What You Make Possible
Troubleshooting Cisco Catalyst 4500 Series Switches

BRKCRS-3142
Session Goal

At the End of this Session, You Should Be Able To:

- Understand various system resources and monitor their usage
- Troubleshoot popular access layer features on Catalyst 4500/4900 switches.
- Emphasis on newer products
  - Include tools: Netflow, EEM, Wireshark, …
  - IOS-XE, Sup7-E, Sup7L-E, 4500X, …
Agenda

- Products Overview
- Basic Troubleshooting Method
- Troubleshooting
  - Interface/Link
  - High CPU
  - IOS-XE Crashes
  - IOS-XE Licenses
  - QoS
  - Flexible NetFlow
  - Wireshark
- Misc. Tools and Tricks
- Summary
Catalyst 4500 +E, -E and Classic Chassis

Modular

24 Gbps per slot
- -E Chassis support 12.2(31)SGA6 onward
- Sup6-E, Sup6L-E and 46xx line card
- 4507R-E, 4510R-E

48 Gbps per slot
- +E Chassis support 12.2(53)SG4 onward
- Sup7-E, 47xx line card IOS-XE 3.2.n SG
- Sup7L-E, IOS-XE 3.2.0(XO), 3.3.0(SG)
- 4507R+E, 4510R+E, 4503-E, 4506-E

6 Gbps per slot
- E-Series and Classic supervisors
- Classic line cards
  - e.g, SupV-10GE, 45xx line card

See the appendix for supervisor, line card, and chassis product and compatibility details.
Architecture Overview
Centralized Architecture

- **Intelligent Supervisors**
  Supervisor Engine 7-E, 7L-E, 6-E, 6L-E, V-10GE, V, IV, II-Plus-10GE, II-Plus-TS, II-Plus

- **Transparent Line Cards**
  Wire-rate, oversubscribed, PoE
  10/100, 10/100/1000, GE, 10GE
  Various physical media front panel ports
  Dedicated per-slot bandwidth to supervisor

- **Switching ASICs**
  Packet Processor
  Forwarding Engine

- **Specialized Hardware**
  TCAM's for ACLs, QoS, L3 forwarding
  NetFlow (NFE) for statistics gathering

---

1. Ternary Content Addressable Memory
2. Optional for Supervisor IV and V. Integrated in Supervisor V-10GE, Sup7-E, 7L-E
Agenda

- Products Overview
- Basic Troubleshooting Method
- Troubleshooting
  - Interface/Link
  - High CPU
  - IOS-XE Crashes
  - IOS-XE Licenses
  - QoS
  - Flexible NetFlow
  - Wireshark
- Misc. Tools and Tricks
- Summary
Basic Troubleshooting Method

1. Define Problem
   - Symptoms? System Messages? User Input?

2. Gather Facts

3. Consider Possibilities
   - Need to have a good understanding about how the system looks like when it is healthy

4. Create Action Plan

5. Execute Action Plan

6. Observe Results

Documentation

Want to learn more? Check out CCNP Practical Studies: Troubleshooting by Donna Harrington.

Basic Troubleshooting Method

Brainstorm potential root causes

<table>
<thead>
<tr>
<th>Category</th>
<th>Possible Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Issue</td>
<td>Bad Hardware?</td>
</tr>
<tr>
<td></td>
<td>Transient Hardware?</td>
</tr>
<tr>
<td></td>
<td>Hardware Limitation?</td>
</tr>
<tr>
<td>Software Issue</td>
<td>Bugs?</td>
</tr>
<tr>
<td></td>
<td>Software Limitation?</td>
</tr>
<tr>
<td>Config/Design</td>
<td>Mis-configuration?</td>
</tr>
<tr>
<td></td>
<td>Reaching Capacity?</td>
</tr>
<tr>
<td>Traffic</td>
<td>DOS Attack?</td>
</tr>
<tr>
<td></td>
<td>Traffic Pattern Change?</td>
</tr>
<tr>
<td></td>
<td>Bad peer/server?</td>
</tr>
</tbody>
</table>

1. Define Problem
2. Gather Facts
3. Consider Possibilities
4. Create Action Plan
5. Execute Action Plan
6. Observe Results
Basic Troubleshooting Method

1. Define Problem
2. Gather Facts
3. Consider Possibilities
4. Create Action Plan
5. Execute Action Plan
6. Observe Results

• Further information and examples are in the later section “Troubleshooting”

What needs to be done to isolate each potential root cause?
Make a change, measure results, rollback change if problem persists
Problem solved? If not, continue action plan
Caution!

- **debug** and **show platform** commands to follow
- Excessive debug output to console may disable switch
- **show platform** commands are intended for in-depth troubleshooting by Cisco engineers
- Use **debug** and **show platform** commands only when advised by TAC
- **show platform** CLIs are not officially supported IOS commands
- Not all commands apply to all platforms.
  - Some are IOS-XE specific (Supervisor 7-E, 7L-E and 4500X-32)
Agenda

- Products Overview
- Basic Troubleshooting Method
- Troubleshooting
  - Interface/Link
  - High CPU
  - IOS-XE Crashes
  - IOS-XE Licenses
  - QoS
  - Flexible NetFlow
  - Wireshark
- Misc. Tools and Tricks
- Summary
Troubleshooting Interface/Link Issues

Analyzing Link Stability

- Up? Down? Flapping?
- Drops? No link? No PoE? Errors?
Troubleshooting Interface/Link Issues

Potential Issues

- Physical layer errors
- Packet drops
- Inline power
- Link flapping (Appendix)
  - logging event link-status
  - show platform software interface <> all | inc downs:\|PimPhyport
- Auto negotiation (Appendix)
  - show platform software interface <> mii

1. This command should be run twice and the results from the second run should be used.
## Troubleshooting Interface/Link Issues

### Physical Layer Errors

Catalyst-4506# `show interfaces g5/5 count errors | exclude \0\*0\*0\*0`  

<table>
<thead>
<tr>
<th>Port</th>
<th>CrcAlign-Err</th>
<th>Dropped-Bad-Pkts</th>
<th>Collisions</th>
<th>Symbol-Err</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi5/5</td>
<td>23736730</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Undersize</th>
<th>Oversize</th>
<th>Fragments</th>
<th>Jabbers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Single-Col</th>
<th>Multi-Col</th>
<th>Late-Col</th>
<th>Excess-Col</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Deferred-Col</th>
<th>False-Car</th>
<th>Carri-Sen</th>
<th>Sequence-Err</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See Appendix for Error descriptions

1. Match speed and duplex
2. Isolate bad hardware using “known good” hardware  
   - Switch port → optical module if applicable → Cable/Fiber → NIC
   
   *e.g. SFF8472-5-THRESHOLD_VIOLATION: Gi5/1: Rx power low alarm*
3. Exclude patch panel if possible
4. Peer misbehaving? Sniff wire for malformed frames
Troubleshooting Interface/Link Issues

Packet Drops

- **Symptom:** Intermittent connection issue due to packet drops

- **Gather Facts**
  - Check for physical layer issue
  - Check places where drop could occur
  - Check for changes in traffic pattern

- **Consider possibilities**
  - Physical Layer Error (i.e. CRC)
  - Congestion in Tx direction
  - Congestion in Rx direction

- Create and execute action plan

- Observe results
Troubleshooting Interface/Link Issues
Packet Drops in Transmit direction

Tx-Queue Full
- Over-subscription
- Peer is sending Pause frames

![Diagram showing packet processing engine, classic linecard, and front panel ports with drops and pause frames.]
Troubleshooting Interface/Link Issues

Packet Drops in Transmit direction

1. Is the port oversubscribed in the transmit direction?

```
SUP6-E# show interfaces g2/47 counters detail | begin Drops
Port     Tx-Drops-Queue-5  Tx-Drops-Queue-6  Tx-Drops-Queue-7  Tx-Drops-Queue-8
Gi2/47   0                  0                  0                37748571

SUP6-E# show interfaces g2/47 counters detail | begin Drops
Port     Tx-Drops-Queue-5  Tx-Drops-Queue-6  Tx-Drops-Queue-7  Tx-Drops-Queue-8
Gi2/47   0                  0                  0                37874327
```

Queue 8 is the default queue with no QoS Configured

2. Is the port’s peer sending pause frames?

```
SUP6-E# show interfaces g2/47 counters detail | begin RxPause
Port    Rx-No-Pkt-Buff    RxPauseFrames   TxPauseFrames   PauseFramesDrop
Gi2/47  0                  130                0                0

SUP6-E# show interfaces g2/47 counters detail | begin RxPause
Port    Rx-No-Pkt-Buff    RxPauseFrames   TxPauseFrames   PauseFramesDrop
Gi2/47  0                  133                0                0
```

Peer still Pausing
Troubleshooting Interface/Link Issues

4648 Linecard

Packet Drops in Receive direction
• Minimal buffer on receiving stub ASIC

The uplinks are two 3G links for each stub ASIC.

6 ports share one 3G link and oversubscription ratio is 2:1.

Note - 4748 is Linerate
Troubleshooting Interface/Link Issues
4648 Linecard Packet Drops in Receive Direction

- Incrementing (rxFifo stub) overruns

Sup6-E# show interface gi1/13 | include overrun
  0 input errors, 0 CRC, 0 frame, 86432 overrun, 0 ignored
Sup6-E# show interface gi1/13 | include overrun
  0 input errors, 0 CRC, 0 frame, 206658 overrun, 0 ignored

- Confirm incrementing Rx-No-Pkt-Buff

Sup6-E# show interface gi1/13 counter all | begin Rx-No
<table>
<thead>
<tr>
<th>Port</th>
<th>Rx-No-Pkt-Buff</th>
<th>RxPauseFrames</th>
<th>TxPauseFrames</th>
<th>PauseFramesDrop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/13</td>
<td>206658</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

- Check Platform Stub ASIC Counter (Optional)

- On Classic Linecards
  Sup6-E# show platform software interface g2/1/stub | in Rx No Packet Buffer
  Rx No Packet Buffer Count : 563740397

- On 46xx and 47xx Linecards
  Sup7-E# show platform software interface gi1/13 stub stat | in Overrun
  OverrunPackets : 206658 (look for Rx Stats)

- Rx-No-Pkt-Buff can also be due to global pkt buffer depletion – see QoS
Troubleshooting Power over Ethernet

- **Symptom:** IP phone is not powered on
- **Gather Facts**
  - Inspect hardware LEDs/Status
  - Analyze power allocation
- **Consider possibilities**
  - Insufficient power?
  - Bad phone/port/linecard/power supply
- **Create and execute action plan**
  - Use debug to check PoE negotiation
  - Change connections to isolate issue
- **Observe results**
Troubleshooting Power over Ethernet

Sanity Check

1. Inspect LEDs (You can check the LED status from CLI)

   SUP6-E# show environment status
   <snip>
   Supervisor Led Color : Green
   Module 1 Status Led Color : Green
   Module 2 Status Led Color : Green  PoE Led Color : Green

2. Analyze Power Status

   SUP6-E# show power detail

   Power
   Supply  Model No          Type       Status       Sensor   Status
   ------  ------------------  ---------  ------------  --------  -------
   PS1     PWR-C45-4200ACV   AC 4200W   good       good     good
   PS1-1   110V              good       good
   PS1-2   110V              good
   PS2     
   Watts Used of System Power(12V)
   Mod   Model                budgeted instantaneous peak out of reset in reset
   ----  ---------------------  ----------  ----------  ---------  --------
   1    WS-X4648-RJ45V-E      92          --          --        92        10
   2    WS-X4548-GB-RJ45V     60          --          --        60        25

- PoE is operational on the line card
- If not good, check power supply LEDs
- Linecards are fully powered
## Troubleshooting Power over Ethernet

### Sanity Check (Continued)

### 3. Analyze Power Budget

**SUP6-E# show power detail**

<table>
<thead>
<tr>
<th>Power Summary (in Watts)</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Used</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>System Power (12V)</td>
<td>847</td>
</tr>
<tr>
<td>Inline Power (-50V)</td>
<td>6</td>
</tr>
<tr>
<td>Backplane Power (3.3V)</td>
<td>40</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>893</strong></td>
</tr>
</tbody>
</table>

The switch tries to allocate the highest power level requested by the phone. For example, if the phone asks for 6, 8, or 10 W via CDP, and more than 10 W is available, the switch will allocate 10 W to the phone. **PoE white paper**


**Cisco Power Calculator:** [http://tools.cisco.com/cpc/launch.jsp](http://tools.cisco.com/cpc/launch.jsp)

### Catalyst 4500 power allocation rules:

1. Power line cards before IP phones
2. Prefer static over auto power
## 4. Analyze Line Card Status

**SUP6-E# show module**

<table>
<thead>
<tr>
<th>Mod</th>
<th>Ports</th>
<th>Card Type</th>
<th>Model</th>
<th>Serial No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>48</td>
<td>10/100/1000BaseT POE E Series</td>
<td>WS-X4648-RJ45V-E JAE1329EAVL</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>48</td>
<td>10/100/1000BaseT (RJ45)V, Cisco/IEEE</td>
<td>WS-X4548-GB-RJ45V JAE10244L7P</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>18</td>
<td>10GE (X2), 1000BaseX (SFP)</td>
<td>WS-X4606-X2-E JAE12021FMP</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>Sup 6-E 10GE (X2), 1000BaseX (SFP)</td>
<td>WS-X45-SUP6-E JAE1223KL3G</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>Sup 6-E 10GE (X2), 1000BaseX (SFP)</td>
<td>WS-X45-SUP6-E JAE12460E61</td>
<td></td>
</tr>
</tbody>
</table>

**M MAC addresses**

<table>
<thead>
<tr>
<th>Start</th>
<th>End</th>
<th>Hw</th>
<th>Fw</th>
<th>Sw</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0024.1446.2d93</td>
<td>0024.1446.2dc2</td>
<td>1.0</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0018.1958.cf70</td>
<td>0018.1958.cf9f</td>
<td>3.3</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>001d.4573.0ada</td>
<td>001d.4573.0aeb</td>
<td>1.0</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0022.90e0.d6c0</td>
<td>0022.90e0.d6c5</td>
<td>1.1</td>
<td>12.2(44r)SG 12.2(53)SG</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>0022.90e0.d6c6</td>
<td>0022.90e0.d6cb</td>
<td>1.2</td>
<td>12.2(44r)SG 12.2(53)SG</td>
<td>Ok</td>
</tr>
</tbody>
</table>

Other status includes: Faulty, Authfail, Offline, PwrOver, PwrMax, PwrDeny. See Appendix for details.

If not Ok, try resetting after executing all troubleshooting steps:

```
hw-module module <module> reset
```
Analyze Power Allocation
Phone Drawing More Power than it Should?

- What if device is exceeding power a little or at the start? – not IEEE compliant!
  - Solution – configure static power

```
SUP6-E# show power inline g1/48
...<Confirm Normal Operation – use detail option for additional debug>
SUP6-E# show running-config interface g2/2
interface GigabitEthernet2/2
  power inline police
SUP6-E# INLINEPOWEROVERDRAWN: Inline powered device connected on port Gi2/2 exceeded its policed threshold.
ERR_DISABLE: inline-power error detected on Gi2/2, putting Gi2/2 in err-disable state
SUP6-E#
SUP6-E# show power inline police g2/2
Available:1580(w) Used:77(w) Remaining:1503(w)

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Admin Police</th>
<th>Oper Police</th>
<th>Cutoff Power</th>
<th>Power Overdrawn</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi2/2</td>
<td>auto</td>
<td>errdisable</td>
<td>errdisable</td>
<td>overdrawn</td>
<td>0.0</td>
<td>0.0</td>
</tr>
</tbody>
</table>
```

Action: errdisable is default

Inline power policing available in 12.2(50)SG onward on 20+ W per port PoE line cards
IEEE and Cisco PD Negotiation

- Power Negotiation can occur via CDP, LLDP 802.3at or LLDP-MED
- Switch "locks" to first protocol packet (CDP or LLDP) that has the power negotiation TLV
- LLDP 802.3at power negotiation TLV overrides the LLDP-MED power negotiation TLV

- Recommend - disable all but the desired power negotiation protocols on the switch interface & peer

### Cat 4K Feature

<table>
<thead>
<tr>
<th>Cat 4K Feature</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP 802.1ab</td>
<td>12.2(44)SG</td>
</tr>
<tr>
<td>LLDP 802.3at PoE+ TLV, LLDP-MED</td>
<td>12.2(54)SG</td>
</tr>
</tbody>
</table>

- Sup6-E(config)# lldp run
- Sup6-E(config)# int gi 3/1
- Sup6-E(config-if)# lldp tlv-select power-management

- **Warning!** If protocols are mismatched at the two ends (switch and PD), power negotiation will fail!

802.3af PoE 12.95W
PoE vs. Data Issue

- Change connections
  - Try a different line card, phone or cable

- Is this a PoE issue or a PoE and data issue?
  - Disconnect phone, and connect non-PoE device

- Configure “power inline never” on the port
  - Verify the link comes up

- Collect additional debugs
  - `SUP6-E# show platform chassis module <id>`
  - `SUP6-E# debug interface g1/48`

Condition 1 set
- `SUP6-E# debug ilpower powerman`

- Disconnect PD, Connect PD, collect debugs
  - `SUP6-E# undebug all`
  - All possible debugging has been turned off
  - `SUP6-E# undebug interface g1/48`

Tips: When PoE is enabled on a port, auto MDIX is disabled. Please make sure you use the correct cable type. See the note in the Catalyst4500 configuration guide.

