00-0c-8c-70-88	12	ARPA
11.1.1.1	12.1.1.1	TCP	11001	Telnet	00-00-0c-09-50-66	11	ARPA
12.1.1.1	11.1.1.1	TCP*	Telnet	11001	00-00-0c-8c-70-88	12	ARPA
11.1.1.1	10.68.5.1	TCP	11002	Telnet	00-00-0c-09-50-66	11	ARPA
10.68.5.1	11.1.1.1	ICMP	-	-	00-d0-00-3f-a3-ff	8	ARPA
10.68.5.1	11.1.1.1	TCP*	Telnet	11002	00-d0-00-3f-a3-ff	8	ARPA
11.1.1.1	10.68.5.1	ICMP	-	-	00-00-0c-09-50-66	11	ARPA
11.1.1.1	12.1.1.1	ICMP	-	-	00-00-0c-09-50-66	11	ARPA

ESrc	DPort	Sport	Stat-Pkts	Stat-Bytes	Uptime	Age
ARPA	7/4	7/3	4	400	00:00:30	00:00:30
ARPA	7/3	7/4	16	688	00:00:26	00:00:24
ARPA	7/4	7/3	18	757	00:00:26	00:00:24
ARPA	7/3	1/3	61	4968	00:00:16	00:00:06
ARPA	1/3	7/3	4	400	00:00:33	00:00:33
ARPA	1/3	7/3	69	2845	00:00:17	00:00:06
ARPA	7/3	1/3	4	400	00:00:33	00:00:33
ARPA	7/3	7/4	4	400	00:00:32	00:00:31

Destination-IPX	Destination-MAC	Vlan	EDst	ESrc	Port	Stat-Pkts
Stat-Bytes						
Uptime						
Age						

MSFC 11.1.1.2 (Module 15):

Total entries displayed: 8

Notas

- En una red activa, el número de flujos creados puede llegar a varios miles. Ejecute el comando **show mls entry ip [destination/source]** para mostrar un flujo específico en lugar de mostrar la tabla de flujo completo, como se muestra a continuación.

tamer (enable) **show mls entry ip destination 12.1.1.1**

Destination-IP	Source-IP	Prot	DstPrt	SrcPrt	Destination-MAC	Vlan	EDst
MSFC 11.1.1.2 (Module 15):							
12.1.1.1	-	-	-	-	00-00-0c-8c-70-88	12	ARPA

ESrc	DPort	Sport	Stat-Pkts	Stat-Bytes	Uptime	Age
ARPA	7/4	7/3	4	400	00:00:30	00:00:30

- Puede verificar las estadísticas del flujo ejecutando el comando **show mls statistics**, como se muestra a continuación.

```
tamer (enable) show mls statistics entry ip 15
                                     Last      Used
Destination IP  Source IP      Prot DstPrt  SrcPrt  Stat-Pkts  Stat-Bytes
-----
MSFC 11.1.1.2 (Module 15):
12.1.1.1      11.1.1.1      ICMP -      -        9        900
11.1.1.1      10.68.5.1     TCP  11005   Telnet  20         913
11.1.1.1      10.68.5.1     TCP  11004   Telnet  0          0
10.68.5.1     11.1.1.1     ICMP -      -        4        400
10.68.5.1     12.1.1.1     ICMP -      -        9        900
12.1.1.1     10.68.5.1     ICMP -      -        4        400
11.1.1.1     10.68.5.1     ICMP -      -        4        400
11.1.1.1     12.1.1.1     ICMP -      -        9        900
```

Solución de problemas en una conexión específica

Si tiene problemas de conectividad en una dirección IP específica o entre dos hosts específicos, intente con la siguiente solución de problemas:

- Ejecute el comando **show mls entry ip [destination|source]** para ver si se ha creado el flujo.
- Ejecute el comando **show mls statistics entry [source|destination]** varias veces seguidas para ver si los contadores de paquetes de estado para ese acceso directo están aumentando.
- Verifique el flujo relevante.

