Troubleshooting Catalyst® Switches—Part 2
Session CDC-302

Agenda

- Terminology
- Multi-Layer Switching
- Multicast Multi-Layer Switching
- Layer 3 Access Control Lists
- Layer 3 Quality of Service
- Redundancy Issues in the Catalyst 6000
- FlexWan Basics
Multi-Layer Switching—Terminology

- MLS-RP (Routing Processor): Runs the routing protocols and responsible for routing the first packet of a flow
- MLS-SE (Switching Engine): Once the first packet is routed by the MLS-RP, the MLS-SE will be able to short-cut the packets for the rest of the flow

ACL and ACE—Terminology

- Access Control List (ACL)—a list of permit or deny statements that can be used to control access to or through a network device
- Access Control Entry (ACE)—a single line or entry in a ACL
Agenda

- Terminology
- Multi-Layer Switching
- Multicast Multi-Layer Switching
- Layer 3 Access Control Lists
- Layer 3 Quality of Service
- Redundancy Issues in the Catalyst 6000
- FlexWan Basics

MLS Cat5—Theory MLS Entry Creation

- Both the Candidate Packet and the Enabler Packet must pass through the same switch for a flow to be built
MLS Cat5—Problem
MLS-RP Not Seen on MLS-SE

• The router and switch are configured for multilayer switching, but when you do a show mls you don’t see the router

Switch> (enable) show mls
IP Multilayer switching enabled

MLS-RP IP MLS-RP ID XTAG MLS-RP MAC-Vlans
---------------- ------------ ---- ---------------------------------

Switch> (enable)

MLS Cat5—Solution
MLS-RP Not Seen on MLS-SE

• In configuring MLS order does matter. Enter the MLS interface commands in this order

  mls rp vtp-domain <domain name>
  mls rp vlan-id <vlan#>
  mls rp ip
  mls management-interface
MLS Cat5—Problem
MLS-RP Not Seen on MLS-SE

• Use the show mls rp command on the router to verify its configuration

```
router#show mls rp
ip multilayer switching is globally enabled
mls id is 0030.f2c9.561c
mls ip address 0.0.0.0
mls ip flow mask is destination
number of domains configured for mls 1

vlan domain name: vtpdomain
<....some output deleted....>

router currently aware of following 0 switch(es):
   no switch id's currently exists in domain
```

MLS Cat5—Solution
MLS-RP Not Seen on MLS-SE

• The RP IP address is chosen the moment that the mls rp ip global configuration statement is entered. So make sure there is an IP address configured on the router at that time. The fix for this is to reload the router after completing the configuration.
MLS Cat5—Problem
High CPU on MLS-RP

• With MLS enabled there is still a lot of traffic that is being switched by the MLS-RP causing higher then expected CPU utilization

• For the Catalyst 5000, the MLS-RP can be a 4000 Series or 7000 Series Router, as well as an Route Switch Module, Route Switch Feature Card, Multilayer Switch Module or Multilayer Switch Feature Card

MLS Cat5—Solution
High CPU on MLS-RP

• The RP and SE are seeing each other so why aren’t there active entries?

Switch> (enable) show mls
Total packets switched = 14
Total Active MLS entries = 0
IP Multilayer switching enabled
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
Configured flow mask is Destination flow
Active IP MLS entries = 0

<table>
<thead>
<tr>
<th>IP MLS-RP IP</th>
<th>MLS-RP ID</th>
<th>XTAG</th>
<th>MLS-RP MAC-Vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.6.1.149</td>
<td>0030f2c9561c</td>
<td>2</td>
<td>00-30-f2-c9-56-38 1-2</td>
</tr>
</tbody>
</table>

Copyright © 1998, Cisco Systems, Inc. All rights reserved. Printed in USA.
3207_06_2001_c1_X.scr
MLS Cat5—Solution
High CPU on MLS-RP

• In this scenario switch 1 will not maintain an flow entry for the path between A and B

![Diagram showing flow between A and B]

