Troubleshooting Catalyst Switches (Part I)

Session 2807
Objective

To be able to identify, resolve, and prevent problems associated with Catalyst®
series switches.

Agenda

- Client-Server Network Issues
- VLAN Assignment Issues
- Trunking Issues
- FastEtherChannel/GigEtherChannel
- Spanning Tree Issues
- Multilayer Switching Issues
Sample Problem

- Legacy client-server network has been working but is out of gas
- Replace shared bandwidth with switched, dedicated bandwidth
- At initial rollout users on workstations attached to Catalysts can’t log in

Life “B.C.” (Before Catalyst)

- Shared bandwidth
- Router backbone
- User segment, router, server segment
- Easily troubleshoot
Workstations Having Problems When on Switch

- DHCP request fails
- NetWare GNS request fails
- IPX® frame type discovery fails
- User login fails

Is the Workstation Connected?

```
Switch> (enable) show port 10/2
Port   Name  Status   Vlan  Level  Duplex Speed  Type
-----   -------  --------  -----  -------  ---------  -------
1/2     connected    17    normal half  100  100BaseTX
```
Is the Switch Receiving?

Switch> (enable) show mac 10/2

<table>
<thead>
<tr>
<th>MAC</th>
<th>Rcv-Frms</th>
<th>Xmit-Frms</th>
<th>Rcv-Multi</th>
<th>Xmit-Multi</th>
<th>Rcv-Broad</th>
<th>Xmit-Broad</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>---------</td>
<td>-----------</td>
<td>-----------</td>
<td>------------</td>
<td>-----------</td>
<td>------------</td>
</tr>
<tr>
<td>10/2</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC</th>
<th>Delv-Exced</th>
<th>MTU-Exced</th>
<th>In-Discard</th>
<th>Lrn-Discard</th>
<th>In-Lost</th>
<th>Out-Lost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Rcv-Unicast</th>
<th>Rcv-Multicast</th>
<th>Rcv-Broadcast</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Xmit-Unicast</th>
<th>Xmit-Multicast</th>
<th>Xmit-Broadcast</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Does the Switch Know the MAC Address?

- In this scenario the address is not learned for at least 15 seconds

Switch> (enable) show cam dynamic 10/2

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

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Dest MAC/Route Des</th>
<th>Destination Ports or VCs / [Protocol Type]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00-e0-b0-fb-0a-38</td>
<td>10/2 [ALL]</td>
</tr>
</tbody>
</table>

Total Matching CAM Entries Displayed = 1
Assessing the Situation

- Workstations get link
- The switch is transmitting almost nothing to workstation at first—takes 30 seconds
- The MAC address is not learned for the first 15 seconds of link even though workstation transmitted

Using the Clues

- The switch ports acts like they are blocked for 30 seconds
- After 30 seconds the switch starts forwarding normally
- It takes 15 seconds for the switch to start learning the MAC address
The “Root” Cause

- The Catalyst is an IEEE 802.1d transparent bridge and must normally go through 15 seconds of listening, then 15 seconds of learning before forwarding when link is asserted.
- During that 30 seconds, NetWare GNS, DHCP request, NT login, or frame-type discovery may fail.

The Solution

- Use the following command on Catalyst ports connected directly to workstations:

  ```
  Switch> (enable) set spantree portfast 2/5 enable
  ```

  Warning: SpanTree port fast start should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc. to a fast start port can cause temporary spanning tree loops. Use with caution.
  SpanTree port 2/5 fast start enabled.
On many of the new 10/100 blades for the Catalyst switches there are the features for Fast EtherChannel and trunking.

By default FEC and trunking are set to auto-negotiate, which also delay ports from forwarding packets.

To resolve the delay caused by FEC and trunking on client ports, disable these features with the following commands:

```
Switch> (enable) set port channel 2/5 off
Port(s) 2/5 are assigned to admin group 46.
Port(s) 2/5 channel mode set to off.
```

```
Switch> (enable) set trunk 2/5 off
Port(s) 2/5 trunk mode set to off.
```
To resolve all three causes of port startup delay in newer Catalyst code, the following command is a macro that configures all three options:

```
Switch> (enable) set port host 2/6-7
Port(s) 2/6-7 channel mode set to off.
Spantree ports 2/6-7 fast start enabled.
Port(s) 2/6-7 trunk mode set to off.
```
**Initial VLAN Assignments**