Por ejemplo, para una sesión FTP de un archivo grande entre el servidor TFTP 12.1.1.1 y el cliente TFTP 11.1.1.1, debe verificar los dos flujos siguientes:

- Uno con destino 12.1.1.1 que debería acertarse sólo por el reconocimiento de TFTP (paquete pequeño) (origen del flujo 12.1.1.1 si se utiliza el flujo de origen y destino).
- Uno con destino 11.1.1.1 que debe ser encontrado por muchos paquetes grandes (la transferencia de archivos real) (origen del flujo 11.1.1.1 si se utiliza el flujo destino-origen). Este es un ejemplo de TFTP entre 12.1.1.1 y 11.1.1.1 de un archivo de aproximadamente 7.6 MB. A continuación se observa la tabla de estadísticas MLS antes del comienzo del TFTP:

```
tamer (enable) show mls statistics entry
                                     Last      Used
Destination IP  Source IP      Prot DstPrt  SrcPrt  Stat-Pkts  Stat-Bytes
-----
MSFC 11.1.1.2 (Module 15):
12.1.1.1      11.1.1.1      ICMP -      -        4        400
11.1.1.1      12.1.1.1      ICMP -      -        4        400
12.1.1.1      11.1.1.1      TCP  11000   Telnet  20         894
```

El TFTP acaba de empezar. Los dos flujos adicionales creados para el tráfico TFTP (puerto UDP 69) se muestran a continuación.

```
tamer (enable) show mls statistics entry
                                     Last      Used
Destination IP  Source IP      Prot DstPrt  SrcPrt  Stat-Pkts  Stat-Bytes
-----
MSFC 11.1.1.2 (Module 15):
12.1.1.1      11.1.1.1      ICMP -      -        4        400
12.1.1.1      11.1.1.1      UDP  69      50532   343       10997
11.1.1.1      12.1.1.1      ICMP -      -        4        400
11.1.1.1      12.1.1.1      UDP  50532   69      343       186592
12.1.1.1      11.1.1.1      TCP  11000   Telnet  20         894
```

La transferencia TFTP acaba de terminar. Se transfieren aproximadamente 8.1 MB desde el servidor al cliente en 14,903 paquetes, lo cual implica un promedio de 544 bytes de tamaño para cada paquete. En la otra dirección, se recibe la misma cantidad de paquetes con un tamaño promedio de 476.949 dividido por 14.904, lo que hace 33 bytes.

Tamer (enable) **show mls statistics entry**

Destination IP	Source IP	Last		Used		Stat-Pkts	Stat-Bytes
		Prot	DstPrt	SrcPrt			

MSFC 11.1.1.2 (Module 15):							
12.1.1.1	11.1.1.1	ICMP	-	-	4	400	
12.1.1.1	11.1.1.1	UDP	69	50532	14904	476949	
11.1.1.1	12.1.1.1	ICMP	-	-	4	400	
11.1.1.1	12.1.1.1	UDP	50532	69	14903	8107224	
12.1.1.1	11.1.1.1	TCP	11000	Telnet	20	894	

Estas tablas deberían darle una idea de cómo debería ser su patrón de tráfico.

Ejemplo 2: Dos MSFC en el mismo chasis configurado para HSRP

A continuación se muestra la configuración en ejecución de los dos MSFC configurados para HSRP y el resultado del comando **show standby**. La MSFC en la ranura 15 está activa para la VLAN 12 y la MSFC en la ranura 16 está activa para la VLAN 11.

Ranura 15	Ranura 16
<pre>tamer-msfc#wr t Building configuration... Current configuration: ! version 12.1 no service pad service timestamps debug uptime service timestamps log uptime no service password- encryption ! hostname tamer-msfc ! boot system flash bootflash: c6msfc-ds-mz.121-1.E2.bin ! ip subnet-zero ip cef ! ! ! ! interface Vlan1 ip address 10.200.11.120 255.255.252.0 !</pre>	<pre>tamer-msfc-2#wr t Building configuration... Current configuration: ! version 12.1 no service pad service timestamps debug uptime service timestamps log uptime no service password- encryption ! hostname tamer-msfc-2 ! boot system flash bootflash:c6msfc-jsv- mz.121-2.E.bin ! ip subnet-zero ! ! ! ! interface Vlan1 ip address 10.200.11.121 255.255.252.0 ! interface Vlan8</pre>