Includes – various register dumps, electrical current usage, interrupts, …

- Power device (PD)/phone not powering up at all?
  - Confirm the device is IEEE compliant, check with vendor
  - Validate with 3rd party PD testers
  - Device capacitance or impedance as per IEEE?
Analyze Power Allocation

- Does the PoE line card support **enough power per port?**
- Does the PoE line card support **enough power?** (slots 3-10 pair limit in 4510)

<table>
<thead>
<tr>
<th>Line Card</th>
<th>PoE per Line Card</th>
<th>PoE per Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-X4748-UPOE+E</td>
<td>1440</td>
<td>60W</td>
</tr>
<tr>
<td>WS-X4748-RJ45V+E</td>
<td>1440</td>
<td>30W</td>
</tr>
<tr>
<td>WS-X4648-RJ45V+E</td>
<td>750 W</td>
<td>30 W</td>
</tr>
<tr>
<td>WS-X4548-RJ45V+</td>
<td>1050 W</td>
<td>30 W</td>
</tr>
<tr>
<td>WS-X4648-RJ45V-E</td>
<td>750 W</td>
<td>20 W</td>
</tr>
<tr>
<td>WS-X4548-GB-RJ45V</td>
<td>750 W</td>
<td>15.4 W</td>
</tr>
<tr>
<td>WS-X4524-GB-RJ45V</td>
<td>750 W</td>
<td>15.4 W</td>
</tr>
<tr>
<td>WS-X4248-RJ45V</td>
<td>750 W</td>
<td>15.4 W</td>
</tr>
<tr>
<td>WS-X4248-RJ21V</td>
<td>750 W</td>
<td>15.4 W</td>
</tr>
<tr>
<td>WS-X4224-RJ45V</td>
<td>750 W</td>
<td>15.4 W</td>
</tr>
<tr>
<td>WS-X4148-RJ45V</td>
<td>750 W</td>
<td>7 W</td>
</tr>
<tr>
<td>WS-X4148-RJ21V</td>
<td>750 W</td>
<td>7 W</td>
</tr>
</tbody>
</table>


# Troubleshooting Link and PoE Issues

<table>
<thead>
<tr>
<th>Troubleshooting Steps</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Link debounce settings</td>
<td>show interfaces debounce</td>
</tr>
<tr>
<td>Check number of debounce events</td>
<td>show platform software interfaces mii</td>
</tr>
<tr>
<td>Check Digital Optical Monitoring Data</td>
<td>show interface &lt;&gt; transceiver detail</td>
</tr>
<tr>
<td>Verify PoE line card is online</td>
<td>show module</td>
</tr>
<tr>
<td>Verify inline power available and operational</td>
<td>show power detail</td>
</tr>
<tr>
<td>Verify the inline power status of the port</td>
<td>show power inline &lt;interface&gt; [detail]</td>
</tr>
<tr>
<td>Verify PoE line card supports enough power per port, per slot</td>
<td>Appendix table, line card datasheets</td>
</tr>
<tr>
<td>Verify phone is not drawing more power than it should</td>
<td>show power inline police &lt;interface&gt;</td>
</tr>
<tr>
<td>Verify power negotiation is successful</td>
<td>debug interface &lt;interface&gt;</td>
</tr>
<tr>
<td></td>
<td>debug ilpower powerman</td>
</tr>
<tr>
<td></td>
<td>undebug all</td>
</tr>
<tr>
<td></td>
<td>undebug interface &lt;interface&gt;</td>
</tr>
<tr>
<td>Gather various module specific debugs</td>
<td>show platform chassis module &lt;id&gt;</td>
</tr>
</tbody>
</table>
Agenda

- Products Overview
- Basic Troubleshooting Method
- Troubleshooting
  - Interface/Link
  - High CPU
  - IOS-XE Crashes
  - IOS-XE Licenses
  - QoS
  - Flexible NetFlow
  - Wireshark
- Misc. Tools and Tricks
- Summary
Monitoring System Health
Baselining and Troubleshooting the Platform

- Packet Processor
- Forwarding Engine
- Line Card
  - Front Panel Ports
  - Stub ASICs
- Supervisor 7-E
  - MPC 8572 dual core
  - Utilization Low? Normal? High?
- Shared Packet Memory
- TCAMs
- CPU
- Tx Queue Memory
Troubleshooting High CPU

- **Symptom:** CPU usage is higher than expected baseline value

- **Gather Facts**
  - Analyze IOS-XE Processes
  - Analyze IOS processes
  - Analyze Platform Depending Processes
  - Analyze Traffic

- **Consider possibilities**
  - Out of system resources?
  - Unexpected traffic / DoS Attack?
  - Software bug?
  - Mis-configuration / Expected behavior?

- **Create and execute action plan**

- **Observe results**
CPU Tasks Overview

What Does the Catalyst 4500 CPU Do?

- Runs IOS/IOS-XE
- Runs Catalyst 4500 processes
- Sends and receives control packets
  - BPDU • CDP • VTP • PAgP • LACP • DTP • UDLD • and more!
- Processes packets not supported in hardware
  - Host learning • IPX • Appletalk • protocol control packets • ARP • packets with IP options • packets with expired TTL • IP tunneling • SNMP* • Telnet* • SSH* • ACL logging • RPF failure • packet fragmentation • CPU as SPAN source • DHCP and IGMP snooping • ICMP unreachable • ACLs programmed in software, and others …

* If the Catalyst 4500 switch is the destination.
### System Show Commands

**SUP7-E# show process cpu**

Core 0: CPU utilization for five seconds: 2%; one minute: 2%; five minutes: 2%
Core 1: CPU utilization for five seconds: 2%; one minute: 1%; five minutes: 1%

<table>
<thead>
<tr>
<th>PID</th>
<th>Runtime(ms)</th>
<th>Invoked</th>
<th>uSecs</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>TTY</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>869</td>
<td>618</td>
<td>140672</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>init</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>79</td>
<td>11050</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>kthreadd</td>
</tr>
<tr>
<td>3</td>
<td>737</td>
<td>128263</td>
<td>5749</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>migration/0</td>
</tr>
<tr>
<td>9433</td>
<td>2921947</td>
<td>113125288</td>
<td>1</td>
<td>4.20</td>
<td>4.53</td>
<td>4.10</td>
<td>0</td>
<td>iosd</td>
</tr>
</tbody>
</table>

**SUP7-E# show processes cpu detailed process iosd sorted**

Core 0: CPU utilization for five seconds: 4%; one minute: 2%; five minutes: 2%
Core 1: CPU utilization for five seconds: 6%; one minute: 3%; five minutes: 2%

<table>
<thead>
<tr>
<th>PID</th>
<th>T</th>
<th>C</th>
<th>TID</th>
<th>Runtime(ms)</th>
<th>Invoked</th>
<th>uSecs</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>TTY</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>9433</td>
<td>L</td>
<td></td>
<td>11383</td>
<td>1131416</td>
<td>0</td>
<td>6.70605</td>
<td>A</td>
<td>4.39062</td>
<td>4.12207</td>
<td>0</td>
<td>iosd</td>
</tr>
<tr>
<td>9433</td>
<td>L</td>
<td>1</td>
<td>984896</td>
<td>4669930</td>
<td>0</td>
<td>7.11</td>
<td>A</td>
<td>5.44</td>
<td>5.11</td>
<td>0</td>
<td>iosd</td>
</tr>
<tr>
<td>9433</td>
<td>L</td>
<td>1</td>
<td>1961205</td>
<td>6644042</td>
<td>0</td>
<td>6.22</td>
<td>A</td>
<td>5.44</td>
<td>5.11</td>
<td>0</td>
<td>iosd</td>
</tr>
<tr>
<td>9433</td>
<td>L</td>
<td>1</td>
<td>829</td>
<td>18630</td>
<td>0</td>
<td>0.00</td>
<td>A</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>iosd</td>
</tr>
<tr>
<td>71</td>
<td>I</td>
<td></td>
<td></td>
<td>55575</td>
<td>8787502</td>
<td>1.11</td>
<td>R</td>
<td>1.00</td>
<td>1.00</td>
<td>0</td>
<td>Cat4k Mgmt HiPri</td>
</tr>
<tr>
<td>52</td>
<td>I</td>
<td></td>
<td></td>
<td>4221576</td>
<td>2152734</td>
<td>0.33</td>
<td>R</td>
<td>0.33</td>
<td>0.33</td>
<td>0</td>
<td>IDB Work</td>
</tr>
<tr>
<td>72</td>
<td>I</td>
<td></td>
<td></td>
<td>1033445</td>
<td>1988579</td>
<td>0.33</td>
<td>R</td>
<td>0.33</td>
<td>0.33</td>
<td>0</td>
<td>Cat4k Mgmt LoPri</td>
</tr>
<tr>
<td>89</td>
<td>I</td>
<td></td>
<td></td>
<td>4</td>
<td>132</td>
<td>0.00</td>
<td>R</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>Exec</td>
</tr>
<tr>
<td>161</td>
<td>I</td>
<td></td>
<td></td>
<td>15088</td>
<td>3355425</td>
<td>0.00</td>
<td>R</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>CEF, IPv4 process</td>
</tr>
<tr>
<td>6</td>
<td>I</td>
<td></td>
<td></td>
<td>0</td>
<td>1</td>
<td>0.00</td>
<td>R</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>IPC ISSU Receive Pr</td>
</tr>
<tr>
<td>5</td>
<td>I</td>
<td></td>
<td></td>
<td>0</td>
<td>1</td>
<td>0.00</td>
<td>R</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>Retransmission of I</td>
</tr>
<tr>
<td>8</td>
<td>I</td>
<td></td>
<td></td>
<td>280</td>
<td>35866</td>
<td>0.00</td>
<td>R</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>Pool Manager</td>
</tr>
</tbody>
</table>

**Processes you used to see in traditional IOS**

- Cat4k Mgmt HiPri
- IDB Work
- Cat4k Mgmt LoPri
- Exec
- CEF, IPv4 process
- IPC ISSU Receive Pr
- Retransmission of I
- Pool Manager
Troubleshooting High CPU, Continued

NOTE: Catalyst 4500 and 4900 switches can maintain hardware switching while the CPU is high.

Troubleshooting High CPU, Continued

1. Identify the culprit process

```
SUP7-E# show processes cpu detailed process iosd sorted | exc 0.00% 0.00%
CPU utilization for five seconds: 99%/0%; one minute: 83%; five minutes: 74%
```

```
<table>
<thead>
<tr>
<th>PID</th>
<th>Runtime(ms)</th>
<th>Invoked</th>
<th>uSecs</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>TTY</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>54</td>
<td>17854928</td>
<td>8896641</td>
<td>2004</td>
<td>67.91%</td>
<td>56.57%</td>
<td>40.44%</td>
<td>0</td>
<td>Cat4k Mgmt LoPr</td>
</tr>
<tr>
<td>115</td>
<td>95652</td>
<td>491125</td>
<td>194</td>
<td>26.87%</td>
<td>21.82%</td>
<td>9.43%</td>
<td>0 IP Input</td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>4130652</td>
<td>17306489</td>
<td>234</td>
<td>3.03%</td>
<td>3.04%</td>
<td>3.08%</td>
<td>0</td>
<td>Cat4k Mgmt HiPr</td>
</tr>
<tr>
<td>121</td>
<td>143860</td>
<td>1265474</td>
<td>113</td>
<td>0.39%</td>
<td>0.33%</td>
<td>0.34%</td>
<td>0</td>
<td>Spanning Tree</td>
</tr>
<tr>
<td>179</td>
<td>68548</td>
<td>21100380</td>
<td>3</td>
<td>0.07%</td>
<td>0.06%</td>
<td>0.06%</td>
<td>0</td>
<td>HSRP Common</td>
</tr>
<tr>
<td>38</td>
<td>10752</td>
<td>342104</td>
<td>31</td>
<td>0.07%</td>
<td>0.06%</td>
<td>0.07%</td>
<td>0</td>
<td>IDB Work</td>
</tr>
<tr>
<td>7</td>
<td>299140</td>
<td>46492</td>
<td>6434</td>
<td>0.00%</td>
<td>0.11%</td>
<td>0.07%</td>
<td>0</td>
<td>Check heaps</td>
</tr>
<tr>
<td>7</td>
<td>299140</td>
<td>46492</td>
<td>6434</td>
<td>0.00%</td>
<td>0.11%</td>
<td>0.07%</td>
<td>0</td>
<td>Inline power inc</td>
</tr>
<tr>
<td>42</td>
<td>113948</td>
<td>6550</td>
<td>17396</td>
<td>0.00%</td>
<td>0.02%</td>
<td>0.00%</td>
<td>0</td>
<td>Per-minute Jobs</td>
</tr>
</tbody>
</table>

Cat4k specific management processes

2. Collect detailed information on Cat4k management processes

```
SUP7-E# show platform health
```

```
<table>
<thead>
<tr>
<th>K5CpuMan</th>
<th>%CPU</th>
<th>%CPU Target</th>
<th>Average %CPU</th>
<th>Total</th>
<th>CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review</td>
<td>30.00</td>
<td>70.81</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

CPU manager process is beyond its target
Troubleshooting High CPU, Continued

3. Determine if any CPU queues are dropping packets

SUP7-E# show platform cpu packet statistics

Packets Dropped by Packet Queue

<table>
<thead>
<tr>
<th>Queue</th>
<th>Total</th>
<th>5 sec avg</th>
<th>1 min avg</th>
<th>5 min avg</th>
<th>1 hour avg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ip Option</td>
<td>10715071</td>
<td>118803</td>
<td>71866</td>
<td>15919</td>
<td>0</td>
</tr>
</tbody>
</table>

SUP7-E# show platform cpu packet statistics

Packets Dropped by Packet Queue

<table>
<thead>
<tr>
<th>Queue</th>
<th>Total</th>
<th>5 sec avg</th>
<th>1 min avg</th>
<th>5 min avg</th>
<th>1 hour avg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ip Option</td>
<td>15167180</td>
<td>112673</td>
<td>84910</td>
<td>27502</td>
<td>0</td>
</tr>
</tbody>
</table>

CPU queue drop in IP Option incremented
Troubleshooting High CPU, Continued

4. SPAN CPU to glean more info about the packets

```
SUP7-E# show running-config | include monitor

monitor session 1 source cpu rx
monitor session 1 destination interface Gi1/48

SUP7-E# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
  RX Only : CPU
Destination Ports : Gi1/48
  Encapsulation : Native
  Ingress : Disabled
  Learning : Disabled
```
Troubleshooting High CPU, Continued

4. SPAN CPU using debug tools

```
SUP7-E# debug platform packet all buffer
platform packet debugging is on
SUP7-E# show platform cpu packet buffered
Total Received Packets Buffered: 1024
-------------------------------------
Index 0:
3 days 23:23:18:54927 - RxVlan: 1006, RxPort: Gi1/1
Priority: Normal, Tag: No Tag, Event: 11, Flags: 0x40, Size: 64
Eth: Src 00:00:0B:00:00:00 Dst 00:22:90:E0:D6:FF Type/Len 0x0800
Ip: ver:IpVersion4 len:24 tos:0 totLen:46 id:0 fragOffset:0 ttl:64
proto:tcp
    src: 10.10.10.100 dst: 172.16.100.100 hasIpOptions firstFragment
lastFragment
Remaining data:
  0: 0x0 0x64 0x0 0x64 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
  10: 0x0 0x0 0x50 0x0 0x0 0x0 0x0 0x8A 0x37 0x0 0x0 0x0 0x0 0x0
  20: 0x0 0x1 0xB5 0x77 0x6A 0x7E
```

Note: This command does not pose any significant CPU overhead and therefore could be used even under high CPU load. Make sure “buffer” is used instead of “log”
System Show Commands

- Show process
- Show process detailed process <process name>\(^1\)
- Show process cpu
- Show process cpu detailed process <process name>\(^1\)
- Show process memory
- Show process memory detailed process <process name>\(^1\)
- Show memory
- Show memory detailed process <process name>\(^1\)
- Show buffer
- Show buffers detailed process iosd\(^1\)

1. IOS-XE command
# Common Cause for Punting Traffic to CPU

<table>
<thead>
<tr>
<th>Common Cause</th>
<th>Recommended Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same interface forwarding</td>
<td>change design, use “no ip redirect”</td>
</tr>
<tr>
<td>ACL logging</td>
<td>disable ACL logging</td>
</tr>
<tr>
<td>ACL deny causing switch to send ICMP unreachable</td>
<td>no ip unreachables$^2$</td>
</tr>
<tr>
<td>Forwarding/Feature exception (out of TCAM/adj space)</td>
<td>reduce TCAM usage resize TCAM region (TCAM2/3)</td>
</tr>
<tr>
<td>SW-supported feature (i.e.GRE)</td>
<td>disable the feature or reduce the amount of traffic</td>
</tr>
<tr>
<td>IP packets with TTL&lt;2</td>
<td>disable the offending traffic</td>
</tr>
<tr>
<td>IP packets with options</td>
<td>disable the offending traffic Control Plane Policing (CoPP)$^1$</td>
</tr>
<tr>
<td>Unexpected control/data traffic</td>
<td>Control Plane Policing (CoPP)</td>
</tr>
</tbody>
</table>

1. CoPP is supported on all legacy supervisor on 12.2(31)SG or newer release
   CoPP is supported on SUP6-E/SUP6L-E /4900M/4948E on 12.2(50)SG or newer release, Sup7-E, Sup7L-E, 4500X IOS-XE 3.1.0(SG) or newer
2. Should be configured on all the L3 interfaces of the switch.
## Troubleshooting High CPU

### Command Summary

<table>
<thead>
<tr>
<th>Troubleshooting Steps</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check CPU usage on IOS threads</td>
<td><code>show process cpu detailed process iosd [sorted]</code></td>
</tr>
<tr>
<td>Check CPU usage on platform dependent threads</td>
<td><code>show platform health</code></td>
</tr>
<tr>
<td>Check traffic on the CPU queue</td>
<td><code>show platform cpu packet statistics</code></td>
</tr>
<tr>
<td>SPAN the traffic send to the CPU queue</td>
<td><code>monitor session 1 source cpu rx</code></td>
</tr>
<tr>
<td></td>
<td><code>monitor session 1 destination interface Gi1/48</code></td>
</tr>
<tr>
<td>SPAN the traffic send to the CPU queue using</td>
<td><code>debug platform packet all buffer</code></td>
</tr>
<tr>
<td>internal inband capture tool</td>
<td><code>show platform cpu packet buffered</code></td>
</tr>
</tbody>
</table>
# System Show Memory Commands

Similar Concepts Apply to Other Show Process/Memory Commands

## SUP7-E# show processes memory sorted

System memory : 2011684K total, 766145K used, 1245539K free, 85468K kernel reserved
Lowest(b) : 701665280

