Drop Vector	Meaning	Next Steps
ACL_DROP	This drop vector indicates that a packet or frame is encountering a sup TCAM index with a drop result due to a matching condition in the sup TCAM rule or due to a policer. A common reason why traffic would be dropped with this drop vector is if traffic is received on the switch, coming from the fabric, with the destination address set to an IP or MAC that the switch has a remote learn for with no **B** (bounce) flag.	Contact TAC to verify the sup TCAM rules that the traffic is hitting on the switch.
DCI_SCLASS_XLATE_MISS	Typically observed on spines in Multisite or Remote Leaf environments. This drop vector indicates that traffic is being received from the ISN with a defined **sclass** (src pcTag) that the spine does not have a translation entry for. Translation entries on spines get configured when a contract relationship is established between two EPGs or when **L2 Stretch** is configured in a BD on NDO.	Check the translation entries on the spine by running the **show dcimgr repo sclass-maps** command. If the expected entry is missing, then ensure that a contract relationship has been established between the EPGs that are trying to communicate. Also, check other spines in the same site to see if the entry is present or not. If a contract relationship has been established between the EPGs that are trying to communicate, but the translation entry is still missing, then contact TAC for further assistance.
DCI_VNID_XLATE_MISS	Typically observed on spines in Multisite or Remote Leaf environments. This drop vector indicates that traffic is being received from the ISN with a defined VNID that the spine does not have a translation entry for. Translation entries on spines get configured when a contract relationship is established between two EPGs or when **L2 Stretch** is configured in a BD on NDO.	Check the translation entries on the spine by running the **show dcimgr repo vnid-maps** command. If the expected entry is missing, then ensure that a contract relationship has been established between the EPGs that are trying to communicate. Also, check other spines in the same site to see if the entry is present or not. If a contract relationship has been established between the EPGs that are trying to communicate, but the translation entry is still missing, then contact TAC for further assistance.
INFRA_ENCAP_SRC_TEP_MISS	Typically observed in Multipod, Multisite or GOLF environments. This drop vector indicates that the switch has no tunnel pointing back to the source TEP. For Multipod, each leaf should have allowed prefix-list ranges for creating tunnels back to remote pod TEP addresses. For Multisite, the source TEP is an IP address configured on a loopback interface of a spine in the ingress site.	For Multipod, verify that the leaf has a prefix-list matching the remote pod TEP address by running the **moquery -c tunnelCtrlPfxEntry** command. Also, verify that eltmc has this prefix-list by running the **show system internal eltmc info pfxwl_table** command from **vsh_lc**. For Multisite, verify that a route pointing back to the source TEP is present in the RIB of VRF **overlay-1**. For GOLF, verify that a route pointing back to the source TEP is present in the RIB of VRF **overlay-1**. Also, verify that the leaf has routes coming from the GOLF router with the next-hop set to the TEP of the GOLF router. Finally, verify that the router MAC and RD advertised by the GOLF router are correct. If the expected output from any of the above is missing, and/or the root cause cannot be determined, then contact TAC for further assistance.
INNER_IDS_G0	This drop vector indicates that something about the packet or frame is invalid according to defined networking standards. For example, if class E addresses are observed, then the IDS check may drop this traffic. **CSCvc51695** is an example where this drop vector was observed for 127.0.0.0 (local host only) addresses.	Verify that nothing about the packet or frame looks "off". Are expected MAC or IP addresses being used? Are any reserved L2, L3, or L4 values being used? If nothing looks "off" about the packet or frame, and/or the issue cannot be resolved, then contact TAC for further assistance.
L3_BINDING_FAILURE	This drop vector indicates that First Hop Security with source guard is enabled on the BD. If the received traffic is sourced from an IP address that exists in the FHS binding table, but from a different MAC address than what is tied to that IP address in the binding table, this drop vector may be observed.	Verify that a **First Hop Security Policy** is configured in the BD by checking the **Advanced/Troubleshooting** tab. On the leaf, verify the FHS binding table by running the **show fhs bt all** command. Next, get the source IP and source MAC addresses from the ELAM **ereport**. Verify that the source IP address exists in the FHS table, and that the MAC address that is tied to it is different than what is seen in the ELAM **ereport**. If the above conditions are met, then verify what MAC address should be tied to that IP address. If the dropped traffic is the correct traffic, then it should send an ARP request, DHCP request, etc. from that MAC address to update the table. Another option is to disable FHS in the BD. If the issue cannot be resolved, then contact TAC for further assistance.
MC_L2_MISS	This drop vector indicates that the dropped traffic is multi-destination traffic, and that the ingress VNID/VLAN is not programmed on the switch. This is frequently seen in conjunction with the **VLAN_XLATE_MISS** drop vector.	Refer to the **Next Steps** column in the **VLAN_XLATE_MISS** row of this table.
MEM_ERR	This drop vector indicates that there are duplicate hardware entries matching the packet or frame.	It's likely that a switch reload will need to be performed to recover from the hardware programming problem. However, please gather the output of the ELAM **ereport**, tech supports and TAC outputs from the switch, and then contact TAC for further assistance before reloading.
OUTER_CBL_CHECK	This drop vector indicates that traffic is being received in the infra VLAN on an interface where the infra VLAN is not programmed.	For TAH ASICs (any switch model ending in **EX**), run the **show plat int sug table tah_sug_lua_outervlanmbrtable 0x3** command in vsh_lc and gather the value displayed right after **info_leaf_port_members=** in the output. For ROC ASICs (any switch model ending in FX/FX2/FX3), run the **show plat int hom table roc_hom_lua_outervlanmbrtable 0x3** command in vsh_lc and gather the value displayed right after **info_leaf_port_members=** in the output. Next, take that value and verify what interfaces the infra VLAN is programmed on by running the **show plat int hal l2 ifmap-to-ifname 0 0 <value>** command. If the interface where the traffic was triggered is missing from the output, then contact TAC for further assistance.