MLS Cat5—Solution
High CPU on MLS-RP

• What if we go to the other extreme?

```
Switch> (enable) show mls
Total packets switched = 928928
Total Active MLS entries = 14576
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
Configured flow mask is Destination flow
Active IP MLS entries = 14072
<...some output deleted...>

IPX Multilayer switching aging time = 256 seconds
IPX flow mask is Destination flow
IPX max hop is 255
Active IPX MLS entries = 504
<...some output deleted...>
```
MLS Cat5—Solution
High CPU on MLS-RP

• The hardware can support up to 16K flow entries, additional flows will be switched by the MLS-RP.
  
  A full flow mask will use the entries much quicker than a source-destination or destination only mask.

• If ip access-groups are configured on the vlan interfaces, then the flow mask will be changed to Destination-Source Flow or Full Flow.

---

Switch> (enable) show mls entry ip destination 172.10.1.2
Destination-IP Source-IP Prot DstPrt SrcPrt Destination-Mac Vlan EDst ESrc DPort SPort Stat-Pkts Stat-Bytes Uptime Age
------------------ -------------- ------ --------- --------- ----------------------- -------
------- ------- -------- -------- ------------- --------------- ---------- -----
172.10.1.2     172.10.10.5 UDP 2001 2001 00-d0-06-24-6f-fc 2
ARPA ARPA 1/1 4/1 43 1978 00:02:54 00:00:02
172.10.1.2     172.10.10.5 UDP 5001 5001 00-d0-06-24-6f-fc 2
ARPA ARPA 1/1 4/1 42 1932 00:02:51 00:00:03
172.10.1.2     172.10.10.5 UDP 3001 3001 00-d0-06-24-6f-fc 2
ARPA ARPA 1/1 4/1 43 1978 00:02:54 00:00:02
172.10.1.2     172.10.10.5 UDP 63 63 00-d0-06-24-6f-fc 2
ARPA ARPA 1/1 4/1 843 38778 00:17:24 00:02:59
MLS Cat5—Solution
High CPU on MLS-RP

• Destination-Source Flow

Switch> (enable) show mls entry ip destination 172.10.1.2
Destination-IP Source-IP Prot DstPrt SrcPrt Destination-Mac Vlan Edst Esrc DPort SPort Stat-Pkts Stat-Bytes Uptime Age
-------------------- -------------- ------ --------- --------- ----------------------- -------
------- ------- -------- -------- ------------- --------------- ---------- -----
172.10.1.2 172.10.10.5 - - - 00-d0-06-24-6f-fc 2
ARPA ARPA 1/1 4/1 46 2116 00:00:46 00:00:00

• Destination Flow

Switch> (enable) show mls entry ip destination 172.10.1.2
Destination-IP Source-IP Prot DstPrt SrcPrt Destination-Mac Vlan Edst Esrc DPort SPort Stat-Pkts Stat-Bytes Uptime Age
-------------------- -------------- ------ --------- --------- ----------------------- -------
------- ------- -------- -------- ------------- --------------- ---------- -----
172.10.1.2 - - - - 00-d0-06-24-6f-fc 2
ARPA ARPA 1/1 4/1 61 2806 00:01:01 00:00:00

• Applying an extended access-list

router(config-if)#interface vlan 2
router(config-if)#access-group 100 out
router(config-if)#
2001 May 13 22:38:54 %MLS-5-FLOWMASKCHANGE:IP flowmask changed from DEST to FULL
**MLS Cat5—Solution**

High CPU on MLS-RP

- If show mls shows few flows then maybe the IP traffic being routed cannot be MLS switched
  - IP packets with IP options set will NOT be MLS switched
  - IP fragments will NOT be MLS switched
  - Policy-Based Routing will NOT be MLS switched