<table>
<thead>
<tr>
<th>PID</th>
<th>Text</th>
<th>Data</th>
<th>Stack</th>
<th>Dynamic</th>
<th>RSS</th>
<th>Total</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>9433</td>
<td>67796</td>
<td>798408</td>
<td>84</td>
<td>260</td>
<td>958692</td>
<td>1016172</td>
<td>iosd</td>
</tr>
<tr>
<td>4894</td>
<td>1132</td>
<td>202012</td>
<td>84</td>
<td>4696</td>
<td>33064</td>
<td>277488</td>
<td>ffmpeg</td>
</tr>
<tr>
<td>4890</td>
<td>620</td>
<td>723312</td>
<td>84</td>
<td>6264</td>
<td>20856</td>
<td>761528</td>
<td>eicored</td>
</tr>
<tr>
<td>7696</td>
<td>144</td>
<td>200536</td>
<td>84</td>
<td>1448</td>
<td>20048</td>
<td>221512</td>
<td>cli agent</td>
</tr>
</tbody>
</table>

## SUP7-E# show processes memory detailed process iosd

Processor Pool Total: 805306368 Used: 248185408 Free: 557120960
I/O Pool Total: 16777216 Used: 169360 Free: 16607856

<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>Allocated</th>
<th>Freed</th>
<th>Holding</th>
<th>Getbufs</th>
<th>Retbufs</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>247024032</td>
<td>6004936</td>
<td>229557272</td>
<td>0</td>
<td>0</td>
<td><em>Init</em></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2411464</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td><em>Sched</em></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>42496728</td>
<td>40453336</td>
<td>1396176</td>
<td>5409841</td>
<td>362940</td>
<td><em>Dead</em></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>395048</td>
<td>3328656024</td>
<td>435080</td>
<td>0</td>
<td>0</td>
<td>Chunk Manager</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>184</td>
<td>184</td>
<td>37032</td>
<td>0</td>
<td>0</td>
<td>Load Meter</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>40032</td>
<td>0</td>
<td>0</td>
<td>Deferred Events</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>44600</td>
<td>11664</td>
<td>40048</td>
<td>0</td>
<td>0</td>
<td>SpanTree Helper</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>40032</td>
<td>0</td>
<td>0</td>
<td>Retransmission</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>40032</td>
<td>0</td>
<td>0</td>
<td>IPC ISSU Receive</td>
</tr>
</tbody>
</table>

Processors you used to see in traditional IOS:

- iosd
- ffmpeg
- eicored

- chunk manager
- load meter
- deferred events
- span tree helper
- retransmission
- ipa issu receive

Shows memory held by process
Agenda

- Products Overview
- Basic Troubleshooting Method
- Troubleshooting
  - Interface/Link
  - High CPU
  - IOS-XE Crashes
  - IOS-XE Licenses
  - QoS
  - Flexible NetFlow
  - Wireshark
- Misc. Tools and Tricks
- Summary
IOS-XE Architecture

- IOS-XE kernel is Linux
  - Iosd, ffm, licensed are applications
- Process crashes cause crashinfo file and (optionally) core file

1. Enhanced crash dump is supported on Sup6-E from 15.0(2)SG.

15.0(2)SG and SG1 – crashdump missing in classic Sups. Missing board specific information in –E series Sups.
Crash files in IOS-XE

Crashinfo

- All process crashes create crashinfo file
- Essential process crash results in supervisor reload
- IOSd crashdump has extra features
  - All processes follow IOS-XE crashinfo format
  - IOSd crashdump = IOS-XE crashinfo + classic IOS crashdump features
  - E.g., IOSd crashdump has CLI cmds, log buffer and chunk malloc & free
- Extra features extended to other processes from IOS-XE 3.3.0(SG) onwards
- Crashinfo is similar to IOS show platform crashdump
- Crashinfo files (text) are small (< 1MB)
- Crashinfo: partition – 135 MB on Sup7-E
Core files in IOS-XE

Fullcore

- Fullcore is the Linux core dump for crashing process
- Fullcore files (binary) can be large
  - FFM with max L3 routes can be 130 MB

```
Sup7-E(config)# exception coredump
Enables the generation of compressed process core dump file
```

```
SUP7-E#show exception information
Exception configuration information
Coredump file - disabled, compressed enabled
Maximum number of files
  Core - 10 file(s)
  Process crashinfo - 10 file(s)
Configured storage devices
  1 - crashinfo:
    2 - not assigned
    3 - not assigned
Dump protocol - not configured                   (not supported)
```

Recommended!
Kernel files in IOS-XE
Kinfo and Koops

- Kernel crashes are rare
  - create kinfo_file, koops.dat
- Kinfo files in kinfo: partition
  - show platform kinfo and show platform slavekinfo
- Collect all
  - crashinfo, fullcore, kinfo, koops.dat files around the time of the crash and provide TAC
  - If you have syslog server, collect output for 24 hours prior to crash
- Recommended software to see kinfo
  - IOS-XE 3.2.n and 15.0(1r)SG5
Crash CLIs in IOS-XE

Sup7-E#show exception files
Exception crashinfo files:
Most Recent Crashinfo file:
  crashinfo:crashinfo_iosd_20101103-201110-UTC
Files in crashinfo:
  crashinfo_iosd_20101021-044244-UTC
  fullcore_iosd_20101021-044244-UTC
  crashinfo_iosd_20101103-201110-UTC
Sup7-E#dir crashinfo:

Sup7-E(config)#exception crashinfo maximum-files?
<1-20> A value between 1-20

Sup7-E(config)#exception dump device?
second Second search device to store crashinfo
third Third device to store crashinfo
Sets the second and third storage devices that are checked for available
storage space for saving the new crash files.
crashinfo: is default device cannot be changed

Sup7-E(config)#exception dump device second usb0: (e.g., usb, sd cards)

•dir crashinfo: and dir slavecrashinfo: in "sh tech" from IOS-XE 3.2.0(SG)
•crashinfo:last_crashinfo and slavecrashinfo:last_crashinfo give the names of the most recent crashinfo files on Active and Standby
Agenda

- Products Overview
- Basic Troubleshooting Method
- Troubleshooting
  - Interface/Link
  - High CPU
  - IOS-XE Crashes
  - IOS-XE Licenses
  - QoS
  - Flexible NetFlow
  - Wireshark
- Misc. Tools and Tricks
- Summary
IOS-XE Licensing (CSL)

Overview

- Cisco Software Licensing – CSL is used in IOS-XE

Universal Image
  Entservices, Ipbase & LANbase license levels
  Universal K9
  Universal image with crypto module

Feature Sets
  Entservices
  Ipbase
  Lanbase

Universal Image
  Entservices
  Ipbase
  Lanbase

Feature Set License

Entservices
Ipbase
Lanbase

=
IOS-XE Licensing

Overview

- Permanent license is node-locked
- License is for a chassis UDI (Universal Device Identifier), but stored on Supervisor bootflash
- License synced to hot standby supervisor

*Product Activation Key (PAK) is NOT generated*
License Show Commands

Show License All

Sup7e# show license all
License Store: Primary License Storage
StoreIndex: 0 Feature: internal_service  Version: 1.0 License Type: Evaluation
   Evaluation period left: 23 hours 59 minutes  License State: Active, Not in Use, EULA accepted
... StoreIndex: 2 Feature: entservices  Version: 1.0  License Type: Permanent
   License State: Active, In Use
... License Store: Dynamic License Storage
StoreIndex: 0 Feature: entservices  Version: 1.0  License Type: Evaluation
   Evaluation total period: 8 weeks 4 days  Evaluation period left: 4 weeks 3 days
   License State: Inactive
... Sup7e# show license in-use
<Shows license being used currently>

1. Licenses tied to UDI are stored in primary storage. Licenses not tied to UDI are stored in Dynamic License storage
2. End User License Agreement (EULA) acceptance is needed for evaluation or expiring licenses (not for Permanent)
Troubleshooting License Installation

License Must Be Installed and Operational

Problem – Switch does not boot with the desired license

Consider Possibilities

– Is license accessible? Is license installed? Is license operational?

• The system will boot up with default Lanbase license level if no licenses are installed

```
Sup7e# dir bootflash:
44268 ... Jan 4 2011 21:46:41 ...7slot_ent_FOX1418GEW0_20110103155106655.lic
```

```
sup7e#license install
bootflash:7slot_ent_FOX1418GEW0_20110103155106655.lic
Installing licenses from
"bootflash:7slot_ent_FOX1418GEW0_20110103155106655.lic
Installing...Feature:entservices...Successful:Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install
```
Troubleshooting License Installation

Is License Operational?

Sup7e# `show license all`
License Store: Primary License Storage
StoreIndex: 2  Feature: entservices  Version: 1.0
  License Type: Permanent
  License State: Active, Not in Use
  License Count: Non-Counted
  License Priority: Medium

• Solution - Reboot required to make the license operational

Sup7e# `show version`
Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3 Switch Software
(cat4500e-UNIVERSAL-M), Version 03.01.00.SG RELEASE SOFTWARE (fc4)
License Information for 'WS-X45-SUP7-E'
  License Level: lanbase  Type: Default. No valid license found
  Next reboot license Level: entservices
Troubleshooting License Installation

License Operational After Reboot

• Save configuration and reload

Sup7e# show license all
License Store: Primary License Storage
StoreIndex: 2 Feature: entservices  Version: 1.0
    License Type: Permanent
    License State: Active, In Use
    License Count: Non-Counted
    License Priority: Medium

Sup7e# show version
Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3 Switch Software (cat4500e-UNIVERSAL-M), Version 03.01.00.SG RELEASE SOFTWARE (fc4)

License Information for 'WS-X45-SUP7-E'
    License Level: entservices  Type: Permanent
    Next reboot license Level: entservices
License Installation – Dual Sups

License Bootlevel: HA Upgrade

- Software upgrade from say IPbase to Entservices
- Problem – Repeated SSO switchovers are not upgrading software
  - Entservices license is installed
- Standby supervisor will always boot to the same license level as that of Active supervisor

Consider possibility – new license level not operational

Solution
1. Active running IPbase license and redundancy mode is SSO
2. Upgrade to Entservices license
   use “license install <>”
3. Change license boot level

Sup7e(config)#license boot level entservices
License Installation – Dual Sups
License Bootlevel: HA Upgrade

4. Save configuration
   `Sup7e# write mem`

5. Reload Active
   `Sup7e# redundancy force-switchover`

6. New Active running Ipbase
7. Standby comes up in RPR mode and running Entservices
8. Reload the Active – RPR switchover
9. New Active running Entservices
   Small traffic loss with RPR switchover
10. Standby comes up in SSO mode and running Entservices
Troubleshooting Built-in License
License Bootlevel: Using a Built-In or Demo

- Problem – Switch boots to Lanbase even with built-in evaluation Entservices license
- Consider possibility – license not operational

- Solution
  - Customer needs to use a built-in or demo license for emergency purpose
  - Boot level needs to be forced

```
Sup7e(config)# license boot level entservices
```

- Save and reload to take effect

Note - Switch will boot to Lanbase if no license present
# Troubleshooting Licensing

## Command Summary

<table>
<thead>
<tr>
<th>Troubleshooting Steps</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display all licenses</td>
<td>show license all</td>
</tr>
<tr>
<td>Currently used license</td>
<td>show license in-use</td>
</tr>
<tr>
<td>Detailed license information</td>
<td>show license detail &lt;feature name&gt;</td>
</tr>
<tr>
<td>Displays evaluation license</td>
<td>show license evaluation</td>
</tr>
<tr>
<td>Displays expiring license</td>
<td>show license expiring</td>
</tr>
<tr>
<td>Shows all the license files</td>
<td>show license file</td>
</tr>
<tr>
<td>Shows all permanent licenses</td>
<td>show license permanent</td>
</tr>
<tr>
<td>Displays license statistics</td>
<td>show license statistics</td>
</tr>
<tr>
<td>Brief summary of license(s)</td>
<td>show license summary</td>
</tr>
</tbody>
</table>
Agenda

- Products Overview
- Basic Troubleshooting Method
- Troubleshooting
  - Interface/Link
  - High CPU
  - IOS-XE Crashes
  - IOS-XE Licenses
  - QoS
  - Flexible NetFlow
  - Wireshark
- Misc. Tools and Tricks
- Summary
Sup 7-E Packet Flow with QoS

- Sequential processing
  - Ingress - Classify, Police, Mark
  - Egress - Classify, Police, Mark
  - Egress - Queue

- Modular QoS CLI (MQC) model used
  - Same in Sup6-E, SupL-E, 4900M, 4948E(-F), Sup7-E, Sup7L-E and 4500X-32
**Configuring Auto QoS**

Auto QoS on Sup7-E and Related

<table>
<thead>
<tr>
<th>Classification</th>
<th>Marking</th>
<th>Queuing</th>
<th>Policing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>policy-map AutoQos-VoIP-Input-Dscp-Policy</strong></td>
<td><strong>set dscp ef</strong></td>
<td><strong>priority</strong></td>
<td><strong>set dscp cs3</strong></td>
</tr>
<tr>
<td><strong>class AutoQos-VoIP-Bearer-Dscp</strong></td>
<td><strong>set cos 5</strong></td>
<td><strong>police cir percent 33</strong></td>
<td><strong>set bandwidth remaining percent 5</strong></td>
</tr>
<tr>
<td><strong>set qos-group 46</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>class AutoQos-VoIP-Control-Dscp26</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>set qos-group 26</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>class AutoQos-VoIP-Control-Dscp24</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>set qos-group 24</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:** QoS group is like an internal label and typically used for the following purpose:

1. To leverage a large range of traffic classes
2. If changing the Precedence or DSCP value is undesirable.

- Auto QoS macros used for voice/phones
  - e.g., `config-if# auto qos voip cisco-phone`
- Also available for video devices in IOS15.1(1)SG1, IOS-XE 3.3.0

---

Notes: `dbl`, shape, bandwidth, queue-limit and priority commands are queuing commands
Troubleshooting QoS Actions

SUP6-E# show policy-map int gi1/36 output
GigabitEthernet1/36

Service-policy output: AutoQos-VoIP-Output-Policy

Class-map: AutoQos-VoIP-Bearer-QosGroup (match-all)

625530530 packets
Match: qos-group 46
QoS Set
  ip dscp ef
  cos 5
priority queue:
  Transmit: 32344068480 Bytes, Queue Full Drops: 0 Packets
police:
  cir 33 %
  cir 330000000 bps, bc 10312500 bytes
conformed Packet count - n/a,
  transmit
exceeded Packet count - n/a,
  drop
conformed 325185000 bps, exceed 97368000 bps

Notes: Input classification displays the statistics using the packet counts, Queuing and Policing display the statistics using “bytes”, classmap stats are shared across interfaces with the same policy map
**Troubleshooting QoS**

**Check Hardware Resources**

<table>
<thead>
<tr>
<th>CAM Utilization Statistics</th>
<th>Used</th>
<th>Free</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input Security (160)</strong></td>
<td>42</td>
<td>(2 %)</td>
<td>2006</td>
</tr>
<tr>
<td><strong>Input Security (320)</strong></td>
<td>66</td>
<td>(3 %)</td>
<td>1982</td>
</tr>
<tr>
<td><strong>Input Qos (160)</strong></td>
<td>15</td>
<td>(0 %)</td>
<td>2033</td>
</tr>
<tr>
<td><strong>Input Qos (320)</strong></td>
<td>14</td>
<td>(0 %)</td>
<td>2034</td>
</tr>
<tr>
<td><strong>Input Forwarding (160)</strong></td>
<td>2</td>
<td>(0 %)</td>
<td>2046</td>
</tr>
<tr>
<td><strong>Input Unallocated (160)</strong></td>
<td>0</td>
<td>(0 %)</td>
<td>55296</td>
</tr>
</tbody>
</table>

QoS uses the same feature TCAM as security

Check TCAM usage for ACLs, security, L3 routes, PBR, DHCP Snoop, IPSG, WCCPv2, etc.

TCAM exhausted?

