

Troubleshoot Hardware Program for Multicast on 6500/7600 Devices

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Troubleshoot](#)

[Verify](#)

Introduction

This document describes how to troubleshoot and verify multicast hardware programming on 6500 and 7600 platforms.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Multicast.

Components Used

The information in this document is based on 7600 with SUP720 12.2(33)SXJ6 or above.

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.

Background Information

On 6500 and 7600 devices, multicast forward values are programmed in hardware for faster forwards and CPU preservation.

There are two types of multicast replication possible in this devices:

- Ingress replication
- Egress replication

Egress replication is the preferred method because replication is done on the line cards that exits which saves fabric utilization.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

First check the mroute state to ensure that the (S,G) state is created.

```
R1#show ip mroute 239.1.1.5
```

```
IP Multicast Routing Table
```

```
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
```

```
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
```

```
T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
```

```
X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
```

```
U - URD, I - Received Source Specific Host Report,
```

```
Z - Multicast Tunnel, z - MDT-data group sender,
```

```
Y - Joined MDT-data group, y - Sending to MDT-data group,
```

```
V - RD & Vector, v - Vector
```

```
Outgoing interface flags: H - Hardware switched, A - Assert winner
```

```
Timers: Uptime/Expires
```

```
Interface state: Interface, Next-Hop or VCD, State/Mode
```

```
(* , 239.1.1.5), 7w0d/stopped, RP 10.1.1.1, flags: SJC
```

```
Incoming interface: Null, RPF nbr 0.0.0.0
```

```
Outgoing interface list:
```

```
Vlan102, Forward/Sparse, 1y33w/00:02:48
```

```
(192.168.1.1, 239.1.1.5), 6d00h/00:02:50, flags: MT
```

```
Incoming interface: GigabitEthernet6/2, RPF nbr 172.16.2.2
```

```
Outgoing interface list:
```

```
Vlan102, Forward/Sparse, 6d00h/00:02:48
```

Ensure that the S,G state is created with traffic which goes in on Gig6/2 and is requested on vlan 102.

You can also use the count version of the previous command to see that packet counters increases.

Verify

Use this section in order to confirm that your configuration works properly.

Verify that vlan 102 is a hardware switched outgoing interfaces, you can also see the number of packets switched and the total number of hardware switched flows.

```
R1#show platform software multicast ip group 239.1.1.5
```

```
Multicast hardware switched flows:
```

```
(192.168.1.1, 239.1.1.5) Incoming interface: GigabitEthernet6/2, Packets Switched: 4076111744
```

```
Hardware switched outgoing interfaces:
```

```
Vlan102
```

```
Total hardware switched flows: 25
```

Now check the internal vlan usage to know which internal vlan was assigned to the incoming interface Gig6/2.

```
R1#show vlan internal usage
```

```
VLAN Usage
```

```
-----
```

```
1006 online diag vlan0
```

```

1007 online diag vlan1
1008 online diag vlan2
1009 online diag vlan3
1010 online diag vlan4
1011 online diag vlan5
1012 PM vlan process (trunk tagging)
1013 Control Plane Protection
1014 vrf_0_vlan
1015 Container0
1016 IPv6-mpls RSVD VLAN
1017 IPv4 VPN 0 Egress multicast
1018 IP Multicast Partial SC vpn(0)
1019 Multicast VPN 0 QOS Vlan
1020 GigabitEthernet6/2
1021 GigabitEthernet5/2

```

You can see that interface GigabitEthernet6/2 was assigned internal vlan 1020.

Proceed to check the CEF program in the Supervisor.

```
R1#remote command switch show mls cef ip multicast source 192.168.1.1 group 239.1.1.5
```

```

Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial, E - Encapsulation, D -
Decapsulation, M - MAC rewrite, T - Forwarding
c - Central Rewrite, p - Primary Input, r - Recirculation, h - Entry sitting on Encap/Decap VRF
layer
Source/mask Destination/mask RPF/DF Flags #packets #bytes rwindex Output Vlans/Info
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
192.168.1.1/32 239.1.1.5/32 V11020 CTP 4077289327 104637396418 0x7FFA V1102 [1 oifs]
192.168.1.1/32 239.1.1.5/32 V11017 Tc 0 0 0x7FFA V1102 [1 oifs]