**MLS Cat5—Problem**

MLS too Many Moves

- The series of messages shown below is usually thought of as a MLS problem.

```plaintext
%MLS-4-MOVEOVERFLOW:Too many moves, stop MLS for 5 sec(40000000)
%MLS-4-RESUMESC:Resume MLS after detecting too many moves
%MLS-4-MOVEOVERFLOW:Too many moves, stop MLS for 5 sec(40000000)
%MLS-4-RESUMESC:Resume MLS after detecting too many moves
```
MLS Cat5—Solution
MLS too Many Moves

• Too many moves is usually caused by one of two things
  A bridge loop...
  In a LANE environment, where a CAM entry can move back and forth between the BUS and Data Direct VCs

MLS Cat6 Sup I—Problem
High CPU on MSFC

• On a Catalyst 6000 with Supervisor I / MSFC, MLS happens automatically for traffic between VLANs configured on the MSFC
• Still a lot of traffic is being switched by the MSFC causing higher then expected CPU utilization
MLS Cat6 Sup I—Solution
High CPU on MLS-RP

- The hardware can support up to 32K flow entries, additional flows will be switched by the MSFC
- IP access-group ACLs do not effect the flow mask
- Microflow policing uses the same flow cache as the MLS cache. Thus the number flows being policed will reduce the number of MLS entries available accordingly

MLS Cat6 Sup I—Solution
High CPU on MSFC

- If show mls shows few flows then maybe the IP traffic being switched cannot be MLS switched
  - IP packets with IP options set will NOT be MLS switched
  - IP fragments will NOT be MLS switched
  - Policy-Based Routing can be MLS switched if it is matching IP and only setting next-hop
  - Unicast RPF will NOT be MLS switched
MLS Cat6 Sup II—Theory
MLS CEF Switching

- The PFC2 on the Sup2 is programmed by the MSFC2 with a copy of the MSFC's FIB and adjacency table.
- The PFC2 depends on the MSFC for routing and ARP information corresponding to FIB and adjacency updates.

MLS Cat6 Sup II—Problem
High CPU on MSFC

- On a Catalyst 6000 with Supervisor II, packets are CEF switched in the PFC by default
- Still a lot of traffic is being switched by the MSFC causing higher than expected CPU utilization
MLS Cat6 Sup II—Solution
High CPU on MLS-RP

• First check the MSFC routing table

```
msfc#show ip route 192.168.99.0
Routing entry for 192.168.99.0/24
  Known via "rip", distance 120, metric 1
  Last update from 192.168.100.3 on Vlan6, 00:00:11 ago
  Routing Descriptor Blocks:
    * 192.168.100.3, from 192.168.100.3, 00:00:11 ago, via Vlan6
  Route metric is 1, traffic share count is 1
```

• Also check the MSFC arp cache

```
msfc#show ip arp 192.168.100.3
Protocol Address          Age (min)  HardwareAddr   Type   Interface
Internet  192.168.100.3         118   0004.9a0b.aec2  ARPA   Vlan6
```

• Next check the MSFC CEF table

```
msfc15#show ip cef 192.168.99.0 detail
192.168.99.0/24, version 27, cached adjacency 192.168.100.3
  0 packets, 0 bytes
     via 192.168.100.3, Vlan6, 0 dependencies
     next hop 192.168.100.3, Vlan6
     valid cached adjacency
```

• Also check the MSFC adjacency table

```
msfc15#show adjacency vlan 6 detail
Protocol Interface     Address
IP   Vlan6             192.168.100.3(11)
  0 packets, 0 bytes
  00049A0BAEC2
  0D0D06246FFC0800
ARP   01:46:20
```
MLS Cat6 Sup II—Solution
High CPU on MLS-RP

• Then check the SupII’s CEF table

```
Cat6500> (enable) show mls cef mac
Module 15: Physical MAC-Address 00-d0-06-24-6f-fc
```
```
Cat6500> (enable) sh mls entry cef ip 192.168.99.0/24
Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight
---------- -------------------------- -------------------------- --------------------------
15 resolved 192.168.99.0 255.255.255.0 192.168.100.3 1
```