C4K_HWACLMAN-4-ACLHWPROGERR: ... hardware TCAM limit, qos being disabled on relevant interface.
Troubleshooting QoS
Applying Output QoS on Etherchannel

- MQC for port-channels on the Sup6-E/Sup7-E
  - Policy with queuing actions – only physical ports
  - Policy with non-queuing actions – only port channel

```
SUP6-E(config-if)# int Te5/1
SUP6-E(config-if)# service-policy output uplink
% A service-policy with non-queuing actions should be attached to the port-channel associated with this physical port.

SUP6-E(config-if)# int port-channel 1
SUP6-E(config-if)# service-policy output uplink
% A service-policy with queuing actions can be attached in output direction only on physical ports.
```
Output QoS on Etherchannel

```plaintext
policy-map non-queue
    class AutoQos-VoIP-Bearer-QosGroup
        set dscp ef
        set cos 5
        police cir 600000000
    class AutoQos-VoIP-Control-QosGroup26
        set dscp af31
        set cos 3

policy-map queue-only
    class AutoQos-VoIP-Bearer-QosGroup
        priority
    class AutoQos-VoIP-Control-QosGroup26
        bandwidth remaining percent 5
    class class-default
        dbl

interface Port-channel 1
    switchport
    service-policy input AutoQos-VoIP-Input-Cos-Policy
    service-policy output non-queue
end

interface Te5/1
    channel-group 1 mode on
    service-policy output queue-only
```

*Note – Auto QoS is not supported on etherchannel*
## Queue Memory Allocation

<table>
<thead>
<tr>
<th>Entry</th>
<th>Sup6-E or Sup6L-E or Sup7L-E</th>
<th>Sup7-E Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total queue memory</td>
<td>512K</td>
<td>1M</td>
</tr>
<tr>
<td>Free Reserve: global pool</td>
<td>100K (200 Chunks)</td>
<td>100K</td>
</tr>
<tr>
<td>CPU port &amp; Drop queue</td>
<td>20K</td>
<td>40K</td>
</tr>
<tr>
<td>Queue entries per slot(^1)</td>
<td>(x = 400K / nSlots(^2))</td>
<td>(X = 860K / nSlots)</td>
</tr>
<tr>
<td>Queue entries per port on a line card</td>
<td>(y = x / nPorts(^3))</td>
<td>(y = x / nPorts)</td>
</tr>
<tr>
<td>Queue entries per class transmit queue</td>
<td>(z = y / nTxQs(^4))</td>
<td>(z = y / nTxQs)</td>
</tr>
</tbody>
</table>

1. In a redundant chassis, two supervisor slots are treated as one
2. \(nSlots\) – number of Slots
3. \(nPorts\) – number of Ports in a line card
4. \(nTxQs\) – number of transmit queues in use

Use this to check queue memory:

```
show platform software qm
```
### Queue Memory Allocation

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Queue Depth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without qos service-policy or non-queuing qos service-policy</td>
<td>Control packet queue: 16&lt;br&gt;Default queue: min(y -16, 8184)</td>
</tr>
<tr>
<td>With queuing service-policy with some queues with queue-limit and some without</td>
<td>Queues with queue-limit: specified size&lt;br&gt;Queues without queue-limit: min(y / 8, 8184)&lt;br&gt;Default queue without queue-limit: any valid size between 56 to 8184</td>
</tr>
</tbody>
</table>

\[ y = \text{Queue entries per port on a line card} \]

**What if allocated queue memory exceeds port limit?**

- Free Reserve queue memory will be used – check `show platform software qm | inc Chunk`
- When Free Reserve memory is exhausted:
  - `%C4K_HWPORTMAN-3-TXQUEUEALLOCFAILED: Failed to allocate the needed queue entries for Gi6/13`
  - Solution – decrease queue depths on a per port basis, combine classes under the same queue
Transmit Queue Allocation

```
policy-map egress_queueing
  class dscp32-48
    police cir 990000
      conform-action transmit
      exceed-action drop
    priority
  class dscp0-15
    bandwidth 250000
    queue-limit 400
  class dscp16-31
    bandwidth 250000
    queue-limit 512
  class class-default

Sup6E-4503E# show platform hardware interface g2/48 tx-queue

<table>
<thead>
<tr>
<th>Phyport</th>
<th>T x Q</th>
<th>Head</th>
<th>Tail</th>
<th>Pre Empty</th>
<th>Empty Num Packets</th>
<th>BaseAddr</th>
<th>Size</th>
<th>Shape-Ok</th>
<th>TxQ Subport</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi2/48</td>
<td>0</td>
<td>0x0000</td>
<td>0x0000</td>
<td>True</td>
<td>0</td>
<td>0x5ECE8</td>
<td>352</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>Gi2/48</td>
<td>1</td>
<td>0x0000</td>
<td>0x0000</td>
<td>True</td>
<td>0</td>
<td>0x000000</td>
<td>0</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>Gi2/48</td>
<td>2</td>
<td>0x0000</td>
<td>0x0000</td>
<td>True</td>
<td>0</td>
<td>0x000000</td>
<td>0</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>Gi2/48</td>
<td>3</td>
<td>0x0000</td>
<td>0x0000</td>
<td>True</td>
<td>0</td>
<td>0x000000</td>
<td>0</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>Gi2/48</td>
<td>4</td>
<td>0x0000</td>
<td>0x0000</td>
<td>True</td>
<td>0</td>
<td>0x000000</td>
<td>0</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>Gi2/48</td>
<td>5</td>
<td>0x0000</td>
<td>0x0000</td>
<td>True</td>
<td>0</td>
<td>0x5EB58</td>
<td>512</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>Gi2/48</td>
<td>6</td>
<td>0x0000</td>
<td>0x0000</td>
<td>True</td>
<td>0</td>
<td>0x5EB58</td>
<td>400</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>Gi2/48</td>
<td>7</td>
<td>0x008A</td>
<td>0x0088</td>
<td>False</td>
<td>1421</td>
<td>0x5EE48</td>
<td>1520</td>
<td>True</td>
<td>False</td>
</tr>
</tbody>
</table>
```

Low prty queues can be starved, policer recommended

Note - Reverse order of queues with respect to CLI except for the first and the last

The last queue is the default queue
Troubleshooting Shared Packet Memory

- Linked list of memory cells to store packets
- About 64K max in Sup6-E
- Packet memory utilization indicates traffic congestion
- Monitor freelist cell counter

```
Catalyst-4506# show platform hardware interface all | include FreeListCount
FreeListCount: 64268
Catalyst-4506# show platform hardware interface all | include FreeListCount
FreeListCount: 63100
Catalyst-4506# show platform hardware interface all | include FreeListCount
FreeListCount: 63140
Catalyst-4506# show platform hardware interface all | include FreeListCount
FreeListCount: 63148
```

Troubleshooting Shared Packet Memory

- Linked list of memory cells to store packets
- About 64K max in Sup6-E
- Packet memory utilization indicates traffic congestion
- Monitor freelist cell counter
Troubleshooting Shared Packet Memory

Packet Memory Depletion

Packet mem 64K*280Byte cells in Sup6-E & Sup6L-E, 128K*256Byte cells in Sup7-E & Sup7L-E

Potential Cause | Why?
--- | ---
Jumbo frames | • Shared packet memory divided into fixed-sized cells
• Large packets use more cells and pointers than small packets

Deep transmit queues and egress oversubscription | • Transmit queues contain pointers to packets in packet memory
• Packets stay in shared packet memory until transmitted
• If the transmit queue is full and deep, freeing packet memory will be delayed

Solution: Use queue-limit

(config)# Policy Map egress_queue_limit
class class-default
queue-limit 1024

Problem seen more with fixed configuration boxes.

Solution - max default queue limit reduced from 8184 to 3072 in 4500x and Sup7L-E

New global CLI introduced since 15.0(2)SG1/3.2.1(SG)

(config)# hw-module system max-queue-limit <value>

1. Needs Supervisor reload to take effect

Rx-No-Pkt-Buff will be seen on **show interface counter all**

Check interface txQs for tail drops
# Troubleshooting QoS

## Command Summary

<table>
<thead>
<tr>
<th>Troubleshooting Steps</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check QoS configuration</td>
<td>show running-config</td>
</tr>
<tr>
<td>Check classification/marking/policing on interface</td>
<td>show policy-map interface &lt;&gt;</td>
</tr>
<tr>
<td>Check freelist availability</td>
<td>show platform hardware interface all</td>
</tr>
<tr>
<td>Check QoS TCAM resource</td>
<td>show platform hardware acl statistics utilization brief</td>
</tr>
<tr>
<td>Check policer hardware resource</td>
<td>show platform hardware qos policer utilization</td>
</tr>
<tr>
<td>Check interface hardware tx-queue</td>
<td>show platform hardware interface &lt;&gt; tx-queue</td>
</tr>
<tr>
<td>Check various drops on interface</td>
<td>show interface &lt;&gt; count all</td>
</tr>
<tr>
<td>Check queue memory of various modules</td>
<td>show platform software qm</td>
</tr>
<tr>
<td>Check freelist memory</td>
<td>show platform hardware interface all</td>
</tr>
</tbody>
</table>
Agenda

- Products Overview
- Basic Troubleshooting Method
- Troubleshooting
  - Interface/Link
  - High CPU
  - IOS-XE Crashes
  - IOS-XE Licenses
  - QoS
  - Flexible NetFlow
  - Wireshark
- Misc. Tools and Tricks
- Summary
Troubleshooting Flexible NetFlow

Overview

- Flexible NetFlow (FnF) introduced with Sup7-E, Sup7L-E and 4500X-32
- Flexible NetFlow does not have a fixed tuple to collect
  - Original netflow - source IP address, destination IP address, source port number, destination port number, protocol type, Type of Service, and input interface
- Flow is user defined with Flexible NetFlow
- Flexible netflow supports L2, IPv4 and IPv6 fields
- Support both v9 and v5 export formats

Uses of Netflow

- Troubleshooting – profile for suspected patterns and port – take action, see Netflow and EEM\(^1\) integration
  - Network security
  - Usage monitoring and billing

Note – Flexible Netflow, EEM and Wireshark are not available with lanbase license

1. EEM - Automated operational management in real time, monitor for specific events, take predefined actions. Ciscolive 2012, BRKNMS-2030, TEC CRS-3000

Cisco Public
Troubleshooting Flow Export

- Problem – Flow stats not received at collector
- Approach - Consider various possibilities
  - Flow export is done with UDP. Possible packet loss
  - Verify connectivity to the collector
  - Netflow problem can be with the collector as well
  - Confirm NetFlow export version matches the collector
  - Mandatory fields are required for v5 export

```
Sup7-E(config)#flow exporter flowexporter1
Sup7-E(config-flow-exporter)#destination 10.10.22.22
Sup7-E(config-flow-exporter)#export-protocol netflow-v5
Sup7-E(config-vlan-config)#ip flow monitor flowmonitor1 input
```

Warning: Exporter flowexporter1 could not be activated because the following fields are mandatory:

- ipv4 source address
- ipv4 destination address
- transport source-port
- transport destination-port
- ipv4 protocol
Flow Cache Collisions

- Flow table size 8K hash buckets, 16 entries per bucket = 128K – usable approx. 108K because of hash collisions

- Flows stats can be missing due to Collisions or Isolation threshold

```
Sup7-E# show running flow monitor ipv4fm record ipv4fr
Sup7-E# show platform hardware flow table utilization
Netflow Hardware Table Bucket Usage Statistics
Buckets w/ X Bucket Count Used Entry Count Used Entries (% of Buckets) (% of Entries)
--------------- -------------- -------------- ----------------- -----------------  
0              8176 ( 99.8) 0      ( 0.0)                 
1              32    ( 0.1)  32    ( 0.0)                 
```

```
Sup7-E# show flow record ipv4fr
match ipv4 source address
match ipv4 destination address
collect counter packets
```

```
Sup7-E# show flow monitor ipv4fm cache format record
Cache size: 1024
Current entries: 32
High Watermark: 32
```

cache entries <> limits the number of flows on per-monitor basis - change cache size to 16

%C4K_HWFLOWMAN-5-FLOWUNACCOUNTEDPACKETS: Flow stats for 46444030 packets are not accounted due to hardware hash collisions or full hardware flow table

Solution – Increase Isolation threshold, try different keys to index
Netflow EEM Integration Example

- NetFlow Counters are available for EEM\(^1\)
- Consider an example which looks for packets that have Time To Live (TTL) less than or equal to 1 received by the router
- CPU processing is required to respond to packets with TTL value \(\leq 1\) – e.g., DoS attack
- EEM can take various actions, syslog, send SNMP trap, send email, …
- Available since IOS-XE 3.2.0(SG)

```
Sup7-E#show event manager version
Embedded Event Manager Version 3.20
```

### EEM Integration Example

1. Packets with TTL=1 sent to the switch
2. NetFlow Engine collects the flow capturing the TTL value:

<table>
<thead>
<tr>
<th>Sup7-E#sh runn flow record ttl</th>
<th>Sup7-E(config)# event manager applet ttl</th>
</tr>
</thead>
<tbody>
<tr>
<td>match ipv4 ttl</td>
<td>event nf monitor-name &quot;ttl&quot;</td>
</tr>
<tr>
<td>match ipv4 protocol</td>
<td>event-type create event1 entry-value &quot;2&quot;</td>
</tr>
<tr>
<td>match ipv4 source address</td>
<td>field ipv4 ttl entry-op lt</td>
</tr>
<tr>
<td>match ipv4 destination address</td>
<td>action 1.0 syslog msg</td>
</tr>
<tr>
<td>collect counter bytes</td>
<td>&quot;Flow Monitor $_nf_monitor_name reported Low TTL for $_nf_source_address $_nf_dest_address&quot;</td>
</tr>
<tr>
<td>collect counter packets</td>
<td></td>
</tr>
<tr>
<td>collect timestamp sys-uptime first</td>
<td></td>
</tr>
<tr>
<td>collect timestamp sys-uptime last</td>
<td></td>
</tr>
</tbody>
</table>

Sup7-E#sh runn flow monitor ttl

Current configuration:

```
flow monitor ttl
record ttl
cache timeout active 40
```

Sup7-E#sh runn int gi 6/1

```
o no switchport
ip flow monitor ttl input
ip address 10.10.10.2 255.255.255.254
```

3. Following Syslog is recorded:

```
%HA_EM-6-LOG: ttl: Flow Monitor ttl reported Low TTL for 10.10.10.3 10.10.10.4
```

---

**Flow Monitor is integrated with EEM**

**TTL 1 packets can cause High Cpu**

---

**Check – show flow monitor ttl cache format record for IP TTL: 1**
What NF Fields can EEM track?

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
<th>Datalink</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination IP addr</td>
<td>Destination IP addr</td>
<td>dot1q</td>
</tr>
<tr>
<td>DSCP</td>
<td>DSCP</td>
<td>Source MAC address</td>
</tr>
<tr>
<td>Precedence</td>
<td>Flow-label</td>
<td>Destination MAC address</td>
</tr>
<tr>
<td>Protocol</td>
<td>Hop-limit</td>
<td></td>
</tr>
<tr>
<td>Source IP address</td>
<td>Next-header</td>
<td></td>
</tr>
<tr>
<td>ToS</td>
<td>Precedence</td>
<td></td>
</tr>
<tr>
<td>Total-length</td>
<td>Protocol</td>
<td></td>
</tr>
<tr>
<td>TTL</td>
<td>Source IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Traffic-class</td>
<td></td>
</tr>
</tbody>
</table>

- **IPv4 Fields**: Destination IP addr, DSCP, Precedence, Protocol, Source IP address, ToS, Total-length, TTL
- **IPv6 Fields**: Destination IP addr, DSCP, Flow-label, Hop-limit, Next-header, Precedence, Protocol, Source IP address, Traffic-class
- **Datalink Fields**: dot1q, Source MAC address, Destination MAC address
- **Counter Fields**: Bytes, Packets
# Troubleshooting Flexible NetFlow

## Command Summary

<table>
<thead>
<tr>
<th>Troubleshooting Steps</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shows utilization of the FnF stats table</td>
<td>show platform hardware flow table utilization</td>
</tr>
<tr>
<td>Display flow mask information</td>
<td>show platform hardware flow mask</td>
</tr>
<tr>
<td>Show flow record</td>
<td>show flow record</td>
</tr>
<tr>
<td>Show flow monitor</td>
<td>show flow monitor</td>
</tr>
<tr>
<td>Show flow exporter</td>
<td>show flow exporter</td>
</tr>
<tr>
<td>Show flow usage for a monitor</td>
<td>show flow monitor &lt;&gt; cache format record</td>
</tr>
<tr>
<td>Filter, Sort and Display flows</td>
<td>show flow monitor &lt;&gt; cache ?</td>
</tr>
<tr>
<td></td>
<td>filter - filtering</td>
</tr>
<tr>
<td></td>
<td>format - formatting</td>
</tr>
<tr>
<td></td>
<td>sort - sorting</td>
</tr>
<tr>
<td></td>
<td>show flow monitor &lt;&gt; cache sort high counter top 4</td>
</tr>
</tbody>
</table>
Agenda

- Products Overview
- Basic Troubleshooting Method
- Troubleshooting
  - Interface/Link
  - High CPU
  - IOS-XE Crashes
  - IOS-XE Licenses
  - QoS
  - Flexible NetFlow
  - Wireshark
- Misc. Tools and Tricks
- Summary
Network Troubleshooting Using Wireshark

Overview

- Superior solution than SPAN/RSPAN
- Supported only on Sup7-E, Sup7L-E and 4500X
- Supported from IOS-XE 3.3.0(SG)
- Wireshark
  - Freeware
  - Supports wide variety of protocols
  - Bundled with the switch operating system
  - Onboard capture, filter, decode and display
  - User space process – wireshark crash will not affect or reload the switch
  - Upto 8 instances supported
  - All wireshark CLIs are exec mode (not config)
Wireshark Concepts

- **Key – Thinking about the Capture Point(s) in detail**
- **Capture point: describes the following**
  - Attachment point: describes to which traffic point and direction the wireshark feature is attached to (e.g., L2 or L3 interface, Vlan, SVI, …)
  - Filters: describes the platform-enforced, application-enforced conditions to which the packets are matched for selection. Filters can be implemented in hardware or software
    - Core filter – Any filter implemented in hardware ACL
    - Capture filter – Filter in wireshark software to write to file
    - Display filter – Filter in wireshark software before displaying
  - Action: describes the action for the selected packets (e.g., display)
  - Limits: sets conditions for terminating wireshark session (e.g., “duration 10” sec, number of packets)
  - Destination: tells where the packets have to be store (e.g., my-pcap file on bootflash)
Wireshark Best Practices

- Avoiding console spew
  - Do not display directly to console without a buffer, file or a duration limit

- Use a simple approach
  - Write to PCAP file on storage, display on switch or using laptop Wireshark GUI

- Avoiding high cpu
  - Only the core filter is implemented in hardware as ACLs. Use the most restricted filter possible
Wireshark Example

Sup7-E#monitor capture mycap int gi 6/1 in match ipv4 protocol tcp 10.1.1.1/32 any file location bootflash:mycap.pcap limit duration 3
Sup7-E#show monitor capture
Status Information for Capture mycap
    Target Type:
        Interface: GigabitEthernet6/1, Direction: in
    Status : Inactive
    Filter Details:
        IPv4
            Source IP:  10.1.1.1/32
            Destination IP:  any
        Protocol: tcp
    File Details:
        Associated file name: bootflash:mycap.pcap
    Buffer Details:
        Buffer Type: LINEAR (default)
    Limit Details:
        Packet Capture duration: 3
Wireshark Example

Sup7-E#monitor capture mycap start
monitor capture mycap start
*Apr 2 18:10:18.238: %BUFCAP-6-ENABLE: Capture Point mycap enabled.