```

Found 1 entries. 1 are mfd entries

```
R1#remote command switch show mls cef ip multicast source 192.168.1.1 group 239.1.1.5
```

```

Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial, E - Encapsulation, D -
Decapsulation, M - MAC rewrite, T - Forwarding
c - Central Rewrite, p - Primary Input, r - Recirculation, h - Entry sitting on Encap/Decap VRF
layer
Source/mask Destination/mask RPF/DF Flags #packets #bytes rwindex Output Vlans/Info
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
192.168.1.1/32 239.1.1.5/32 V11020 CTP 4077354094 104726386276 0x7FFA V1102 [1 oifs]
192.168.1.1/32 239.1.1.5/32 V11017 Tc 0 0 0x7FFA V1102 [1 oifs]

```

Found 1 entries. 1 are mfd entries

From this output verify on the Reverse Path Forwarding (RPF)/ Don't Fragment (DF) column the incoming vlan on which it receives.

You can see V11020 which matches what was seen in the internal vlan usage for Gig6/2.

See V11017 listed, that is the vlan used for the egress replication, and is also included in the internal vlan usage command.

As the output Vlan, you can see Vlan 102 which is your outgoing interface, in case the outgoing interface is a L3 port you must see an internal vlan listed which can then be correlated with the internal vlan usage command to see if it matches.

Notice as well the rwindex column with value 0x7FFA, use this to see the destination interfaces.

```
R1#remote command switch mcast ltl-info index 7ffa
```

```
index 0x7FFA contain ports 1/T1,T2, 2/T1,T2, 3/T1,T2, 4/T1,T2, 5/T1, 6/T1
```

The output shows you the multicast traffic which is sent to the replication modules on the linecards. It has this nomenclature 1/T1,T2. Number 1 stands for module 1, while T1 and T2 are the two replication modules on linecard 1. Ensure that packet is sent to replication modules on linecards 1, 2, 3, 4, 5 and 6.

Check the detail for CEF programming:

```
R1#remote command switch show mls cef ip multicast source 192.168.1.1 group 239.1.1.5 detail
```

```
Multicast CEF Entries for VPN#0
```

```
(172.16.5.51, 239.250.250.2)
```

```
IOSVPN:0 (1) PI:1 (1) CR:0 (1) Recirc:0 (1)
```

```
Vlan:1020 AdjPtr:475138 FibRpfNf:1 FibRpfDf:1 FibAddr:0x30090
```

```
rwvlans:1020 rwindex:0x7FFA adjmac:0a1b.0ddd.bbbb rdt:1 E:0 CAP1:0
```

```
fmt:Mcast l3rwwld:1 DM:0 mtu:1518 rwtype:L2&L3 met2:0x8427 met3:0x8405
```

```
packets:0004079198240 bytes:000000107260242880
```

```
Starting Offset: 0x8427
```

```
V E L0 C:1017 I:0x02028
```

```
Starting Offset: 0x8405
```

```
V E C: 102 I:0x02013
```

```
IOSVPN:0 (1) PI:0 (1) CR:1 (1) Recirc:0 (1)
```

```
Vlan:1017 AdjPtr:475139 FibRpfNf:0 FibRpfDf:1 FibAddr:0x30092
```

```
rwvlans:1017 rwindex:0x7FFA adjmac:0a1b.0ddd.bbbb rdt:1 E:0 CAP1:0
```

```
fmt:Mcast l3rwwld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x8405
```

```
packets:0000000000000 bytes:000000000000000000
```

```
Starting Offset: 0x8405
```

```
V E C: 102 I:0x02013
```

```
Annotation-data: [0x14B455F0]
```

```
A-vlan: 1020 NS-vlan: 0 RP-rpf-vlan: 0
```

```
Anntn flags: [0x10] H
```

```
MTU: 1500 Retry-count: 0
```

```
Sec-entries count: 1
```

```
Met-handle: 0x455BA08 New-Met-handle: 0x0
```

```
Met2-handle: 0x10C07ED0
```

```
HAL L3-data : [0x5F954E8]
```

```
Flags: 0x4 FIB-index: 0x20DE ADJ-index: 0x74002 NF-addr: 0xFFFFFFFF
```

```
ML3 entry type: 0x0 [(S,G) shortcut]
```

```
Flags: 0xA1000000 Vpn: 0 Rpf: 1020 Rw_index: 0x7FFA
```

```
Adj_mtu: 1514 Met2: 0x8427 Met3: 0x8405
```

```
V6-data: NULL
```

```
---Secondary entry [1]---
```

```
HAL L3-data : [0x1831F8F8]
```

```
Flags: 0x4 FIB-index: 0x20DF ADJ-index: 0x74003 NF-addr: 0xFFFFFFFF
```

```
ML3 entry type: 0x0 [(S,G) shortcut]
```

```
Flags: 0x90000000 Vpn: 0 Rpf: 1017 Rw_index: 0x7FFA
```

```
Adj_mtu: 1514 Met2: 0x0 Met3: 0x8405
```

```
V6-data: NULL
```

```
---TE entries---
```

```
Found 1 entries. 1 are mfd entries
```