• Also check the SupII’s adjacency table

```
cs-c6509-16a> (enable) sh mls entry cef ip 192.168.100.3/32 adjacency
Mod: 15
Destination-IP: 192.168.100.3 Destination-Mask: 255.255.255.255
FIB-Type: resolved
AdjType NextHop-IP NextHop-Mac Vlan Encp Tx-Packets Tx-Octets
---------- -------------------------- ------------- -------- -------------------------- --------
connect 192.168.100.3 00-04-9a-0b-ae-c2 6 ARPA 0 0
```

MLS Cat6 Sup II—Solution
High CPU on MSFC

• If the routes are all in hardware, then maybe the packets cannot be MLS CEF switched.

  IP packets with IP options set will NOT be MLS CEF switched

  IP fragments will be MLS CEF switched

  Policy-Based Routing can be MLS CEF switched if it is matching IP and only setting next-hop

  Unicast RPF will be MLS CEF switched, but will cause the hardware routing table to be reduced to 128K entries from 256K entries. Failures will also be sent to the MSFC at 10pps per VLAN
Agenda

- Terminology
- Multi-Layer Switching
- Multicast Multi-Layer Switching
- Layer 3 Access Control Lists
- Layer 3 Quality of Service
- Redundancy Issues in the Catalyst 6000
- FlexWan Basics

Multicast MLS—Problem
MMLS in Inactive State

- With MMLS enabled on the MLS-SE, the MMLS process is still in an inactive state

Switch> (enable) show mls multicast
Admin Status : Enabled
Operational Status : Inactive
Total Entries : 0
MSFC (Module 15):
  IP Address : 10.118.2.58
  Complete Flows : 0
  Partial Flows : 0
Multicast MLS—Solution

MMLS in Inactive State

- For the switch to deal with Multicast packets intelligently, IGMP Snooping needs to be enabled

Switch> (enable) set igmp enable
IGMP feature for IP multicast enabled
Switch> (enable) show mls multicast
Admin Status : Enabled
Operational Status : Active
Total Entries : 15
MSFC (Module 15):
  IP Address : 10.118.2.58
  Complete Flows : 15
  Partial Flows : 0

Multicast MLS—Problem

High CPU on non-DR MSFC

- In a redundant routed multicast environment, the multicast non-Designated Router will see high cpu utilization due to non-Reverse Path Forwarding
Multicast MLS—Solution
High CPU on non-DR MSFC

- In a dual chassis with single supervisor configuration, a router ACL can be applied to kill the multicast non-RPF traffic for pim sparse mode

interface Vlan2
ip address 172.10.1.2 255.255.255.0 alt ip address 172.10.1.3 255.255.255.0
ip access-group 105 in
!
access-list 105 permit ip 172.10.1.0 0.0.0.255 any
access-list 105 permit ip any 224.0.0.0 0.0.0.255
access-list 105 permit ip any 224.0.1.0 0.0.0.255
access-list 105 deny ip any 224.0.0.0 15.255.255.255

Multicast MLS—Solution
High CPU on non-DR MSFC

- In a dual supervisor configuration or in pim dense mode, the solution is to migrate to Cat OS 6.2 to get the non-RPF Multicast Fast Drop (MFD) feature
- This feature is only supported on Supervisor 2s, and is enabled by default
Agenda

• Terminology
• Multi-Layer Switching
• Multicast Multi-Layer Switching
• Layer 3 Access Control Lists
• Layer 3 Quality of Service
• Redundancy Issues in the Catalyst 6000
• FlexWan Basics

Layer 3 ACLs—Problem
ACL Is Being Software Switched

• A new IP access-group is configured on a
VLAN interface, and now the MSFC is
having to route many more packets on
that interface then it did before the access-
group was applied
Layer 3 ACLs—Solution
ACL Is Being Software Switched

- If an ACL is configured with the log key word, any hits on that ACE will be passed to the MSFC to create the log entry
- If ip unreachables in enabled for a vlan interface, then any ACL denys will be passed to the MSFC to send the ICMP unreachable message