Sup7-E#

Sup7-E#dir bootflash:mycap.pcap
14596 -rw- 32856 Apr 2 2012 18:10:21 +00:00 mycap.pcap

- Packet header display

Sup7-E#show monitor capture file bootflash:mycap.pcap
1 0.000000 10.1.1.1 -> 10.1.2.10 TCP [TCP ZeroWindow] 0 > 0 [<None>] Seq=1 Win=0 Len=70

- Packet detailed display

Sup7-E#show monitor capture file bootflash:mycap.pcap detailed
Frame 141: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits)
  Arrival Time: Apr 2, 2012 18:10:19.965938000 Universal
  Ethernet II, Src: aa:bb:cc:dd:ee:ff , Dst: 01:00:00:01:01
    Time to live: 50

Frame 139: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits)
  Arrival Time: Apr 2, 2012 18:10:19.941937000 Universal
  Time to live: 100

Sup7-E#show monitor capture file bootflash:mycap.pcap display-filter "ip.ttl == 100"
# Wireshark Commands

<table>
<thead>
<tr>
<th>Troubleshooting Steps</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a monitor</td>
<td>monitor capture mycap int gi x/y …</td>
</tr>
<tr>
<td>Display monitor details</td>
<td>show monitor capture</td>
</tr>
<tr>
<td>Start/stop a monitor session</td>
<td>monitor capture mycap start</td>
</tr>
<tr>
<td>Display a pcap file</td>
<td>show monitor capture file &lt;filename&gt;</td>
</tr>
<tr>
<td>Display a pcap file in detail</td>
<td>show monitor capture file &lt;filename&gt; detailed</td>
</tr>
<tr>
<td>Display a pcap file with filter</td>
<td>show monitor capture file &lt;filename&gt; display-filter “filter-detail”</td>
</tr>
<tr>
<td>Check if wireshark is running</td>
<td>show proc cpu</td>
</tr>
</tbody>
</table>
Agenda

- Products Overview
- Basic Troubleshooting Method
- Troubleshooting
  - Interface/Link
  - High CPU
  - IOS-XE Crashes
  - IOS-XE Licenses
  - QoS
  - Flexible NetFlow
  - Wireshark
- Misc. Tools and Tricks
- Summary
Embedded Event Manager

- Monitor and collect output using EEM

```plaintext
event manager applet high-cpu
event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.10.1 get-type exact entry-op
g entry-val "$80" poll-interval 10
action 1.0 syslog msg "HIGH_CPU! CPU is at: $snmp_oid_val"
action 2.0 cli command "enable"
action 2.1 cli command "show process cpu | redirect bootflash:cpu.txt"
action 2.2 cli command "configure terminal"
action 2.3 cli command "event manager scheduler suspend"
Sup6-E#
%HA_EM-6-LOG: TEST: HIGH_CPU! CPU is at: 99
```

- Using EEM as remedy or workaround

```plaintext
event manager applet interface-flapping
event syslog pattern ".*UPDOWN.*GigabitEthernet1/1.*" occurs 4
action 1.0 syslog msg "GigabitEthernet Interface 1/1 changed state 4 times"
action 2.0 cli command "enable"
action 2.2 cli command "configure terminal"
action 2.3 cli command "interface GigabitEthernet1/1"
action 2.4 cli command "shutdown"
%LINK-3-UPDOWN: Interface Gig...1/1, changed state to down
```
Misc. Tools and Tricks
L3 Counters on E-Series Platform

- ACL and L3 interface counter are NOT enabled by default on E-Series switch
- Limited (4K) statistics resources available – usage
  - Counters can be ipv4, ipv6, combined or separate
  - `show platform hardware vlan statistic summary`
    Check the Free Entries column
- Need to enable the counters manually using IOS commands

1. The E-Series supervisor and switch refers to Sup6-E, SUP6L-E, 4900M and 4948E(-F), Sup7-E, Sup7L-E and 4500X
Misc. Tools and Tricks

More Tips on Counter

- L3 interface counter does not work on SUP6-E?
  - Need “counter” keyword under interface VLAN configuration

```
SUP6-E# show interfaces vlan 10
Vlan10 is up, line protocol is up
<snip>
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
<snip>
0 packets input, 0 bytes, 0 no buffer
1 packets output, 80 bytes, 0 underruns
SUP6-E(config)# interface vlan 10
SUP6-E(config-if)# counter
SUP6-E# show int vlan 10
Vlan10 is up, line protocol is up
<snip>
5 minute input rate 1967000 bits/sec, 176 packets/sec
5 minute output rate 1967000 bits/sec, 176 packets/sec
L3 in Switched: ucast: 65014 pkt, 96350748 bytes - mcast: 0 pkt, 0 bytes
L3 out Switched: ucast: 65014 pkt, 96350748 bytes - mcast: 0 pkt, 0 bytes
65014 packets input, 96350748 bytes, 0 no buffer
65033 packets output, 96352268 bytes, 0 underruns
```

Counters showed all zeroes

Counters are now working correctly
Access-List Counter on E-Series Switch
Using Hardware Counters

- Not seeing counters on access list?
  - Need to add the keyword “hardware statistics”

```plaintext
SUP6-E# show access-lists 100
Extended IP access list 100
  10 deny tcp any any eq telnet
  20 permit ip any any (413 estimate matches)
SUP6-E#
SUP6-E# config terminal
SUP6-E(config)# access-list 100 hardware statistics
SUP6-E#
SUP6-E# show run | in access-list 100
access-list 100 deny tcp any any eq telnet
access-list 100 permit ip any any
access-list 100 hardware statistics
SUP6-E#
SUP6-E# show access-lists 100
Extended IP access list 100
  10 deny tcp any any eq telnet
  20 permit ip any any (194699 matches)
```
Misc. Tools and Tricks

Some Quick Tips

- Enable NTP to troubleshoot across switches
- Include date and time for debug and log messages
  - `service timestamps [debug, log] msec localtime show-timezone`
- Automatically output time and CPU utilization with each command (exec mode)
  - `terminal exec prompt timestamp`
- Include comments on the console as reminders
  - `Sup6E-4503E#!!! show module after peer reload`
  - `Sup6E-4503E# show module`
Misc. Tools and Tricks
Making Life Easier…

- Review open caveats sections in release notes
- Search Bug Toolkit for known issues
- Reference Output Interpreter to decode command output
- Reference System Message Guide for mitigation recommendations
- Smart Call Home in 12.2(52)SG
Agenda

- Products Overview
- Basic Troubleshooting Method
- Troubleshooting
  - Interface/Link
  - High CPU
  - IOS-XE Crashes
  - IOS-XE Licenses
  - QoS
  - Flexible NetFlow
  - Wireshark
- Misc. Tools and Tricks
- Summary
Troubleshooting the Catalyst 4500

Summary

- Top-down approach
  - Verify configuration is correct and hardware is good
  - Perform sanity check with IOS `show` commands
  - Dig deeper with Catalyst 4500 `show platform` commands

- Leverage tools
  - Preventive – traffic policing
  - Inspective – Netflow, wireshark
  - Corrective - EEM

- Reference online resources
  - Catalyst 4000 Troubleshooting TechNotes
  - Catalyst 4500 Configuration Guide and Release Notes
  - NetPro discussion groups on [http://www.cisco.com](http://www.cisco.com)

- Contact the Cisco Technical Assistance Center (TAC)
  - Provide output from `show tech-support`
Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Passport points for each session evaluation you complete.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.

Don’t forget to activate your Cisco Live Virtual account for access to all session material, communities, and on-demand and live activities throughout the year. Activate your account at the Cisco booth in the World of Solutions or visit www.ciscolive.com.
Final Thoughts

- Get hands-on experience with the Walk-in Labs located in World of Solutions, booth 1042
- Come see demos of many key solutions and products in the main Cisco booth 2924
- Visit www.ciscoLive365.com after the event for updated PDFs, on-demand session videos, networking, and more!
- Follow Cisco Live! using social media:
  - Facebook: https://www.facebook.com/ciscoliveus
  - Twitter: https://twitter.com/#!/CiscoLive
  - LinkedIn Group: http://linkd.in/CiscoLI
Appendix Topics

- Supervisors, line cards, and fixed configuration switches
- Link error counters
- Decode module status
- Additional Troubleshooting Information
  - Link flapping
  - Auto Negotiation
  - Packet Buffer Memory
  - SSO, NSF, ISSU
  - QoS on classic supervisor
  - TCAM Resources
  - Unicast Forwarding
  - L2 Multicast – IGMP Snooping
  - ACL Resources
  - Security Features
  - License migration – Chassis and Supervisor
## Supervisor Comparison

<table>
<thead>
<tr>
<th>Supervisor</th>
<th>Layer 2/3/4 Services</th>
<th>Bandwidth &amp; Throughput</th>
<th>Chassis Support</th>
<th>Line Cards</th>
<th>Uplinks</th>
<th>NetFlow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor 7-E</td>
<td>Full L2/3/4, enhanced routing, IPv6</td>
<td>848 Gbps</td>
<td>-E/+E Chassis</td>
<td>E-series &amp; classic</td>
<td>4x10GE</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>250 mpps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor 7L-E</td>
<td>Full L2/3/4, enhanced routing, IPv6</td>
<td>520 Gbps</td>
<td>-E/+E Chassis</td>
<td>E-series &amp; classic</td>
<td>2x10GE</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>225 mpps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor 6-E</td>
<td>Full L2/3/4, enhanced routing, IPv6</td>
<td>320 Gbps</td>
<td>All E-Series and Classic</td>
<td>E-Series &amp; Classic</td>
<td>4 x GE or 2 x 10 GE (TwinGig)</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>250 mpps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor 6L-E</td>
<td>Basic Layer 2/3/4</td>
<td>280 Gbps</td>
<td>All E-Series and Classic</td>
<td>E-Series &amp; Classic</td>
<td>2 x 10 GE, 4 x GE, 10 GE and 2 x GE, or 2 x GE and 10GE</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>225 mpps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor V-10GE</td>
<td>Full L2/3/4, enhanced routing, IPv6</td>
<td>136 Gbps</td>
<td>See Sup 6-E</td>
<td>Classic</td>
<td>4 x GE and 2 x 10GE</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>102 mpps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor V</td>
<td>See Sup V-10GE</td>
<td>96 Gbps</td>
<td>See Sup 6-E</td>
<td>Classic</td>
<td>2 x GE</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>72 Mpps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor IV</td>
<td>See Sup V-10GE</td>
<td>64 Gbps</td>
<td>All except 4510R-E &amp; 4510R</td>
<td>Classic</td>
<td>2 x GE</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>48 mpps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor II-Plus-10GE</td>
<td>Basic Layer 2/3/4</td>
<td>108 Gbps</td>
<td>See Sup IV</td>
<td>Classic</td>
<td>4 x GE and 2 x 10GE</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>81 mpps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor II-Plus</td>
<td>Basic Layer 2/3/4</td>
<td>64 Gbps</td>
<td>See Sup IV</td>
<td>Classic</td>
<td>2 x GE</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>48 mpps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor II-Plus-TS</td>
<td>Basic Layer 2/3/4</td>
<td>64 Gbps</td>
<td>4503-E 4503</td>
<td>Classic</td>
<td>8 x GE &amp; 12 10/100/1000 PoE</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>48 mpps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. EIGRP, OSPF, BGP, IS-IS.
2. IPv6 in software.
3. Bi-directional.
### Supervisor Comparison, Continued

<table>
<thead>
<tr>
<th>Supervisor</th>
<th>Unicast Routes</th>
<th>Security ACL &amp; QoS entries</th>
<th>Input &amp; Output Policers</th>
<th>NAC &amp; DHCP snooping entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor 7-E</td>
<td>256,000</td>
<td>128,000</td>
<td>16,000 input/output, user configurable</td>
<td>12,000</td>
</tr>
<tr>
<td>Supervisor 7L-E</td>
<td>64,000</td>
<td>64,000</td>
<td>16,000 input/output, user configurable</td>
<td>12,000</td>
</tr>
<tr>
<td>Supervisor 6-E</td>
<td>256,000</td>
<td>128,000</td>
<td>16,000 input/output, user configurable</td>
<td>12,000</td>
</tr>
<tr>
<td>Supervisor 6L-E</td>
<td>57,000</td>
<td>32,000</td>
<td>16,000 input/output, user configurable</td>
<td>3072</td>
</tr>
<tr>
<td>Supervisor V-10GE</td>
<td>128,000</td>
<td>64,000</td>
<td>8,000 each direction</td>
<td>6,000</td>
</tr>
<tr>
<td>Supervisor V</td>
<td>128,000</td>
<td>64,000</td>
<td>1,000 each direction</td>
<td>3,000</td>
</tr>
<tr>
<td>Supervisor IV</td>
<td>128,000</td>
<td>64,000</td>
<td>1,000 each direction</td>
<td>3,000</td>
</tr>
<tr>
<td>Supervisor II-Plus-10GE</td>
<td>32,000</td>
<td>32,000</td>
<td>512 each direction</td>
<td>3,000</td>
</tr>
<tr>
<td>Supervisor II-Plus</td>
<td>32,000</td>
<td>32,000</td>
<td>512 each direction</td>
<td>3,000</td>
</tr>
<tr>
<td>Supervisor II-Plus-TS</td>
<td>32,000</td>
<td>32,000</td>
<td>512 each direction</td>
<td>3,000</td>
</tr>
</tbody>
</table>
## Line Card Comparison

<table>
<thead>
<tr>
<th>Type</th>
<th>Line Card</th>
<th>Ports</th>
<th>Speed</th>
<th>Port Type</th>
<th>Wire-rate or Oversubscribed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>+E series</td>
<td>WS-4748-UPOE+E</td>
<td>48</td>
<td>10/100/1000</td>
<td>RJ45</td>
<td>Wire-rate</td>
</tr>
<tr>
<td></td>
<td>WS-4748-RJ45V+E</td>
<td>48</td>
<td>10/100/1000</td>
<td>RJ45</td>
<td>Wire-rate</td>
</tr>
<tr>
<td></td>
<td>WS-X4712-SFP+E</td>
<td>12</td>
<td>10GBASE-X</td>
<td>SFP+</td>
<td>2.5:1 oversubscribed</td>
</tr>
<tr>
<td>E-Series</td>
<td>WS-X4648-RJ45-E</td>
<td>48</td>
<td>10/100/1000</td>
<td>RJ45</td>
<td>2:1 oversubscribed</td>
</tr>
<tr>
<td></td>
<td>WS-X4640-CSFP-E</td>
<td>80</td>
<td>1000BASE-X</td>
<td>CSFP</td>
<td>4:1 oversubscribed</td>
</tr>
<tr>
<td></td>
<td>WS-X4624-SFP-E</td>
<td>24</td>
<td>1000BASE-X</td>
<td>SFP</td>
<td>Wire-rate</td>
</tr>
<tr>
<td></td>
<td>WS-X4612-SFP-E</td>
<td>12</td>
<td>1000BASE-X</td>
<td>SFP</td>
<td>Wire-rate</td>
</tr>
</tbody>
</table>
# Line Card Comparison

<table>
<thead>
<tr>
<th>Type</th>
<th>Line Card</th>
<th>Ports</th>
<th>Speed</th>
<th>Port Type</th>
<th>Wire-rate or Oversubscribed?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>E-Series</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WS-X4648-RJ45V-E</td>
<td>48</td>
<td>10/100/1000</td>
<td>RJ45</td>
<td>2:1 oversubscribed</td>
<td></td>
</tr>
<tr>
<td>WS-X4648-RJ45V+E</td>
<td>48</td>
<td>10/100/1000</td>
<td>RJ45</td>
<td>2:1 oversubscribed</td>
<td></td>
</tr>
<tr>
<td>WS-X4606-X2-E</td>
<td>6</td>
<td>10GBASE-X</td>
<td>X2 or SFP w/ TwinGig</td>
<td>2.5:1 (X2) and Wire-rate (SFP)</td>
<td></td>
</tr>
<tr>
<td><strong>Classic FE over Fiber</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WS-X4248-FE-SFP</td>
<td>48</td>
<td>1000BASE-X</td>
<td>SFP</td>
<td>Wire-rate</td>
<td></td>
</tr>
<tr>
<td>WS-X4124-FX-MT</td>
<td>24</td>
<td>100BASE-FX</td>
<td>MM MT-RJ</td>
<td>Wire-rate</td>
<td></td>
</tr>
<tr>
<td>WS-X4148-FX-MT</td>
<td>48</td>
<td>100BASE-FX</td>
<td>MM MT-RJ</td>
<td>Wire-rate</td>
<td></td>
</tr>
<tr>
<td>WS-X4148-FE-BD-LC</td>
<td>48</td>
<td>100BASE-BX10-D</td>
<td>SMF Single LC</td>
<td>Wire-rate</td>
<td></td>
</tr>
<tr>
<td><strong>Classic FE over Copper</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WS-X4124-RJ45</td>
<td>24</td>
<td>10/100</td>
<td>RJ45</td>
<td>Wire-rate</td>
<td></td>
</tr>
<tr>
<td>WS-X4148-RJ</td>
<td>48</td>
<td>10/100</td>
<td>RJ45</td>
<td>Wire-rate</td>
<td></td>
</tr>
<tr>
<td>WS-X4148-RJ21</td>
<td>48</td>
<td>10/100</td>
<td>RJ45</td>
<td>Wire-rate</td>
<td></td>
</tr>
<tr>
<td><strong>Classic FE PoE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WS-X4224-RJ45V</td>
<td>24</td>
<td>10/100</td>
<td>RJ45</td>
<td>Wire-rate</td>
<td></td>
</tr>
<tr>
<td>WS-X4248-RJ45V</td>
<td>48</td>
<td>10/100</td>
<td>RJ45</td>
<td>Wire-rate</td>
<td></td>
</tr>
<tr>
<td>WS-X4248-RJ21V</td>
<td>48</td>
<td>10/100</td>
<td>RJ21</td>
<td>Wire-rate</td>
<td></td>
</tr>
</tbody>
</table>
### Line Card Comparison, Continued