<pre> interface Vlan8 ip address 10.68.5.2 255.255.252.0 ! interface Vlan11 ip address 11.1.1.2 255.255.255.0 no ip redirects standby 11 preempt standby 11 ip 11.1.1.3 ! interface Vlan12 ip address 12.1.1.2 255.255.255.0 no ip redirects standby 12 priority 105 preempt standby 12 ip 12.1.1.3 ! router eigrp 1 network 10.0.0.0 network 11.0.0.0 network 12.0.0.0 no auto-summary ! ip classless ! line con 0 transport input none line vty 0 4 login ! end </pre>	<pre> ip address 10.68.5.4 255.255.252.0 ! interface Vlan11 ip address 11.1.1.4 255.255.255.0 no ip redirects standby 11 priority 105 preempt standby 11 ip 11.1.1.3 ! interface Vlan12 ip address 12.1.1.4 255.255.255.0 no ip redirects standby 12 preempt standby 12 ip 12.1.1.3 ! router eigrp 1 network 10.0.0.0 network 11.0.0.0 network 12.0.0.0 no auto-summary ! ip classless! ! line con 0 transport input none line vty 0 4 login ! end </pre>
---	--

<pre> tamer-msfc>show standby Vlan11 - Group 11 Local state is Standby, priority 100, may preempt Hellotime 3 holdtime 10 Next hello sent in 00:00:00.814 Hot standby IP address is 11.1.1.3 configured Active router is 11.1.1.4 expires in 00:00:09 Standby router is local Standby virtual MAC address is 0000.0c07.ac0b 4 state changes, last state change 00:06:36 Vlan12 - Group 12 Local state is Active, priority 105, may preempt Hellotime 3 holdtime 10 Next hello sent in 00:00:02.380 Hot standby IP address is 12.1.1.3 configured Active router is local </pre>	<pre> tamer-msfc-2#show standby Vlan11 - Group 11 Local state is Active, priority 105, may preempt Hellotime 3 holdtime 10 Next hello sent in 00:00:02.846 Hot standby IP address is 11.1.1.3 configured Active router is local Standby router is 11.1.1.2 expires in 00:00:08 Standby virtual MAC address is 0000.0c07.ac0b 2 state changes, last state change 00:07:02 Vlan12 - Group 12 Local state is Standby, priority 100, may preempt Hellotime 3 holdtime 10 Next hello sent in 00:00:02.518 Hot standby IP address is 12.1.1.3 configured </pre>
--	---

Standby router is 12.1.1.4 expires in 00:00:09 Standby virtual MAC address is 0000.0c07.ac0c 2 state changes, last state change 00:12:22	Active router is 12.1.1.2 expires in 00:00:07, priority 105 Standby router is local Standby virtual MAC address is 0000.0c07.ac0c 4 state changes, last state change 00:04:08
--	--

La información del ejemplo anterior todavía es válida. Para verificar qué ha cambiado después de configurar HSRP, vea el resultado de los comandos MLS a continuación.

Activación de comandos show mls

```
tamer (enable) show mls
Total packets switched = 29894
Total Active MLS entries = 0
  MSFC 11.1.1.2 (Module 15) entries = 0
  MSFC 10.200.11.121 (Module 16) entries = 0
IP Multilayer switching aging time = 256 seconds
IP Multilayer switching fast aging time = 0 seconds, packet threshold = 0
IP Current flow mask is Full flow
Active IP MLS entries = 0
Netflow Data Export version: 7
Netflow Data Export disabled
Netflow Data Export port/host is not configured.
Total packets exported = 0
IP MSFC ID      Module XTAG MAC                      Vlans
-----
11.1.1.2       15      1    00-d0-d3-9c-9e-3c 12,11,8,1
                00-00-0c-07-ac-0c 12
10.200.11.121  16      2    00-d0-bc-f0-07-b0 1,8,11,12
                00-00-0c-07-ac-0b 11

IPX Multilayer switching aging time = 256 seconds
IPX flow mask is Destination flow
IPX max hop is 15
Active IPX MLS entries = 0
```

```
IPX MSFC ID      Module XTAG MAC                      Vlans
-----
11.1.1.2       15      1    -                      -
10.200.11.121  16      2    -                      -
```

- Ahora hay dos routers MLS vistos por el PFC.
- Para cada router mostrado, la dirección MAC que utiliza el grupo HSRP es 00-00-0c-07-ac-xx. Estas direcciones MAC son las direcciones MAC virtuales utilizadas por HSRP. Sólo puede observar la dirección MAC del grupo 11 conectado al router que está activado para dicho grupo (ranura 15 para VLAN 12 y ranura 16 para VLAN 11). Esto significa que además de los paquetes con la dirección MAC de destino como la dirección MAC MSFC, también se consideran los paquetes candidatos, que son paquetes con MAC de destino como la dirección HSRP.
- Como se indica en el primer ejemplo, también necesita ver estas direcciones HSRP en la tabla CAM de Capa 2 que apuntan a la MSFC.

```
tamer (enable) show cam 00-00-0c-07-ac-0c
```

```
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.  
X = Port Security Entry
```

```
VLAN  Dest MAC/Route Des      [COs]  Destination Ports or VCS / [Protocol Type]  
-----  
12    00-00-0c-07-ac-0c R#          15/1  
Total Matching CAM Entries Displayed = 1  
tamer (enable)
```

```
tamer (enable) show cam 00-00-0c-07-ac-0b
```

```
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.  
X = Port Security Entry
```

```
VLAN  Dest MAC/Route Des      [COs]  Destination Ports or VCS / [Protocol Type]  
-----  
11    00-00-0c-07-ac-0b R#          16/1  
Total Matching CAM Entries Displayed = 1  
tamer (enable)
```