Layer 3 ACLs—Solution
ACL Is Being Software Switched

- Also check to make sure that the ACL was programmed into hardware by the MSFC

```console
router# show fm summary
Interface: Vlan1
 TCAM screening for features is INACTIVE inbound
Interface: Vlan2
 TCAM screening for features is ACTIVE outbound
 TCAM screening for features is ACTIVE inbound
```
Layer 3 ACLs—Problem Errors When Applying ACL

- When you apply an access-list to a VLAN interface one of the following messages appear:

```
router(config)#interface vlan 1
router(config-if)#ip access-group 100 in
<router>%ACL-3-NOLOU:Acl engine is out of logical operation unit
<router>%ACL-3-RACLMAPCOMMITFAIL:Failed to map Router ACL to VLAN 1
<switch>%FM-4-TCAM_LOU: Hardware TCAM LOU capacity exceeded
<switch>%FM-4-RACL_REDUCED: Interface Vlan1 routed traffic will be software switched in ingress direction(s)
...OR...
<router>%ACL-3-TCAMFULL:Acl engine TCAM table is full
<router>%ACL-3-RACLMAPCOMMITFAIL:Failed to map Router ACL to VLAN 1
<switch>%FM-4-TCAM-ENTRY: Hardware TCAM entry capacity exceeded
<switch>%FM-4-RACL_REDUCED: Interface Vlan1 routed traffic will be software switched in ingress direction(s)
```

Layer 3 ACLs—Solution Errors When Applying ACL

- The “Acl engine is out of logical operation unit” message is caused when too many Layer 4 operators are included in a ACL

  L4Ops are gt (1/2 LOU), lt (1/2 LOU), neq (1/2 LOU), range (1 LOU)
  A maximum of 9 L4Ops per router ACL
  A maximum of 32 LOUs for the TCAM
Layer 3 ACLs—Solution
Errors When Applying ACL

- The “Acl engine TCAM table is full” message is caused when the total ACEs for all ACLs on the 6500 are more then what can be programmed into the TCAM

  The PFC has a maximum of 16K entries, shared by RACLs, VACLs, and QoS
  The PFC2 has a maximum of 32K entries, shared by RACLs and VACLs

- To prioritize the programming of one VLANs ACL over another VLANs do the following:

```
interface Vlan1
ip address 10.118.2.58 255.255.255.0
ip access-group 100 in
tcam priority high
```
Agenda

- Terminology
- Multi-Layer Switching
- Multicast Multi-Layer Switching
- Layer 3 Access Control Lists
- Layer 3 Quality of Service
- Redundancy Issues in the Catalyst 6000
- FlexWan Basics

L3 Quality of Service—Problem
L3 QoS Not Applied

- QoS was configured on a VLAN interface, but when traffic was sent through the interface it was not shaped or policed as configured
L3 Quality of Service—Solution
L3 QoS Not Applied

- Layer 3 Quality of Service applied to a VLAN interface will not work as intended, as most of the traffic will be switched by the L3 Switching engine on the Supervisor.
- Either configure Policing/Shaping in CatOS, or use a native interface in Native IOS.

Agenda

- Terminology
- Multi-Layer Switching
- Multicast Multi-Layer Switching
- Layer 3 Access Control Lists
- Layer 3 Quality of Service
- Redundancy Issues in the Catalyst 6000
- FlexWan Basics
Redundancy—Problem
Hybrid Long Fail-Over Times

• When the primary supervisor fails on a Cat6000 L2 should recover in 2-3 seconds, and L3 should recover in 2-5 seconds.