<table>
<thead>
<tr>
<th>Type</th>
<th>Line Card</th>
<th>Ports</th>
<th>Speed</th>
<th>Port Type</th>
<th>Wire-rate or Oversubscribed?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Classic GE over Fiber</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WS-X4302-GB</td>
<td>2</td>
<td>1000BASE-X</td>
<td>GBIC</td>
<td>Wire-rate</td>
<td></td>
</tr>
<tr>
<td>WS-X4306-GB</td>
<td>6</td>
<td>1000BASE-X</td>
<td>GBIC</td>
<td>Wire-rate</td>
<td></td>
</tr>
<tr>
<td>WS-X4418-GB</td>
<td>18</td>
<td>1000BASE-X</td>
<td>GBIC</td>
<td>2 ports Wire-rate 16 ports 4:1 oversubscribed</td>
<td></td>
</tr>
<tr>
<td>WS-X4448-GB-LX</td>
<td>48</td>
<td>1000BASE-LX</td>
<td>SFP</td>
<td>8:1 oversubscribed</td>
<td></td>
</tr>
<tr>
<td>WS-X4448-GB-SFP</td>
<td>48</td>
<td>1000BASE-X</td>
<td>SFP</td>
<td>8:1 oversubscribed</td>
<td></td>
</tr>
<tr>
<td>WS-X4506-GB-T</td>
<td>6 + 6</td>
<td>10/100/1000 &amp; 1000BASE-X</td>
<td>RJ45 with PoE &amp; SFP</td>
<td>Wire-rate</td>
<td></td>
</tr>
<tr>
<td><strong>Classic GE over Copper</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WS-X4424-GB-RJ45</td>
<td>24</td>
<td>10/100/1000</td>
<td>RJ-45</td>
<td>4:1 oversubscribed</td>
<td></td>
</tr>
<tr>
<td>WS-X4448-GB-RJ45</td>
<td>48</td>
<td>10/100/1000</td>
<td>RJ-45</td>
<td>8:1 oversubscribed</td>
<td></td>
</tr>
<tr>
<td>WS-X4548-GB-RJ45</td>
<td>48</td>
<td>10/100/1000</td>
<td>RJ-45</td>
<td>8:1 oversubscribed</td>
<td></td>
</tr>
<tr>
<td><strong>Classic GE over Copper PoE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WS-X4524-GB-RJ45V</td>
<td>24</td>
<td>10/100/1000</td>
<td>RJ-45</td>
<td>4:1 oversubscribed</td>
<td></td>
</tr>
<tr>
<td>WS-X4548-GB-RJ45V</td>
<td>48</td>
<td>10/100/1000</td>
<td>RJ-45</td>
<td>8:1 oversubscribed</td>
<td></td>
</tr>
</tbody>
</table>
# Fixed Configuration Switches

<table>
<thead>
<tr>
<th></th>
<th>WS-C4500X-32</th>
<th>Catalyst 4948E</th>
<th>Catalyst 4900M</th>
<th>Catalyst 4948-10GE</th>
<th>Catalyst 4948</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bandwidth</strong>¹</td>
<td>800 Gbps</td>
<td>176 Gbps</td>
<td>320 Gbps</td>
<td>136 Gbps</td>
<td>96 Gbps</td>
</tr>
<tr>
<td><strong>Throughput</strong></td>
<td>250 M</td>
<td>131 mpps (IPv4) and 110 mpps (IPv6)</td>
<td>250 mpps (IPv4) and 125 mpps (IPv6)</td>
<td>102 mpps</td>
<td>72 mpps</td>
</tr>
<tr>
<td><strong>IPv6</strong></td>
<td>In hardware</td>
<td>In hardware</td>
<td>In hardware</td>
<td>In software</td>
<td>In software</td>
</tr>
<tr>
<td><strong>Height</strong></td>
<td>1RU</td>
<td>1 RU</td>
<td>2 RU</td>
<td>1 RU</td>
<td>1RU</td>
</tr>
<tr>
<td><strong>Max 10/100/1000 ports</strong></td>
<td>0</td>
<td>48</td>
<td>40</td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td><strong>Max 10GE ports</strong></td>
<td>40</td>
<td>4</td>
<td>24</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td><strong>Max GE SFP ports</strong></td>
<td>40</td>
<td>4</td>
<td>32 with TwinGig</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td><strong>Shared packet memory</strong></td>
<td>32MB</td>
<td>17.5MB</td>
<td>16MB</td>
<td>16MB</td>
<td>16MB</td>
</tr>
<tr>
<td><strong>VLANs</strong></td>
<td>4096</td>
<td>4096</td>
<td>4096</td>
<td>2048</td>
<td>2048</td>
</tr>
<tr>
<td><strong>Multicast entries</strong></td>
<td>32,000 (IPv4) and 16,000 (IPv6)</td>
<td>32,000 (IPv4) and 16,000 (IPv6)</td>
<td>56,000 (IPv4) and 28,000 (IPv6)</td>
<td>28,000 (L3) and 16,000 (L2)</td>
<td>28,000 (L3) and 16,000 (L2)</td>
</tr>
<tr>
<td><strong>Security &amp; QoS entries</strong></td>
<td>128,000</td>
<td>32,000 (input) + 32,000 (output)</td>
<td>128,000</td>
<td>32,000</td>
<td>32,000</td>
</tr>
<tr>
<td><strong>MAC addresses</strong></td>
<td>55,000</td>
<td>55,000</td>
<td>55,000</td>
<td>55,000</td>
<td>32,000</td>
</tr>
</tbody>
</table>

1. Bi-directional.
## Link Error Counters

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrcAlign-Err</td>
<td>Counts frames that do not end in an even number of octets and have a bad CRC. Indicates a physical layer issue.</td>
<td>Swap out cable with “known good” cable. Test with “known good” switch port. Test with “known good” NIC card or other peer port. Check for duplex mismatch.</td>
</tr>
<tr>
<td>Symbol-Err</td>
<td>Counts how many times the port receives an invalid symbol.</td>
<td>Swap out cable with “known good” cable. Test with “known good” switch port. Test with “known good” NIC card or other peer port.</td>
</tr>
<tr>
<td>Undersize</td>
<td>Counts frames that are less than 64 bytes.</td>
<td>Sniff peer device to determine if it is sending undersize frames.</td>
</tr>
<tr>
<td>Oversize</td>
<td>Counts frames that are greater than the port’s configured or default MTU.</td>
<td>Verify configured MTU on switch port and its peer.</td>
</tr>
<tr>
<td>Fragments</td>
<td>Counts frames that are less than 64 bytes with a bad CRC.</td>
<td>Swap out cable with “known good” cable. Test with “known good” switch port. Test with “known good” NIC card or other peer port.</td>
</tr>
<tr>
<td>Single-Col</td>
<td>Counts how many times a collision occurs before the port transmitted a frame successfully.</td>
<td>Normal for half-duplex ports. Abnormal for full-duplex ports. Check for duplex mismatch. Check if link is over-utilized.</td>
</tr>
<tr>
<td>Multi-Col</td>
<td>Counts how many times multiple collisions occur before the port transmits a frame successfully.</td>
<td>Normal for half-duplex ports. Abnormal for full-duplex ports. Check for duplex mismatch. Check if link is over-utilized.</td>
</tr>
<tr>
<td>Late-Col</td>
<td>Counts how many times the port detects the collision after the time it takes to send the frame (i.e., 5.12 microseconds for a 64-byte frame on a 100 Mbps link).</td>
<td>Check for duplex mismatch.</td>
</tr>
</tbody>
</table>
## Decoding Module Status

**“Show Module”**

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faulty</td>
<td>Line card failed online diagnostics or line card bring-up sequence</td>
<td>May be a hardware issue. Call TAC.</td>
</tr>
<tr>
<td>Authfail</td>
<td>Line card authentication failed</td>
<td>Report issue to TAC.</td>
</tr>
<tr>
<td>Offline</td>
<td>Line card is not fully booted</td>
<td>Occurs when switch brings the line card online. This should be a transient state.</td>
</tr>
<tr>
<td>In Reset</td>
<td>Line card is powered down</td>
<td>Due to no hw-module module &lt;module&gt; power configuration.</td>
</tr>
<tr>
<td>PwrOver</td>
<td>Module is consuming more than 50 W above administratively allocated inline power</td>
<td>Determine if connected devices are receiving the right amount of inline power according to show power inline. If correct, disconnect phones one at a time, noting the inline power utilization change. If one or more devices trigger a change greater than what is listed in show power inline, those devices may be faulty.</td>
</tr>
<tr>
<td>PwrMax or PwrFault</td>
<td>Module is consuming more than 50 W above the module’s limit</td>
<td>Determine if connected devices are receiving the right amount of inline power according to show power inline. If correct, disconnect phones one at a time, noting the inline power utilization change. If one or more devices trigger a change greater than what is listed in show power inline, those devices may be faulty.</td>
</tr>
<tr>
<td>PwrDeny</td>
<td>Insufficient power to bring module online</td>
<td>Configure dual power supplies in combined mode (power redundancy combined), or install power supplies with higher capacity.</td>
</tr>
</tbody>
</table>
Troubleshooting Link Flapping

Link Flaps

1. Monitor syslog for link down events (logging event link-status)
2. Determine link down duration and current status
3. Isolate bad hardware using “known good” hardware

---

%EC-5-UNBUNDLE: Interface Te1/2 left the port-channel Po1
%DTP-5-NONTRUNKPORTON: Port Te1/2 has become non-trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to down

Catalyst-4507# show interface ten1/2 link
Port  Name       Down Time        Down Since
Tel1/2 Uplink   01 sec           09:36:01  Wed Mar 19 2008

Catalyst-4507# show interface ten1/2 link
Port  Name       Down Time        Down Since
Tel1/2 Uplink   00 secs

Link back up!

---
Troubleshooting Auto Negotiation

Auto Negotiation on Legacy Linecards

```
SUP6-E# show int g2/1 status
Port     Name     Status  Vlan  Duplex  Speed  Type
Gi2/1    connected 100 a-full a-1000 10/100/1000-TX

SUP6-E# show platform software interface g2/1 mii
Gmii Registers for interface Gi2/1
Lemans 2-1(Gi2/1-8) Port 1 Non-Zero Phy Registers
Control Reg : 0x1000( AutoNegEnabled )
Status Reg   : 0x796D( LinkStatusUp AutonegComplete MfPreambleSuppression )
Phy Id       : 0x002062D0
AutonegAdv. Reg : 0x0DE1( 10Half 10Full 100Half 100Full SymmPause AsymmPause )
LinkPartnerAdv. Reg : 0xC001( Ack NextPageEnabled )
AutonegExpansion Reg : 0x0000D
AutonegNextPageTx Reg : 0x2001
1000BaseTControl Reg : 0x0600( 1000Full MasterSlaveClockModeAuto PortModeRepeater )
1000BaseTStatus Reg : 0x3800( LinkPartnerAdv:1000Full RecvStatus LocalOk RemoteOk )
```
Troubleshooting Auto Negotiation

Auto Negotiation on E-series linecards

```
<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Status</th>
<th>Vlan</th>
<th>Duplex</th>
<th>Speed Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi2/1</td>
<td>Phone_Host_Connect</td>
<td>connected</td>
<td>10</td>
<td>a-full</td>
<td>10/100/1000</td>
</tr>
</tbody>
</table>
```

```
Sup6-E# show platform software interface g1/1 mii | begin RegAddress

RegAddress   RegName                           Value
0x04         AutoNegAdvReg                    0x0DE1
0x05         AutoNegLinkPartnerAbilityReg     0xC1E1
0x06         AutoNegExpansionReg              0x0005
0x07         AutoNegNextPageTransmitReg       0x2001
0x08         Undefined/Reserved IEEE Reg      0x0000
0x09         1000BaseTControlReg              0x0200
0x0A         1000BaseTStatusReg               0x7800
```

Refer to “Introduction to the Auto-Negotiation process” by University of New Hampshire Interoperability Laboratory for more information on decoding IEEE 802.3 register values.
Troubleshooting Auto Negotiation

Auto Negotiation on E-series linecards

```
SUP6-E# show interfaces g1/5 status
Port   Name       Status       Vlan       Duplex  Speed   Type
Gi1/5                  connected    1       a-half  a-100  10/100/1000-TX

SUP6-E# Sup6-E# show platform software interface g1/5 mii | begin
RegAddress
RegAddress   RegName                         Value
<snip>
0x04         AutoNegAdvReg                   0x0DE1
0x05         AutoNegLinkPartnerAbilityReg    0x0081
0x06         AutoNegExpansionReg             0x0066
0x07         AutoNegNextPageTransmitReg      0x2001
0x08         Undefined/Reserved IEEE Reg     0x0000
0x09         1000BaseTControlReg             0x0200
0x0A         1000BaseTStatusReg              0x0000
```

NOTE: Want to learn more tips about troubleshooting auto negotiation issues?
# Leveraging Dual Supervisors

<table>
<thead>
<tr>
<th>RPR</th>
<th>SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standby supervisor fully boots after switchover</td>
<td>Standby supervisor boots fully</td>
</tr>
<tr>
<td>L2 and L3 tables rebuilt after switchover</td>
<td>L2 tables, configs synchronized</td>
</tr>
<tr>
<td>Switchover traffic loss: 1-2 min.</td>
<td>Switchover L2 traffic loss: 200 ms</td>
</tr>
<tr>
<td>12.2(12c)EW onward</td>
<td>L3 tables dynamically rebuilt</td>
</tr>
<tr>
<td></td>
<td>12.2(20)EWA onward</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NSF</th>
<th>ISSU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires SSO</td>
<td>Requires SSO</td>
</tr>
<tr>
<td>L3 forwarding continues during switchover</td>
<td>Enables in-service IOS upgrades</td>
</tr>
<tr>
<td>NSF-aware: 12.2(20)EWA onward</td>
<td>Images are NSF-capable</td>
</tr>
<tr>
<td>NSF-capable: 12.2(31)SGA onward</td>
<td>12.2(31)SGA onward</td>
</tr>
</tbody>
</table>
## Troubleshooting Supervisor Redundancy

### Verify Ethernet Out-of-Band Channel (EOBC) Counters

<table>
<thead>
<tr>
<th>Catalyst-4510R# show controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dagobah MAC: <strong>EOBC port</strong></td>
</tr>
<tr>
<td>MAC address: 02:00:00:00:01:00</td>
</tr>
<tr>
<td>Restarted: 1</td>
</tr>
<tr>
<td><strong>Rx packets: 36273</strong></td>
</tr>
<tr>
<td>Rx packets reported by hardware: 36273</td>
</tr>
<tr>
<td>Rx error count: 0</td>
</tr>
<tr>
<td>Rx engine restarted: 0</td>
</tr>
<tr>
<td><strong>Tx packets: 36273</strong></td>
</tr>
<tr>
<td>Tx packets reported by hardware: 36273</td>
</tr>
<tr>
<td>Currently queued Tx packets: 0</td>
</tr>
<tr>
<td>High watermark for Tx queue: 10</td>
</tr>
<tr>
<td>Tx error count: 0</td>
</tr>
<tr>
<td><strong>Dropped Tx packets: 5</strong></td>
</tr>
<tr>
<td>Internal error count: 0</td>
</tr>
<tr>
<td>Interrupt count: 35055</td>
</tr>
<tr>
<td>Link events: 1</td>
</tr>
<tr>
<td>Count of Phy polls: 35327</td>
</tr>
<tr>
<td>Count of postprocessing: 35042</td>
</tr>
<tr>
<td>Phy status: <strong>100Mb Half</strong></td>
</tr>
</tbody>
</table>

- **Continuously incrementing? Initiate a switchover to reset EOBC MAC**
- **EOBC speed and duplex for Classic supervisors**
# Troubleshooting SSO

## Sanity Check

### Must Match
- Supervisor type
- Memory
- IOS version

### Should Match
- Rommon version
- Boot variables

### May Match
- Supervisor Hw revision
- Optical modules
- Configuration register value

---

**Catalyst-4507# show module**

Chassis Type : WS-C4507R

Power consumed by backplane : 40 Watts

<table>
<thead>
<tr>
<th>Mod</th>
<th>Ports</th>
<th>Card Type</th>
<th>Model</th>
<th>Serial No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6</td>
<td>Sup V-10GE 10GE (X2), 1000BaseX (SFP)</td>
<td>WS-X4516-10GE</td>
<td>JAB09160071</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>Sup V-10GE 10GE (X2), 1000BaseX (SFP)</td>
<td>WS-X4516-10GE</td>
<td>JAE1008W6KF</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod</th>
<th>Redundancy role</th>
<th>Operating mode</th>
<th>Redundancy status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Standby Supervisor</td>
<td>SSO</td>
<td>Standby hot</td>
</tr>
<tr>
<td>2</td>
<td>Active Supervisor</td>
<td>SSO</td>
<td>Active</td>
</tr>
</tbody>
</table>

1. Supervisors II-Plus and II-Plus-10GE can be configured with 256 or 512 MB. Use `show version` to verify capacity.

2. Different IOS versions accepted (and expected!) during software upgrade or downgrade using ISSU (12.2(37)SG and beyond).
Troubleshooting SSO, Continued

Standby Offline

Catalyst-4507#show module
Chassis Type : WS-C4507R
Power consumed by backplane : 40 Watts

<table>
<thead>
<tr>
<th>Mod Ports</th>
<th>Card Type</th>
<th>Model</th>
<th>Serial No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6</td>
<td>Sup V-10GE 10GE (X2), 1000BaseX (SFP)</td>
<td>WS-X4516-10GE JAB09160071</td>
</tr>
<tr>
<td>2</td>
<td>Supervisor</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC addresses</th>
<th>HW</th>
<th>FW</th>
<th>SW</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 000c.8523.4940 to 000c.8523.4945</td>
<td>2.0</td>
<td>12.2(25r)EW</td>
<td>12.2(37)SG</td>
<td>Ok</td>
</tr>
<tr>
<td>2 Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod</th>
<th>Redundancy role</th>
<th>Operating mode</th>
<th>Redundancy status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Active Supervisor</td>
<td>SSO</td>
<td>Active</td>
</tr>
<tr>
<td>2</td>
<td>Standby Supervisor</td>
<td>SSO</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Catalyst-4507#
Troubleshooting SSO, Continued

Digging Deeper

If Simplex, check if standby supervisor is present and in ROMMON

If mismatched, supervisor type, IOS version, or memory do not match

If Down, check if standby supervisor is present and in ROMMON

Increments due to:
1. Manual reload via CLI
2. Supervisor removal
3. Hardware or software crash
4. Sup-to-sup keepalive timeout

Output continued on next slide…

<table>
<thead>
<tr>
<th>Catalyst-4507# show redundancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant System Information:</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>Available system uptime = 1 day, 23 hours, 2 minutes</td>
</tr>
<tr>
<td>Switchovers system experienced = 0</td>
</tr>
<tr>
<td>Standby failures = 1</td>
</tr>
<tr>
<td>Last switchover reason = none</td>
</tr>
<tr>
<td>Hardware Mode = Duplex</td>
</tr>
<tr>
<td>Configured Redundancy Mode = Stateful Switchover</td>
</tr>
<tr>
<td>Operating Redundancy Mode = Stateful Switchover</td>
</tr>
<tr>
<td>Maintenance Mode = Disabled</td>
</tr>
<tr>
<td>Communications = Up</td>
</tr>
</tbody>
</table>