- Brand new switch with default configuration; assign some ports to a VLAN and they don’t appear!

```
Switch> (enable) set vlan 10 4/1-8
VLAN 10 modified.
VLAN 1 modified.
VLAN    Mod/Ports
----    -----------------------
10       4/1-8

Vlan 10 is not active.
Switch (enable) show vlan
VLAN    Name            Status  Mod/Ports, Vlans
----    ---------------  ------  ----------------------------
   1    default         active  1/1-2
       4/9-24
       5/1-12
1002   fddi-default    active
```

**VTP**

- VLANs cannot be added or deleted on a VTP client
- A VTP server must have a domain name configured to be active
- The factory default is server mode with no domain name!
- **Set vtp domain <something>** to correct
Use VTP transparent mode as a workaround only—not recommended long term to overcome factory defaults

Older versions of CWSI required all switches to either be client or server. This restriction does not exist with current versions of CWSI

VTP—The Big One

- An existing VTP domain is running well
- Add a new switch
- Almost all production VLANs get deleted everywhere!
A Working VTP Domain

VLAN 1
VLAN 2
VLAN 3
VLAN 4

New Switch with Higher Revision

VTP Rev 4
VTP Rev 7
VTP
VLAN 1
VLAN 2
VLAN 3
VLAN 4
VTP

- The revision number is incremented each time a VLAN is added or deleted via the set vlan and clear vlan commands
- Revision must be synched across entire VTP domain
- VLANs not known to the server of highest revision will be deleted
VTP

- Use show vtp domain early and often

```
Switch> show vtp domain
Domain Name Index Version Local Mode Password
----------------- ------------- ----------- ----------- ----------
mydomain 1 2 server -
Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- ------------- --------------
15 1023 5 4
Last Updater V2 Mode Pruning PruneEligible on Vlans
------------ ------ ------- --------------------------
172.20.44.30 enabled disabled 2-1000
```

VTP

- VTP meltdown can be introduced by either a VTP client or server (both are updaters)
- To set the revision number back for a new switch, either reboot it or set the vtp domain name to something bogus then set it back
- Always reset the VTP revision before deploying a new switch
VTP Pruning Feature

- Available in 2.3(1) and higher code
- VTP pruning will suppress flooding of broadcasts and multicasts across a trunk if no MAC addresses are learned from the other end of that trunk
- Conserves bandwidth on trunks but does not clear VLANs off of trunks

Agenda

- Client-Server Network Issues
- VLAN Assignment Issues
- Trunking Issues
- FastEtherChannel/GigEtherChannel
- Spanning Tree Issues
- Multilayer Switching Issues
Trunking

- A trunk is a link between two devices that carries multiple VLANs simultaneously
- ISL—Inter-Switch Link
- IEEE 802.10—Typically used on FDDI
- IEEE 802.1q—Used on Gigabit and optionally Fast Ethernet ports

Trunk Doesn’t Just Form

- Default setting for trunking is auto mode, yet no trunk when adjacent switches connected

Switch> (enable) show cdp neighbors detail
Device-ID: 066505512
Device Addresses:
  IP Address: 10.6.1.234
  Holdtime: 152 sec
Capabilities: TRANSPARENT_BRIDGE SR_BRIDGE SWITCH
Version:
  WS-C5505 Software, Version McpSW: 3.2(6) NmpSW: 3.2(6)
  Copyright (c) 1995-1999 by Cisco Systems
Platform: WS-C5505
Port-ID (Port on Device): 1/1
Port (Our Port): 1/1
Switch> (enable) show trunk
No ports trunking.
Five Modes of Trunking

• **off** means that the link will not trunk
• **auto** means that the link will negotiate but prefer not to trunk
• **desirable** means that the link will negotiate and prefer to trunk
• **on** means that the link will trunk and will respond to DTP

Trunking

• **nonegotiate** means that the link will trunk but will not listen to DTP
• nonegotiate should only be used a temporary workaround when trunk flapping (trunk/non-trunk) is occurring, or on links to devices that do not understand DTP
Trunking

- Recommended setting is desirable at the core connected to auto at the edge
- On to on is good if the link must trunk