Redundancy—Solution
Hybrid Long Fail-Over Times

• On the supervisor make sure the High-Availability is enabled AND operational

Switch> (enable) show system highavailability
Highavailability: enabled
Highavailability versioning: disabled
Highavailability Operational-status: ON
Redundancy—Solution
Hybrid Long Fail-Over Times

- On the MSFC make sure that HSRP is configured on both MSFCs

```
Router# show standby vlan 2
Vlan2 - Group 0
  Local state is Active, priority 110, may preempt
  Hello time 3 holdtime 10
  Next hello sent in 00:00:00.628
  Hot standby IP address is 172.10.1.254 configured
  Active router is local
  Standby router is 172.10.1.3 expires in 00:00:09
  Standby virtual mac address is 0000.0c07.ac00
  2 state changes, last state change 00:00:13
```

Redundancy—Problem
Hybrid Dual MSFC Systems

- ACLs configured on one MSFC in a dual supervisor system are not applied
- Routes that appear on only one MSFC2 of a dual supervisor 2 system do not get routed in hardware
Redundancy—Solution
Hybrid Dual MSFC Systems

- In dual MSFC systems one MSFC is selected as the designated router
- The designated router is responsible for programming the hardware on the supervisor

```
Router# show redundancy
Designated Router: 1 Non-designated Router: 2
Redundancy Status: designated
```

Agenda

- Terminology
- Multi-Layer Switching
- Multicast Multi-Layer Switching
- Layer 3 Access Control Lists
- Layer 3 Quality of Service
- Redundancy Issues in the Catalyst 6000
- FlexWan Basics
**FlexWAN Module—Problem**

**FlexWAN Not Seen**

- A FlexWAN is installed into the chassis, but is not seen by either the Supervisor or the MSFC
- Hybrid is running at least 5.4(2)/12.1(1)EX
- Native IOS is running at least 12.1(6)E

---

**FlexWAN Module—Solution**

**FlexWAN Not Seen**

- The FlexWAN gets the code that it runs from the MSFC IOS image. So the MSFC must be running a –v image
- All Images from 12.1(5a)E are only available with –v

```
msfc15#sh ver
Cisco Internetwork Operating System Software
IOS (tm) MSFC2 Software (C6MSFC2-JSV-M), Version 12.1(7)E, EARLY
DEPLOYMENT RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/cgi-bin/ibld/view.pl?i=support
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 25-Apr-01 03:20 by eaarmas
Image text-base: 0x40008980, data-base: 0x41860000
<...some output deleted...>
```
FlexWAN Module—Solution
FlexWAN Not Seen

- The FlexWAN is only seen by the designated MSFC

```
router#show redundancy
Designated Router: 1 Non-designated Router: 2
Redundancy Status: designated

router#show version
<...some output deleted...>
1 FlexWAN controller (1 Serial)(4 T1).
2 Serial network interface(s)
509K bytes of non-volatile configuration memory.

16384K bytes of Flash internal SIMM (Sector size 512K).
Configuration register is 0x102
```

FlexWAN Module—Problem
FlexWAN Configuration

- Since the FlexWAN is only seen on one MSFC, how do you configure the redundant MSFC with the FlexWAN interfaces
FlexWAN Module—Solution
FlexWAN Configuration

• Config-sync makes the designated MSFC sync its configuration to the non-designated MSFC

```
redundancy
 high-availability
 config-sync

! interface Serial4/0/0
 ip address 10.1.1.2 255.255.255.0
 dsu bandwidth 44210
 framing c-bit

! interface Vlan2
 ip address 172.10.1.2 255.255.255.0 alt ip address 172.10.1.3 255.255.255.0
 ip pim dense-mode
 standby priority 110 preempt alt standby priority 90 preempt
 standby ip 172.10.1.1 alt standby ip 172.10.1.1
```

Before testing redundancy, make sure that HA is operating on the Supervisor and Config-Sync is operating on the MSFC

```
Switch> (enable) show system highavailability
Highavailability: enabled
Highavailability versioning: disabled
Highavailability Operational-status: ON

Router#show redundancy
Designated Router: 1 Non-designated Router: 2
Redundancy Status: designated
Config Sync AdminStatus : enabled
Config Sync RuntimeStatus : enabled
```
Troubleshooting Catalyst® Switches—Part 2

Session CDC-302

Please Complete Your Evaluation Form

Session CDC-302