1. Issue show redundancy switchover history for more information.
Troubleshooting SSO, Continued

Digging Deeper

Current Processor Information:
-----------------------------------
Active Location = slot 2
Current Software state = **ACTIVE**
Uptime in current state = 1 day, 23 hours, 2 minutes
Image Version = Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500-ENTSERVICES-M), Version 12.2(40)SG, RELEASE SOFTWARE (fc2)

Peer Processor Information:
-----------------------------
Standby Location = slot 1
Current Software state = **STANDBY HOT**
Uptime in current state = 1 hour, 9 minutes
Image Version = Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500-ENTSERVICES-M), Version 12.2(40)SG, RELEASE SOFTWARE (fc2)

DISABLED: check if standby supervisor is present, in ROMMON
STANDBY COLD: check for supervisor type, IOS version, and memory mismatch
Match!
Troubleshooting SSO, Continued

Logging into Standby

- Verify running-config is synchronized to standby supervisor
- Verify hardware tables are synchronized
- Verify software tables are synchronized
- Check standby supervisor’s local log

```
Catalyst-4507# show redundancy | include Standby Location
                        Standby Location = slot 1
Catalyst-4507# session module 1
Connecting to standby virtual console
Type "exit" or "quit" to end this session

Catalyst-4507-standby-console# ^e
Standby console enabled.
```
SSO System Messages

- Over 30 system messages to track redundancy states, behavior, and alerts
- Example: losing standby connectivity and IOS version mismatch

1. %C4K_REDUNDANCY-3-COMMUNICATION: Communication with the peer Supervisor has been lost
2. %C4K_REDUNDANCY-3-SIMPLEX_MODE: The peer Supervisor has been lost
3. %C4K_REDUNDANCY-6-DUPLEX_MODE: The peer Supervisor has been detected
4. %C4K_IOSMPORTMAN-6-MODULEONLINE: Module 2 (WS-X4516-10GE S/N: JAE1008W6KF Hw: 3.0) is online
5. %C4K_REDUNDANCY-2-IOS_VERSION_CHECK_FAIL: IOS version mismatch. Active supervisor version is 12.2(37)SG. Standby supervisor version is 12.2(31)SG. Redundancy feature may not work as expected.
6. %C4K_REDUNDANCY-6-MODE: ACTIVE supervisor initializing for rpr mode
7. %C4K_REDUNDANCY-3-COMMUNICATION: Communication with the peer Supervisor has been established

1. Standby supervisor was removed, reloaded, or crashed
2. One operational supervisor in the switch
3. Standby supervisor detected, online
4. Active and standby supervisor IOS version do not match. NOTE: version check will pass for IOS images that support ISSU.
5. Fall back to RPR mode even though SSO is configured
6. Ready to automatically synchronize VLAN database, calendar, configuration register, and boot variables.
Non-Stop Forwarding Overview
Continuous L3 Forwarding During Switchovers

NSF-capable router
Route processor (RP) switchover!
Route Update!
Catalyst 4510R
NSF-aware switch

- L3 traffic flowing
- Route processor (RP) switchover
- Switch retains adjacency table
- Switch forwards routing updates
- No route flaps! L3 traffic flowing!

NSF-awareness introduced in 12.2(20)EWA

Supervisor Switchover!
Route Update!
Catalyst 4510R
NSF-aware switch

- L3 traffic flowing
- Supervisor switchover
- Router clears adjacency table
- Switch waits for routing updates
- Route flap! L3 traffic stops flowing!

NSF-capability introduced in 12.2(31)SG for classic supervisors and 12.2(44)SG for Supervisor 6-E.

NSF-capable router
Supervisor Switchover!
Route Update!
Catalyst 4510R
NSF-capable switch

- L3 traffic flowing
- Supervisor switchover
- Router retains adjacency table
- Router forwards routing updates
- No route flaps! L3 traffic flowing!
Troubleshooting NSF

Sanity Check

- **Is SSO configured and operational?**
  - `show redundancy states`

- **Is NSF configured?**
  - `show running-config | begin router`

- **Using NSF-aware software and hardware?**
  - 12.2(20)EWA through 12.2(25)SG (always on by default)
  - IP base or enterprise services image
  - Supervisor Engines II-Plus, II-Plus+TS, II-Plus+10GE, IV, V, V-10GE
  - Catalyst 4948 and Catalyst 4948-10GE

- **Using NSF-capable software and hardware?**
  - 12.2(31)SG and beyond
  - Enterprise services IOS image
  - Supervisor Engines V, V-10GE, Catalyst 4948-10GE
Troubleshooting NSF
Digging Deeper: OSPF

Switch-1# show running-config | begin router
router ospf 1
  log-adjacency-changes
  nsf
  network 10.0.0.0 0.255.255.255 area 0
  network 20.0.0.0 0.255.255.255 area 0

Switch-1# show ip ospf 1 | begin Non-Stop
Non-Stop Forwarding enabled, last NSF restart 00:01:24 ago (took 35 secs)
  IETF NSF helper support enabled
  Cisco NSF helper support enabled

Switch-1# show cef state capabilities | include NSF
  CEF NSF capable: yes

Switch-1# show cef state | include NSF
  CEF NSF sync: enabled/running
ISSU Overview
Performing In-Service Software Upgrades

- Enables software upgrades without down-time
- Built on top of SSO and NSF
- Requires images to be compatible
  - `show issu comp-matrix stored`

Troubleshooting ISSU

Sanity Check

- Is SSO configured and operational?
  - `show redundancy states`
- Both images support ISSU?
  - 12.2(31)SGA onward
- Does the hardware match?
  - `show module`
- Is autoboot configured?
  - `show bootvar`
  - Configuration register ends in 2
- Are both images saved on the supervisors?
  - `dir slot0: and dir slaveslot0:`
  - `dir bootflash: and dir slavebootflash:`
Troubleshooting ISSU
Interpreting Error Messages

issu loadversion
%% Loadversion CLI can be run only from Init State
%% Active config-register doesn't have 0x2 as the low order nibble
%% Active and Standby image names should be same
%% User is specifying the old image for Active
%% Active\(^1\) unit ID [ 2 ] is wrong; expected [ 1 ]

issu runversion
%% Runversion CLI can be run only from Loadversion or RunVersion-SwitchOver State
%% Standby unit ID [ 1 ] is wrong; expected [ 2 ]

issu commitversion
%% Acceptversion CLI can be run only from RunVersion or LoadVersion-SwitchOver State
%% Active unit ID [ 1 ] is wrong; expected [ 2 ]

issu acceptversion
%% Acceptversion CLI can be run only from RunVersion or LoadVersion-SwitchOver State
%% Active unit ID [ 1 ] is wrong; expected [ 2 ]

1. Similar messages available for standby supervisor.

show issu state
Detailed ISSU State Transitions

1. loadversion
   - load a new version
2. abortversion
   - recover an active version
3. runversion
   - run new version
4. acceptversion
   - accept new version
5. commitversion
   - commit new version

Transition States:
- ACTIVE OLD
- ACTIVE NEW
- READY OLD
- READY NEW
- STANDBY OLD
- STANDBY NEW
Troubleshooting ISSU
Debugging Supervisor Sync Failures

- Occurs when command is not supported by standby’s IOS version
- Results in RPR mode
- Unconfigure mismatched commands to synchronize supervisors and return to SSO mode

Downgrade from 12.2(37)SG to 12.2(31)SGA3

```
Catalyst-4507# issu loadversion 1 bootflash:cat4500-ipbase-mz.122-31.SGA3 2
slavebootflash:cat4500-ipbase-mz.122-31.SGA3
<<< Wait for standby to fully boot >>>
<<< Wait for startup-config to synchronize to standby >>>
```

```
Please check full list of mismatched commands via:
  show issu config-sync failures mcl
```

```
Mar 5 23:29:33.127: Config Sync: Starting lines from MCL file:
```

```
interface GigabitEthernet7/1
  ! <submode> "interface"
  - dot1x host-mode multi-domain
  ! </submode> "interface"
```

12.2(31)SGA3 does not support 802.1X multi-domain authentication
Quality of Service Overview
Classic Catalyst 4000 Supervisor

Quality of Service Overview
Classic Catalyst 4000 Supervisor

Input
Classify | Police | Mark

Output
Classify | Police | Mark

Catalyst-4948-10GE# show qos maps dscp

CoS-DSCP Mapping Table

<table>
<thead>
<tr>
<th>CoS:</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP:</td>
<td>0</td>
<td>8</td>
<td>16</td>
<td>24</td>
<td>32</td>
<td>40</td>
<td>48</td>
<td>56</td>
</tr>
</tbody>
</table>

Catalyst-4510R# show qos maps cos dscp

CoS-DSCP Mapping Table

<table>
<thead>
<tr>
<th>CoS:</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP:</td>
<td>0</td>
<td>8</td>
<td>16</td>
<td>24</td>
<td>32</td>
<td>40</td>
<td>48</td>
<td>56</td>
</tr>
</tbody>
</table>

Want to learn more? Search for Quality of Service on Cisco Catalyst 4500 Series on http://www.cisco.com
Troubleshooting Quality of Service

Catalyst 4000 QoS – Sanity Check

1. **Global QoS enabled?**
   - Catalyst-4948-10GE# show qos
     - QoS is **enabled globally**
     - IP header DSCP rewrite is enabled
     - QoS is vlan-based on the following interfaces: Gi7/1

2. **Class map correct?**
   - Catalyst-4948-10GE# show class-map userFlows
     - Class Map match-all userFlows (id 2)
       - Match flow ip source-address ip destination-address ip protocol l4 source-port l4 destination-port
     - **User Based Rate Limiting**

3. **Policy map correct?**
   - Catalyst-4948-10GE# show policy-map userFlows
     - Policy Map userFlows
       - Class userFlows
         - police 1 mbps 1 kbyte conform-action transmit exceed-action drop

   - interface GigabitEthernet7/1
     - switchport access vlan 10
     - switchport mode access
     - qos vlan-based

   - interface Vlan10
     - ip address 100.1.1.1 255.255.255.0
     - service-policy input userFlows
## Troubleshooting Classic QoS, Continued

### 4. Ports configured correctly?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-based</td>
<td>Yes</td>
<td>No</td>
<td>Port</td>
</tr>
<tr>
<td>Port-based</td>
<td>No</td>
<td>Yes</td>
<td>VLAN</td>
</tr>
<tr>
<td>Port-based</td>
<td>Yes</td>
<td>Yes</td>
<td>Port</td>
</tr>
<tr>
<td>VLAN-based</td>
<td>Yes</td>
<td>No</td>
<td>Port</td>
</tr>
<tr>
<td>VLAN-based</td>
<td>No</td>
<td>Yes</td>
<td>VLAN</td>
</tr>
<tr>
<td>VLAN-based</td>
<td>Yes</td>
<td>Yes</td>
<td>VLAN</td>
</tr>
</tbody>
</table>

Catalyst-4948-10GE# show qos interface g7/1

<snip>

<table>
<thead>
<tr>
<th>Tx-Queue Bandwidth</th>
<th>ShapeRate</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>QueueSize</td>
<td>(bps)</td>
<td>(bps)</td>
</tr>
<tr>
<td>(packets)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>250000000</td>
<td>disabled</td>
</tr>
<tr>
<td>2</td>
<td>250000000</td>
<td>disabled</td>
</tr>
<tr>
<td>3</td>
<td>250000000</td>
<td>disabled</td>
</tr>
<tr>
<td>4</td>
<td>250000000</td>
<td>disabled</td>
</tr>
</tbody>
</table>

interface g7/2
switchport access vlan 10
switchport mode access
tx-queue 3
priority high

interface g7/1
switchport access vlan 10
switchport mode access qos vlan-based
tx-queue 3
priority high

**NOTE:** Port-based QoS is default. Port configuration determines which policy is applied when policy is configured on the port and its SVI.

Each transmit queue has 25% of the bandwidth, but traffic in queue 3 is sent first.
Troubleshooting Classic QoS, Continued

5. Packets matching class map?

Catalyst-4507# `show policy-map interface vlan 10 input class userFlows`  
Vlan10  
Service-policy input: userFlows  
Class-map: userFlows (match-all)  
776298567 packets  
Match: flow ip source-address ip destination-address ip protocol l4 source-port l4 destination-port  
police: Per-interface  
Conform: 1166067574 bytes Exceed: 5268602114 bytes

6. TCAM resources adequate?

Catalyst-4507# `show platform hardware acl statistics utilization brief`  
<table>
<thead>
<tr>
<th></th>
<th>Entries/Total(%)</th>
<th>Masks/Total(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Acl(PortAndVlan)</td>
<td>0 / 8096 ( 0)</td>
<td>0 / 8096 ( 0)</td>
</tr>
<tr>
<td>Input Acl(PortOrVlan)</td>
<td>0 / 8096 ( 0)</td>
<td>0 / 8096 ( 0)</td>
</tr>
<tr>
<td>Input Qos(PortAndVlan)</td>
<td>0 / 8112 ( 0)</td>
<td>0 / 8112 ( 0)</td>
</tr>
<tr>
<td>Input Qos(PortOrVlan)</td>
<td>2 / 8112 ( 0)</td>
<td>2 / 8112 ( 0)</td>
</tr>
</tbody>
</table>
TCAM Resources
Analyzing Feature and Forwarding TCAMs
Feature TCAM Overview

Storing ACLs and QoS Classification Information

TCAM2

24-bit mask

10.1.1.0
20.1.1.0
Empty
Empty
Empty
Empty
Empty
Empty

16-bit mask

30.1.0.0
40.1.0.0
Empty
Empty
Empty
Empty
Empty
Empty

Sup II-Plus, II-Plus-TS, IV, V
Catalyst 4948

8 entries per mask
Static ACL and QoS regions

TCAM3

24-bit mask

10.1.1.0
20.1.1.0
Empty
Empty
Empty
Empty
Empty

16-bit mask

30.1.0.0
40.1.1.1
Empty
Empty
Empty
Empty
Empty

Sup II-Plus-10GE, V-10GE
Catalyst 4948-10GE

1 entry per mask
Static ACL and QoS regions

TCAM4

IPv4 masks
IPv4 entries

IPv6 masks
IPv6 entries

IPv4 masks
IPv4 entries

IPv4 masks
IPv4 entries

IPv4 masks
IPv4 entries

QoS Region

ACL Region

Sup 6-E, Sup 6L-E
Catalyst 4900M

1 entry per mask
Dynamic blocks replace regions

May exhaust masks before entries
Configuration limited by regions
TCAM utilization flexible

Trick: No 10GE ports → TCAM2 ● E-Series supervisor or 4900M&4948E → TCAM4 ● Everything else → TCAM3
Monitoring Feature TCAM Utilization

TCAM4 on SUP6-E

```
SUP6-E# show platform hardware acl statistics utilization brief
CAM Utilization Statistics
--------------------------
                  Used    Free     Total
Input  Security   (160)  298  (14%)  1750  (86%)  2048
Input  Security   (320)  66   (3%)   1982  (97%)  2048
Input  Qos        (160)   9   (0%)   2039  (100%) 2048
Input  Qos        (320)   2   (0%)   2046  (100%) 2048
Input  Forwarding (160)   4   (0%)   2044  (100%) 2048
Input  Unallocated (160)   0   (0%)  55296 (100%) 55296
Output Security  (160)   8   (0%)   2040  (100%) 2048
Output Security  (320)  12   (0%)   2036  (100%) 2048
Output Unallocated (160)  0   (0%)  61440 (100%) 61440
```

Notes: The number (160) and (320) indicated the size of the TCAM entries.
Verifying Forwarding TCAM Utilization

### Software

**SUP6-E# show ip route summary**

IP routing table name is Default-IP-Routing-Table(0)

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Networks</th>
<th>Subnets</th>
<th>Overhead</th>
<th>Memory (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>3</td>
<td>1</td>
<td>256</td>
<td>608</td>
</tr>
<tr>
<td>static</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>bgp 100</td>
<td>0</td>
<td>10000</td>
<td>640000</td>
<td>1520000</td>
</tr>
</tbody>
</table>

External: 0 Internal: 10000 Local: 0

ospf 100

- Intra-area: 1 Inter-area: 0 External-1: 0 External-2: 0
- NSSA External-1: 0 NSSA External-2: 0

internal 3

Total 6

### Hardware

**SUP6-E# show platform hardware ip route summary | be entity**

<table>
<thead>
<tr>
<th>entity</th>
<th>total</th>
<th>used</th>
<th>free</th>
<th>util%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entries</td>
<td>258048</td>
<td>10035</td>
<td>248013</td>
<td>3</td>
</tr>
<tr>
<td>uRPF Ipv4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>uRPF Ipv6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>UC Ipv4</td>
<td>12288</td>
<td>10028</td>
<td>2260</td>
<td>81</td>
</tr>
<tr>
<td>MC Ipv4</td>
<td>2048</td>
<td>6</td>
<td>2042</td>
<td>0</td>
</tr>
<tr>
<td>UC Ipv6</td>
<td>2048</td>
<td>1</td>
<td>2047</td>
<td>0</td>
</tr>
<tr>
<td>MC Ipv6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SpecDst</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SpecSrc</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>unused</td>
<td>241664</td>
<td>241664</td>
<td>0</td>
<td>100</td>
</tr>
</tbody>
</table>

Of the blocks allocated for IPv4 unicast routes, 81% of the entries are in use

TCAM blocks still available for IPv4/IPv6 unicast/multicast
Troubleshooting Unicast Forwarding

Symptom: Host cannot reach server

Gather Facts
– Verify Layer 1
  – Port/Link status, Counter
– Verify Layer 2
  – STP, MAC learning
– Verify Layer 3
  – Routes, Next-hop, Adjacency
– Verify feature interaction
  – ACL, Port Security…etc.