A Broken Trunk Scenario

- Set both ends for on and yet the trunk won’t stay up
- Native VLAN mismatch

Switch> (enable) set trunk 1/1 on 1-1005 dot1q
Adding vlans 1-1005 to allowed list.
Please use the ‘clear trunk’ command to remove vlans from allowed list.
Port(s) 1/1 allowed vlans modified to 1-1005.
Port(s) 1/1 trunk mode set to on.
Port(s) 1/1 trunk type set to dot1q.
It-S500e (enable) 2000 Jul 15 06:42:02 %DTP-5-TRUNKPORTON: Port 1/1 has become dot1q trunk
2000 Jul 15 06:42:02 %DTP-5-TRUNKPORTON: Port 1/2 has become dot1q trunk
2000 Jul 15 06:42:04 %SPANTREE-2-RX_1QPVIDERR: Rcved pvid_inc BPDU on 1Q port 1/2 vlan 1.
2000 Jul 15 06:42:04 %SPANTREE-2-TX_BLKPORTPVID: Block 1/2 on xmitting vlan 1 for inc peer vlan.
2000 Jul 15 06:42:04 %SPANTREE-2-RX_BLKPORTPVID: Block 1/2 on rcvng vlan 1 for inc peer vlan.
2000 Jul 15 06:42:05 %SPANTREE-2-RX_1QPVIDERR: Rcved pvid_inc BPDU on 1Q port 1/1 vlan 5.
2000 Jul 15 06:42:05 %SPANTREE-2-TX_BLKPORTPVID: Block 1/1 on xmitting vlan 1 for inc peer vlan.
2000 Jul 15 06:42:05 %SPANTREE-2-RX_BLKPORTPVID: Block 1/1 on rcvng vlan 5 for inc peer vlan 1.
Native VLAN

- Native VLAN is the VLAN a port would be assigned to if it were not participating in a trunk
- In 802.1q, frames in the native VLAN are not tagged at all
- Native VLAN on each end of a trunk must match for correct operation

Another Broken Trunk

- A trunk is up but stations within the same VLAN on different switches cannot communicate
- VLANs were pruned manually and now don’t agree
Show trunk tells which VLANs are getting trunked

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1</td>
<td>auto</td>
<td>isl</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>

Port Vlans allowed on trunk

- 2/1 1-1005

Port Vlans allowed and active in management domain

- 2/1 1-2

Port Vlans in spanning tree forwarding state and not pruned

- 2/1 1-2

By default all VLANs (1–1005) get trunked

It is possible to manually add or delete VLANs off a trunk via the set trunk and clear trunk commands
DTP Feature

- Dynamic negotiation of trunking mode
- 4.2(1) or higher code required
- supports on, off, auto, desirable

Want to trunk? 802.1q or ISL? I am ISL -auto.

Trunks and Spanning Tree

- In ISL-trunked networks, there is one unique Spanning Tree per VLAN
- IEEE 802.1q VLANs require a single Spanning Tree for all VLANs
- Cisco offers proprietary PVST+ (per-VLAN Spanning Tree) feature for 802.1q networks
Agenda

- Client-Server Network Issues
- VLAN Assignment Issues
- Trunking Issues
- FastEtherChannel/GigEtherChannel
- Spanning Tree Issues
- Multilayer Switching Issues

EtherChannel

- EtherChannel® is a method of grouping multiple physical links between two devices into a single logical link
- This provides up to 4 GB full-duplex bandwidth between two switches
EtherChannel Doesn’t Just Form

- Default setting for EtherChannel is auto mode, yet no EtherChannel forms when adjacent switches are connected

```
lt-c5505-11a (enable) show cdp neighbor
* - indicates vlan mismatch.
# - indicates duplex mismatch.

Port   Device-ID     Port-ID     Platform
-------- ------------------------------- ------------------------- ------------
 2/1    066512851     2/1         WS-C5505
 2/2    066512851     2/2         WS-C5505

Switch> (enable) show channel
```

Switch> (enable) show channel
Channel Id Ports
--------- -----------------------------------------------

EtherChannel

- EtherChannel also has the **on**, **off**, **auto**, and **desirable** configuration states but they have slightly different meanings

- **on** means that the ports will channelize but will not run PAgP (Port Aggregation Protocol)
• **auto** means the ports will negotiate channelization (i.e. they listen for PAgP) but prefer not to form the channel

• **desirable** means that the ports will send and receive PAgP and will prefer to channelize

---

• **Warning**: auto to on will **not** work

• **Warning**: on to on will work but will not run PAgP

• Recommended is **desirable** to desirable
• Show port channel tells what is going on with FEC

<table>
<thead>
<tr>
<th>Channel Id</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>801</td>
<td>2/1-4</td>
</tr>
</tbody>
</table>

• Spanning tree must be disabled to do FEC on 2.4(x) code. FEC did not exist prior to 2.4(1)