Ejecución de comandos de entrada show mls

```
tamer (enable) show mls entry
```

```
Destination-IP  Source-IP      Prot  DstPrt  SrcPrt  Destination-MAC  Vlan  EDst  
-----  
MSFC 11.1.1.2 (Module 15):  
11.1.1.1      12.1.1.1      ICMP  -       -       00-00-0c-09-50-66 11     ARPA  
MSFC 10.200.11.121 (Module 16):  
12.1.1.1      11.1.1.1      ICMP  -       -       00-10-7b-3b-af-3b 12     ARPA
```

```
ESrc DPort  Sport  Stat-Pkts  Stat-Bytes  Uptime  Age  
-----  
ARPA 7/3    7/4    4          400         00:00:03 00:00:03  
ARPA 7/4    7/3    4          400         00:00:04 00:00:03
```

```
Destination-IPX      Destination-MAC  Vlan  EDst  ESrc  Port  Stat-Pkts  
-----  
Stat-Bytes  Uptime  Age  
-----
```

```
MSFC 11.1.1.2 (Module 15):  
MSFC 10.200.11.121 (Module 16):
```

- Ahora hay dos tablas de accesos directos: uno para los flujos creados por la MSFC y otro para los flujos creados por la segunda MSFC.
- Al hacer ping entre 11.1.1.1 y 12.1.1.1, que son dos PC configurados con la dirección HSRP como su gateway predeterminado, los paquetes de 12.1.1.1 a 11.1.1.1 que llegan a VLAN 12 en el switch fueron cortados por el MSFC en la ranura 15 (ya que es el router HSRP activo para VLAN 12) y el MSFC crea un acceso directo para el destino 11.1.1.1 en la ranura 15. Los accesos directos para los paquetes de 11.1.1.1 a 12.1.1.1 han sido creados en el otro extremo por el MSFC en la ranura 16.

Consejos de Troubleshooting

Creación de flujos

Si no se ha creado un flujo, utilice los siguientes consejos para la resolución de problemas:

- ¿Observa el Supervisor Engine la MSFC con todas las direcciones MAC esperadas al ejecutar el comando show mls? En caso afirmativo, vaya al siguiente paso. Si la respuesta es no, asegúrese de que la MSFC no esté atascada en el modo ROMmon. Verifique que MLS esté habilitado en MSFC activando el comando show mls status.
- ¿La dirección MAC del MSFC está presente cuando se ejecuta el comando show cam? ¿Aparece como una entrada de router cam (R#)?
- Verifique que no haya configurado una función en la MSFC que desactiva MLS. Verifique las funciones que podrían impactar el MLS con la revisión de las notas de versión para la versión del software que está ejecutando. En la tabla siguiente se muestran ejemplos de restricciones. **Restricciones de IP de los comandos del router**
- Compruebe que ha activado una lista de acceso que solicita la gestión del software en lugar de que la procesen los accesos directos de hardware. Consulte [Manejo de Hardware y Software de ACL de IOS](#) para obtener más información.

Si después de seguir todos los consejos mencionados anteriormente todavía experimenta problemas, verifique si la MSFC todavía está siendo alcanzada por muchos paquetes.