SECURITY_GROUP_DENY	This drop vector indicates that the packet or frame is being dropped due to a contract (or lack thereof).	From the ELAM **ereport**, gather the **sclass** (src pcTag) and **dclass** (dst pcTag) and verify that the values are expected. If the values are unexpected, then check for unexpected EP learns (**show endpoint**) or unexpected HAL L3 route entries (**show plat int hal l3 routes**). To find the zoning rule that is being hit for the contract, run the **show sys int aclqos zoning-rules	grep -B 9 "Idx: <value>"** command found in the **Contract Result** section of the ELAM **ereport**. If the zoning rule is not present, or if the behavior observed does not match what's configured in the rule, then contact TAC for further assistance.
TTL_EXPIRED	This drop vector indicates that the switch received routed traffic where the TTL value was decremented to 0 and the packet was dropped.	The most likely root cause is that the external environment is sending traffic with a TTL value of 1 or 2 when the routing decisions require more hops than this. If this is the case, then increase the TTL value in the external environment. Also, loops can result in TTL expiration, so verify that the traffic is not being looped. If it is, then correct the looping behavior. If the issue cannot be resolved, then contact TAC for further assistance.
UC_PC_CFG_TABLE_DROP	This drop vector indicates that the packet is being dropped because there is no route for the destination in the RIB of the VRF. This may also be observed if there is a route present, but it has a drop adjacency.	Run the **show ip route** command in the correct VRF for the destination and verify whether the route is present or not. If the route is not present, try to determine why. Next, verify whether the route is present or not in HAL by running the **show plat internal hal l3 routes** command. If the route is not present, then there is likely a hardware programming failure due to scale or some other issue. If the issue is due to scale, then changing the forwarding scale profile can help resolve the problem. For most other root causes, a reload of the switch could allow the route to get programmed correctly. If the route is present in HAL, then check the next-hop (**show plat int hal l3 nexthops**) or ECMP (**show plat int hal l3 ecmp**) adjacency tables and verify that there is no drop adjacency. If the root cause cannot be found or the issue cannot be resolved, then contact TAC for further assistance.
UC_TENANT_MYTEP_BRIDGE_MISS	This drop vector, when observed on a spine, may indicate that the traffic is destined to the MAC proxy, but the inner destination MAC is not present in the COOP database. This drop vector, when observed on a leaf, may indicate that the traffic is received in a VNID that is not programmed on the leaf (this may be seen in conjunction with **VLAN_XLATE_MISS**).	If the drop is observed on a spine, then verify that the MAC is present in the COOP DB (also, ensure that it is in the correct VNID) by running the **moquery -c coopEpRec -f 'coop.EpRec.mac=="<mac-address>"'** command. If the drop is observed on a leaf, then first determine if the traffic is using the VRF (L3), BD (L2), or FD (STP, AVS/AVE, etc.) VNID. Check the **Outer L4 Header** in the ELAM **ereport** and match it to the segment ID for that VNID. To confirm the VRF VNID, run the **moquery -c l3Ctx** command and check the **encap** entry. To confirm the BD VNID, run the **moquery -c l2BD** command and check the **fabEncap** entry. To confirm the EPG/FD VNID, run the **moquery -c vlanCktEp** command and check the **fabEncap** entry. To confirm the VNID for AVE/AVS, etc. (anything using VXLAN all the way down to the host), run the **moquery -c compEpPD** command and check the entry that corresponds to the EPG. If the root cause cannot be found or the issue cannot be resolved, then contact TAC for further assistance.
UC_TENANT_MYTEP_ROUTE_MISS	This drop vector is uncommon but is likely due to not having a route to the destination. For tenant traffic flows, the **UC_PC_CFG_TABLE_DROP** vector is typically observed if there is no route. The **UC_TENANT_MYTEP_ROUTE_MISS** has been observed when a spine is trying to ping another spine in a different pod and does not have a route to it.	Refer to the **Next Steps** column in the **UC_PC_CFG_TABLE_DROP** row of this table.
VLAN_XLATE_MISS	The VLAN that the traffic is received in is not programmed on the leaf.	In the ELAM **ereport**, verify whether the traffic is tagged or not by checking the value in the **802.1Q tag is valid** line in the **Outer L2 Header** section. Also, check the value in the **Access Encap VLAN** line of the same section, and ensure that it is correct/expected. Next, run the **show vlan extended	grep <vlan-id>** command in **ishell** to check if the VLAN exists on the switch (you can also run the **moquery -c vlanCktEp** command). Finally, run the **show interface switchport** command to check whether the traffic should be received as tagged or untagged. If a VMM domain with dynamic resolution is being used, then verify that there are no faults for **looseNodes**.
SMAC_MISS	This drop vector indicates that the leaf switch does not expect to learn the source MAC. You may see this drop vector in conjunction with fault code F2406, which occurs when EP learning is disabled on an interface. This has been seen in cases where port security has been inadvertently enabled on an interface, disallowing learns for any new MACs beyond the limit defined in the port security policy.	Check if port security, or a similar mechanism that limits MAC learns on an interface, is enabled and not as per design. Either disable it or increase the limit to allow more MAC learns.

CISCO