• If FEC is misconfigured or if FEC detects a Spanning Tree loop, then it will place ports into the DISABLE state
Disable vs. Disabled

- If port is in DISABLE state then PAgP elected to shut the port because it detected a loop
- If port is in DISABLED state then the port has been administratively shutdown
- DISABLE is a clue that something is configured wrong

Agenda

- Client-Server Network Issues
- VLAN Assignment Issues
- Trunking Issues
- FastEtherChannel/GigEtherChannel
- Spanning Tree Issues
- Multilayer Switching Issues
Spanning Tree

- Robust network designs require redundancy
- Proper Spanning Tree execution is crucial to network uptime
- Spanning Tree must be carefully considered when deploying switched networks

Spanning Tree Port Types

- **Root Ports**: Port with Least Cost Path to the Root Bridge
- **Nondesignated Ports**: Ports in Blocking
- **Designated Ports**: Ports Selected for Forwarding
- **Direction of BPDU Flow**
Spanning Tree

- If no manual configuration is done, the network will run fine but there is one consideration:
  
  Where is the root? Without adjustment its location could be anywhere

- Blocking ports at the core of the network could pose problems

Who’s the Root?

I'm the Root?
Choose the Root

- The root of the tree should be in the very core of the network; typically server farm
- In current Catalyst software, use the `set spantree root` macro on the root switch
- In older Catalyst software manually lower the priority parameter

Be Careful

- Spanning Tree is rather complex
- Do not “tune” Spanning Tree parameters manually unless you fully understand, have a plan, and have a reason
- Abide by recommended guidelines for number of Spanning Tree instances
STP Parameters

- Network parameters
  - Hello interval
  - Forward delay
  - Max age
  - Bridge priority (per bridge)
- Port-specific parameters
  - Port cost
  - Port priority

Using Macro Commands

- Eliminate possible errors in manual setting of dozens of parameters
- Achieve settings recommended and tested
Set spantree root

- A macro that sets the bridge priority parameter to 8192 for the specified VLANs, 16384 for secondary roots
- Root bridge dictates hello interval for entire network

```
Switch> (enable) set spantree root 1 dia 2 hello 2
VLAN 1 bridge priority set to 8192.
VLAN 1 bridge max aging time set to 10.
VLAN 1 bridge hello time set to 2.
VLAN 1 bridge forward delay set to 7.
Switch is now the root switch for active VLAN 1.
```
- Use only in the “Access” (closet) layer of the network
- Never use in the core of the network
backbonefast

- A 4.1(x) and higher feature which can bypass waiting for Max Age timer to expire
- Uses a Remote Link Query (RLQ) PDU to test path to the root upon receipt of an inferior BPDU

Detecting Spanning Tree Loops

- Know your network before trouble begins
- Know where root of each tree is
- Know where all the blocked ports are
- Don’t do any tuning you don’t understand
Detecting Spanning Tree Loops

- `show system` will report high backplane utilization
- If STP loop is suspected check your blocked ports for errors using `show port`
- `show spantree <vlan>` to ensure it is correct

Correcting Spanning Tree Loops

- Are there any ports forwarding that should be blocking?
- Are any ports taking physical-layer errors?
- You can temporarily disable redundancy to clear the condition
Agenda

- Client-Server Network Issues
- VLAN Assignment Issues
- Trunking Issues
- FastEtherChannel/GigEtherChannel
- Spanning Tree Issues
- Multilayer Switching Issues

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
<...some output deleted...>

<table>
<thead>
<tr>
<th>MLS-RP IP</th>
<th>MLS-RP ID</th>
<th>XTAG</th>
<th>MLS-RP MAC-Vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Switch> (enable)
In configuring MLS order does matter. Enter the MLS interface commands in this order

```plaintext
mls rp vtp-domain <domain name>
mls rp vlan-id <vlan#>
mls rp ip
mls management-interface
```

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
```
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.

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>
MLS Entry Creation

- Both the Candidate Packet and the Enabled Packet must pass through the same switch for a flow to be built.

MLS Switching

- In this scenario switch 1 will not maintain an flow entry for the path between A and B.
The series of messages shown below is usually thought of as a MLS problem, but it actually and indicator of another problem—a bridge loop!

- **%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

**Final Thoughts**

- Learn and run show commands
- Plan before executing
- Beware the Spanning Tree
Troubleshooting Catalyst Switches

Course 2807

Please Complete Your Evaluation Form

Session 2807