- Algo puede estar haciendo que las entradas se purguen continuamente. Entre las causas posibles de la purga de la tabla de flujo se puede incluir lo siguiente: Intermitente de ruta o cualquier inestabilidad de Capa 3. La memoria caché de ARP cambia en la MSFC. La máscara de flujo cambió en Supervisor Engine. La VLAN de destino está eliminada. La interfaz VLAN se cierra en la MSFC.
- Otras razones para el reenvío del software (paquete que consultan la MSFC) en lugar de accesos directos por hardware pueden incluir lo siguiente: Paquete con la configuración de opción de IP. Paquete con TTL inferior o igual a 1. Paquete que debe fragmentarse.
- Puede tener hasta 128 K de flujo, sin embargo, se utiliza un algoritmo de hash. Si excede los flujos de 32 K, puede comenzar a tener colisión de hash que hará que los paquetes sean enrutados por el software. Una manera de evitar tener demasiados flujos es configurar un envejecimiento rápido para el flujo MLS.
- Recuerde que sólo puede tener MLS para IP, IPX e IP de multidifusión. Si tiene otros tipos de tráfico (por ejemplo, AppleTalk), serán software enrutado y pueden causar picos de la CPU en la MSFC o paquete excesivo que se dispara en el MSFC.
- Como se detalló, los IP MLS e IPX MLS están activados de forma predeterminada, esto no sucede con los IP MLS multidifusión. Si está utilizando la multidifusión de IP, asegúrese de habilitar MLS para la multidifusión tal como se especifica en la guía de configuración.

Nota: Una Notificación de cambio de topología de árbol de extensión (TCN) o puertos inestables en un switch Catalyst 6500/6000 Series no harán que se borre la tabla de flujo de MLS, como ocurrió con MLS en switches Catalyst 5000.

La contabilidad IP excluye el tráfico MLS

En Cisco Catalyst serie 6500, el switching de varias capas (MLS) se implementa de tal manera que una vez que se establece un flujo, el tráfico se conmuta directamente en PFC (conmutado por hardware) y no es procesado por la MSFC, por lo que no existe una contabilidad continua. La contabilización IP sólo registra los flujos nuevos o conmutados por proceso (conmutados por

software) cuando están activados, e incluso entonces sólo hasta que la entrada se introduce en la base de datos. Por lo tanto, el mensaje de advertencia anterior se muestra normalmente cuando se habilita la contabilización IP en dicha plataforma.

```
6500(config)#int fa8/40
6500(config-if)#ip accounting
Accounting will exclude mls traffic when mls is enabled.
```

La contabilidad de NetFlow es el método preferido. Refiérase a [Configuración de NetFlow](#) para obtener más información con respecto a NetFlow.

No se puede configurar la máscara de flujo completa de la interfaz

```
C6500#mls flow ip interface-full
% Unable to configure flow mask for ip protocol: interface-full. Reset
to the default flow mask type: none
```

Ejecute el comando **show fm fie flowmask detail** y verifique si NAT está habilitado y utiliza la máscara *Intf Full Flow*.

```
C6500#show fm fie flowmask detail
!--- Part of the output not shown Primary Flowmasks registered by Features -----
-----+-----+----- Feature Flowmask Flowmask Status -----
-----+-----+-----+----- IP_ACCESS_INGRESS Intf
Full Flow Disabled/Unused IP_ACCESS_EGRESS Intf Full Flow Disabled/Unused NAT_INGRESS Intf Full
Flow Enabled NAT_EGRESS Intf Full Flow Enabled !--- Remaining part of the output not shown
```

Si NAT utiliza la máscara de *flujo completo de Intf* y cuando intenta configurar la interfaz llena para Netflow, hay un problema, ya que hay un conflicto de máscara de flujo. Si desea utilizar Netflow stat, puede intentar utilizar *interface-destination-source* (comando **mls flow ip interface-destination-source**), que no entra en conflicto con el uso de la máscara de NetFlow.

NDE asume que todos los flujos se crean con la misma máscara de flujo. Debido a esta restricción, NDE no se puede habilitar con ciertas funciones que requieren máscaras de flujo conflictivas. Un caso específico es la NAT acelerada por hardware. NDE y NAT acelerada por hardware son mutuamente excluyentes.

NDE falla si se produce alguno de estos eventos:

- NAT acelerada por hardware está habilitada.
- En el switch se han configurado dos o más funciones con máscaras de flujo en conflicto.

Por el contrario, una vez que NDE se ha configurado correctamente, NAT no se puede configurar para funcionar en el hardware y no se pueden configurar en el switch dos funciones diferentes con requisitos de máscara de flujo contradictorios.

Información Relacionada

- [Resolución de Problemas de IP MultiLayer Switching](#)
- [Troubleshooting de Unicast IP Routing con CEF en Catalyst 6500/6000 Series Switches con Supervisor Engine 2 y ejecutando CatOS System Software.](#)
- [Configuración de Conmutación IP multicapa en el Catalyst 5000](#)

- [Soporte Técnico y Documentación - Cisco Systems](#)