Focus on the starting offset I: values

```
R1#remote command switch show mls cef ip multicast source 192.168.1.1 group 239.1.1.5 detail
```

```
Multicast CEF Entries for VPN#0
```

```
(172.16.5.51, 239.250.250.2)
```

```
IOSVFN:0 (1) PI:1 (1) CR:0 (1) Recirc:0 (1)
Vlan:1020 AdjPtr:475138 FibRpfNf:1 FibRpfDf:1 FibAddr:0x30090
rwvlans:1020 rwinde:0x7FFA adjmac:0alb.0ddd.bbbb rdt:1 E:0 CAP1:0
fmt:Mcast l3rwvld:1 DM:0 mtu:1518 rwtype:L2&L3 met2:0x8427 met3:0x8405
packets:0004079198240 bytes:000000107260242880
Starting Offset: 0x8427
V E L0 C:1017 I:0x02028
Starting Offset: 0x8405
V E C: 102 I:0x02013
```

```
IOSVFN:0 (1) PI:0 (1) CR:1 (1) Recirc:0 (1)
Vlan:1017 AdjPtr:475139 FibRpfNf:0 FibRpfDf:1 FibAddr:0x30092
rwvlans:1017 rwinde:0x7FFA adjmac:0alb.0ddd.bbbb rdt:1 E:0 CAP1:0
fmt:Mcast l3rwvld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x8405
packets:0000000000000 bytes:000000000000000000
Starting Offset: 0x8405
V E C: 102 I:0x02013
```

```
Annotation-data: [0x14B455F0]
A-vlan: 1020 NS-vlan: 0 RP-rpf-vlan: 0
Anntn flags: [0x10] H
MTU: 1500 Retry-count: 0
Sec-entries count: 1
Met-handle: 0x455BA08 New-Met-handle: 0x0
Met2-handle: 0x10C07ED0
```

```
HAL L3-data : [0x5F954E8]
Flags: 0x4 FIB-index: 0x20DE ADJ-index: 0x74002 NF-addr: 0xFFFFFFFF
ML3 entry type: 0x0 [(S,G) shortcut]
Flags: 0xA1000000 Vpn: 0 Rpf: 1020 Rw_index: 0x7FFA
Adj_mtu: 1514 Met2: 0x8427 Met3: 0x8405
V6-data: NULL
```

---Secondary entry [1]---

```
HAL L3-data : [0x1831F8F8]
Flags: 0x4 FIB-index: 0x20DF ADJ-index: 0x74003 NF-addr: 0xFFFFFFFF
ML3 entry type: 0x0 [(S,G) shortcut]
Flags: 0x90000000 Vpn: 0 Rpf: 1017 Rw_index: 0x7FFA
Adj_mtu: 1514 Met2: 0x0 Met3: 0x8405
V6-data: NULL
```

---TE entries---

Found 1 entries. 1 are mfd entries

Use those values to see which interfaces are programmed on hardware.

```
R1#remote command switch test mcast ltl-info index 02028
index 0x2028 contain ports 1/T1,T2, 2/T1
```

```
R1#remote command switch test mcast ltl-info index 02013
index 0x2013 contain ports 1/21-33,44, 2/21,23
```

The first index shows the packet must be forwarded to linecard 1 to replication engine 1 and 2 and to linecard 2 replication engine 1.

The second Index shows the packet which forwards out on ports 1/21-33 and 44, this means that replication engine 1 on linecard 1 covers ports from 1/1 to 1/23, while replication engine 2 covers up to 48, also port 2/21 and 2/23 which use replication engine 1 in linecard 2, both outputs match.