Consider possibilities
Create and execute action plan
Observe results
Troubleshooting Unicast Forwarding

Verify Layer 1 Information

- Verify Link/Port Status
  - Refer to Previous Section

- Check Counters

```
SUP6L-E# show interfaces gi1/1 counter
Port   InBytes  InUcastPkts  InMcastPkts  InBcastPkts
Gi1/1  46798374   92196         0            0

Port   OutBytes  OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi1/1  52856492   32932        45688         1

SUP6L-E# show interfaces gi1/1 counter
Port   InBytes  InUcastPkts  InMcastPkts  InBcastPkts
Gi1/1  49757874   94170         0            0

Port   OutBytes  OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi1/1  55817778   34905        45692         1
```
Troubleshooting Unicast Forwarding

Verify Layer 2 Information

- Verify MAC learning
  - Verify Software MAC address Table

```
SUP6L-E# show mac address-table vlan 10
Unicast Entries
<table>
<thead>
<tr>
<th>vlan</th>
<th>mac address</th>
<th>type</th>
<th>protocols</th>
<th>port</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0000.643a.8a07</td>
<td>dynamic ip,ipx,assigned,other</td>
<td>GigabitEthernet1/1</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>0007.0e65.6f3f</td>
<td>dynamic ip,ipx,assigned,other</td>
<td>GigabitEthernet1/45</td>
<td></td>
</tr>
</tbody>
</table>
```

- Verify Hardware MAC address Table (Optional)

```
SUP6L-E# show platform hardware mac-address-table vlan 10
Flags are:
----------
D - Drop
ND - Do not drop

<table>
<thead>
<tr>
<th>Index</th>
<th>Mac Address</th>
<th>Vlan</th>
<th>Type</th>
<th>SinglePort/RetIndex/AdjIndex</th>
</tr>
</thead>
<tbody>
<tr>
<td>53296</td>
<td>0007.0e65.6f3f</td>
<td>10</td>
<td>SinglePort</td>
<td>Gi1/45(52) ND SrcOrDst</td>
</tr>
<tr>
<td>53312</td>
<td>0000.643A.8A07</td>
<td>10</td>
<td>SinglePort</td>
<td>Gi1/1(8) ND SrcOrDst</td>
</tr>
</tbody>
</table>
```

192.168.20.100
192.168.10.100
Troubleshooting Unicast Forwarding

Verify Layer 2 Information

- Verify STP Status

**SUP6L-E# show spanning-tree vlan 10**

```
VLAN0010
Spanning tree enabled protocol ieee
Root ID Priority 32778
   Address 0007.0e65.6f00
   Cost 4
   Port 45 (GigabitEthernet1/45)
   Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
   Address 000f.8f03.2341
   Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
   Aging Time 300
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/1</td>
<td>Desg</td>
<td>FWD</td>
<td>19</td>
<td>128.1</td>
<td>P2p Edge</td>
</tr>
<tr>
<td>Gi1/45</td>
<td>Root</td>
<td>FWD</td>
<td>4</td>
<td>128.45</td>
<td>P2p</td>
</tr>
<tr>
<td>Gi1/46</td>
<td>Altn</td>
<td>BLK</td>
<td>4</td>
<td>128.46</td>
<td>P2p</td>
</tr>
</tbody>
</table>

**SUP6L-E# show platform hardware stp vlan 10 | exclude Disabled**

```
Interface (HalVfeAggportId) Spanning Tree State
-------------------------------
Gi1/1 (8)                     Forwarding
Gi1/45 (52)                   Forwarding
Gi1/46 (53)                   Blocked/Listening
```
Troubleshooting Unicast Forwarding
Verify Layer 3 Information

- Verify router/port configuration
- Verify IP Routes
- Verify Adjacencies
Troubleshooting Unicast Forwarding
Verify Layer 3 Information

- `show router ospf/eigrp <>`
- `show ip route`
- `show ip cef`

192.168.20.0 is the subnet for the server.
Verify the outgoing interface is G1/3.

```
SUP6-E-DIST# show ip route 192.168.20.0 255.255.255.0
Routing entry for 192.168.20.0/24
Known via "ospf 100", distance 110, metric 3, type intra area
Last update from 172.16.100.1 on GigabitEthernet1/3, 03:56:43 ago
Routing Descriptor Blocks:
  * 172.16.100.1, from 192.168.200.2, 03:56:43 ago, via GigabitEthernet1/3
  Route metric is 3, traffic share count is 1

SUP6L-E-DIST# show ip cef 192.168.20.0 255.255.255.0
192.168.20.0/24
  nexthop 172.16.100.1 GigabitEthernet1/3
```
Troubleshooting Unicast Forwarding

Verify Layer 3 Information

**SUP6-E-DIST#** show arp

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Address</th>
<th>Age (min)</th>
<th>Hardware Addr</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>192.168.10.100</td>
<td>31</td>
<td>0000.643a.8a07</td>
<td>ARPA</td>
<td>Vlan10</td>
</tr>
<tr>
<td>Internet</td>
<td>192.168.10.1</td>
<td></td>
<td>0007.0e65.6f3f</td>
<td>ARPA</td>
<td>Vlan10</td>
</tr>
<tr>
<td>Internet</td>
<td>172.16.100.1</td>
<td>109</td>
<td>0022.90e0.d6ff</td>
<td>ARPA</td>
<td>GigabitEthernet1/3</td>
</tr>
<tr>
<td>Internet</td>
<td>172.16.100.2</td>
<td></td>
<td>0007.0e65.6f3f</td>
<td>ARPA</td>
<td>GigabitEthernet1/3</td>
</tr>
</tbody>
</table>

**SUP6-E-DIST#** show adjacency 172.16.100.1 detail

```
Protocol Interface                 Address
IP                              GigabitEthernet1/3 172.16.100.1(14)

<snip>
002290e0d6ff0070e656f3f0800     
L2 destination address byte offset 0
L2 destination address byte length 6
Link-type after encap: ip
ARP
```

**SUP6-E-CORE#** show interfaces g6/3

GigabitEthernet6/3 is up, line protocol is up (connected)

Hardware is Gigabit Ethernet Port, address is 0022.90e0.d6ff (bia 0022.90e0.d6ff)
Internet address is 172.16.100.1/24

---

**EIGRP/OSPF**

Unicast Routing

Table

CEF

S/W adjacency

Table

H/W

Tables
Troubleshooting Unicast Forwarding

Verify Layer 3 Information

```
SUP6-E-DIST# show platform hardware ip route ipv4 network 192.168.20.0 255.255.255.0
-----------------------------------------------------------
Block: 0 En: true EntryMap: LSB Width: 80-Bit Type: Dst
-----------------------------------------------------------
000015: v4 192.168.20.0/24 --> vrf: Global Routing Table (0)
adjStats: true fwdSel: 2 mrpf: 0 (None) fwdIdx: 0 <snip>
adjIndex: 9 vlan: 1006 port: Gi1/3 (250)
 fwdCtrl: 5 sifact4: FwdToCpu sifact6: FwdToCpu
 sa: 00:07:0E:65:6F:3F da: 00:22:90:E0:D6:FF
```

```
SUP6-E-DIST# show platform hardware ip route ipv4 host 192.168.10.100
-----------------------------------------------------------
Block: 0 En: true EntryMap: LSB Width: 80-Bit Type: Dst
-----------------------------------------------------------
000014: v4 192.168.10.100/32 --> vrf: Global Routing Table (0)
adjStats: true fwdSel: 2 mrpf: 0 (None) fwdIdx: 0 <snip>
adjIndex: 10 vlan: 10 port: Gi2/1 (8)
 fwdCtrl: 5 sifact4: FwdToCpu sifact6: FwdToCpu
 sa: 00:07:0E:65:6F:3F da: 00:00:64:3A:8A:D7
```

Source MAC is the MAC of the distribution switch

Destination MACs are the MAC of the next hop router and host

```
show platform hardware ip route [ipv4] network/host
```

---

EIGRP/OSPF

Unicast Routing Table

CEF

S/W adjacency Table

H/W Tables
Troubleshooting Unicast Forwarding

Verify Layer 3 Information

<table>
<thead>
<tr>
<th>L2 Commands for Access Layer Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>- show interface &lt;interface&gt; counters</td>
</tr>
<tr>
<td>- show spanning-tree vlan</td>
</tr>
<tr>
<td>- show platform hardware stp vlan</td>
</tr>
<tr>
<td>- show mac address-table interface</td>
</tr>
<tr>
<td>- show platform hardware mac-address-table address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>L2 Commands for Distribution Layer Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>- show spanning-tree vlan &lt;vlan&gt; interface</td>
</tr>
<tr>
<td>- show platform hardware stp vlan &lt;vlan&gt; interface</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>L3 Commands for Distribution and Core Layer Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>- show interface</td>
</tr>
<tr>
<td>- show ip route</td>
</tr>
<tr>
<td>- show arp</td>
</tr>
<tr>
<td>- show ip cef</td>
</tr>
<tr>
<td>- show adjacency</td>
</tr>
<tr>
<td>- show platform hardware ip route [ipv4] network/host</td>
</tr>
</tbody>
</table>

1. Cisco Catalyst 4900M and 4948E also uses TCAM4, so you can use the same troubleshooting commands.
Troubleshooting L2 Multicast

IGMP Snooping

- Symptom: Host not receiving multicast traffic
- Gather Facts
  - Verify multicast routing entries
  - Verify L2 switch mrouter ports
  - Verify IGMP snooping configuration
  - Verify IGMP groups
- Consider possibilities
- Create and execute action plan
- Observe results

Interested in Cat4500 Multicast Architecture, you might consider attending BRKARC-3322 - Catalyst 6500 & 4500/4900 Ip Multicast Architecture
Troubleshooting L2 Multicast

IGMP Snooping – Verify Configuration

- IGMP Snooping is enabled by default

```
SUP6-E# show ip igmp snooping vlan 200
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping              : Enabled
IGMPv3 snooping            : Enabled
Report suppression         : Enabled
TCN solicit query          : Disabled
TCN flood query count      : 2
Last Member Query Interval : 1000

Vlan 200:
--------
IGMP snooping                       : Enabled
IGMPv2 immediate leave              : Disabled
Explicit host tracking              : Enabled
Multicast router learning mode      : pim-dvmrp
Last Member Query Interval          : 1000
CGMP interoperability mode          : IGMP_ONLY
```

- Disable IGMP snooping (if possible) to verify if the problem is related to IGMP snooping.
# Troubleshooting L2 Multicast

## IGMP Snooping – Verify Software Entries

**SUP6L-E# show ip igmp snooping mrouter**

<table>
<thead>
<tr>
<th>Vlan</th>
<th>ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>Te1/1(dynamic)</td>
</tr>
</tbody>
</table>

**SUP6L-E# show ip igmp snooping groups**

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group</th>
<th>Version</th>
<th>Port List</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>239.10.10.10</td>
<td>v2</td>
<td>Gi2/11, Gi2/12</td>
</tr>
<tr>
<td>200</td>
<td>239.10.10.11</td>
<td>v2</td>
<td>Gi2/11</td>
</tr>
</tbody>
</table>

**SUP6L-E# show mac address-table vlan 200**

### Unicast Entries

<table>
<thead>
<tr>
<th>vlan</th>
<th>mac address</th>
<th>type</th>
<th>protocols</th>
<th>port</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>0000.0a57.8912</td>
<td>dynamic ip,ipx,assigned,other</td>
<td>GigabitEthernet2/11</td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>0000.0a57.8913</td>
<td>dynamic ip,ipx,assigned,other</td>
<td>GigabitEthernet2/12</td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>00e.1324.5dff</td>
<td>dynamic ip,ipx,assigned,other</td>
<td>TenGigabitEthernet1/1</td>
<td></td>
</tr>
</tbody>
</table>

### Multicast Entries

<table>
<thead>
<tr>
<th>vlan</th>
<th>mac address</th>
<th>type</th>
<th>ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>0100.5e0a.0a0a</td>
<td>igmp</td>
<td>Gi2/11,Gi2/12,Te1/1</td>
</tr>
<tr>
<td>200</td>
<td>0100.5e0a.0a0b</td>
<td>igmp</td>
<td>Gi2/11,Te1/1</td>
</tr>
</tbody>
</table>

If the groups are not learned, try to SPAN the host port to make sure it is sending join.

The corresponding L2 MAC address for Multicast groups.
## Troubleshooting L2 Multicast
### IGMP Snooping – Verify Hardware Entries

### show platform hardware mac-address-table vlan 200

<table>
<thead>
<tr>
<th>Index</th>
<th>Mac Address</th>
<th>Vlan</th>
<th>Type</th>
<th>SinglePort/RetIndex/AdjIndex</th>
</tr>
</thead>
<tbody>
<tr>
<td>24176</td>
<td>001E.1324.5DFF</td>
<td>200</td>
<td>SinglePort</td>
<td>Tel/1(248) ND SrCOrDst</td>
</tr>
<tr>
<td>60464</td>
<td>0100.5E0A.0A0A</td>
<td>200</td>
<td>Ret</td>
<td>104441</td>
</tr>
<tr>
<td>60480</td>
<td>0100.5E0A.0A0B</td>
<td>200</td>
<td>Ret</td>
<td>104443</td>
</tr>
</tbody>
</table>

### show platform hardware ret chain index 104443

RetIndex 104443
RetWordIndex: 522215 Link: 1048575(0xFFFFF) FieldsCnt: 1
SuppressRxVlanBridging: false
Vlan: 200 BridgeOnly: N Gi2/11(18)
Vlan: 200 BridgeOnly: N Tel/1(248)

### show platform hardware ret chain index 104441

RetIndex 104441
RetWordIndex: 522205 Link: 1048575(0xFFFFF) FieldsCnt: 1
SuppressRxVlanBridging: false
Vlan: 200 BridgeOnly: N Gi2/11(18) Gi2/12(19)
Vlan: 200 BridgeOnly: N Tel/1(248)

**NOTE:** MET (multicast expansion table) is being used in classic catalyst 4000 platform instead of RET
Troubleshooting L2 Multicast

IGMP Snooping TCN flooding

- Symptom: Multicast flooding even with IGMP snooping enabled
- When Topology Change Notification (TCN) is received, the switch floods multicast traffic to all ports in a VLAN
- This was necessary for redundant topology to ensure continuous delivering of multicast traffic
Troubleshooting L2 Multicast
IGMP Snooping TCN flooding

Sending Traffic for 50 Groups at 10 Mbps each

Multicast Server

TCN

L2

Distribution and Core

500 Mbps multicast is being flooded to the host

Subscribed to 2 groups and receiving 20 Mbps

mrouter port
Troubleshooting L2 Multicast
IGMP Snooping TCN flooding

SUP6L-E# show ip igmp snooping vlan 200 detail
Vlan 200:
--------
Topology change : No

TCN flood query count : 2

•The default flooding period is TWO query interval
•Before TCN occurs

SUP6L-E# show spanning-tree vlan 200 detail | in topology
Number of topology changes 11 last change occurred 00:00:10 ago

SUP6L-E# show ip igmp snooping vlan 200 detail
Vlan 200:
--------
Protocol generating TCN : STP
General Queries Processed : 1

•TCN occurred and ONE query is being processed

SUP6L-E# show ip igmp snooping vlan 200 detail
Vlan 200:
--------
Protocol generating TCN : STP
General Queries Processed : 2
Troubleshooting L2 Multicast

How to Prevent the Flooding?

- **“no ip igmp snooping tcn flood”** allows flexibility to disable multicast flooding on a per port basis.
- **“ip igmp snooping tcn flood query count”** – configure query count to dictate how long multicast flooding would last.
- IGMP Snooping TCN Flooding feature, triggers immediate IGMP Query.
- As soon as TCN is received, multicast will be flooded on all ports in a vlan, until 2nd IGMP query is sent.
# Troubleshooting L2 Multicast

## Command Summary

<table>
<thead>
<tr>
<th>Troubleshooting Steps</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check IGMP Snooping status</td>
<td>show ip igmp snooping vlan &lt;&gt; [detail]</td>
</tr>
<tr>
<td>Check L2 multicast mrouter</td>
<td>show ip igmp snooping mrouter</td>
</tr>
<tr>
<td>Check L2 multicast MAC address table</td>
<td>show mac address-table vlan &lt;&gt;</td>
</tr>
<tr>
<td>Check hardware MAC address table</td>
<td>show platform hardware mac-address-table vlan &lt;&gt;</td>
</tr>
<tr>
<td>Check Replication Expansion Table for igmp snooping groups and ports</td>
<td>show platform hardware ret chain index &lt;&gt;</td>
</tr>
<tr>
<td>Check spanning tree for topology changes</td>
<td>show spanning-tree vlan 200 detail</td>
</tr>
<tr>
<td>Check hardware flooding set if multicast traffic is being flooded</td>
<td>show platform hardware ret floodset vlan 200</td>
</tr>
<tr>
<td>Disable IGMP Snooping TCN flooding on an interface</td>
<td>no ip igmp snooping tcn flood</td>
</tr>
<tr>
<td>Change IGMP Snooping TCN flooding interval</td>
<td>ip igmp snooping tcn flood query count</td>
</tr>
</tbody>
</table>
Access Control List Overview

Understanding ACL Types

- **Port ACL**
  - Applied to L2 ports or EtherChannels
  - Input and output directions supported
  - Match IP and non-IP traffic

- **VLAN ACL**
  - Applied to VLAN in both directions
  - Match IP traffic bridged within or routed into or out of VLAN

- **Router ACL**
  - Applied to L3 ports, L3 EtherChannels, or SVIs
  - Input and output directions supported
  - Match IP traffic

- **MAC ACL**
  - Applied to L2 ports, Etherchannels, or VLAN
  - Match non-IP traffic
Troubleshooting Access Control Lists

Sanity Check

1. Verify ACL configuration
2. Verify TCAM utilization

SUP6-E# show platform hardware acl statistics utilization brief
CAM Utilization Statistics

<table>
<thead>
<tr>
<th></th>
<th>Used</th>
<th>Free</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Security</td>
<td>(160)</td>
<td>41 (2 %)</td>
<td>2007 (98 %)</td>
</tr>
<tr>
<td>Input Security</td>
<td>(320)</td>
<td>66 (3 %)</td>
<td>1982 (97 %)</td>
</tr>
<tr>
<td>Input Unallocated</td>
<td>(160)</td>
<td>0 (0 %)</td>
<td>61440 (100 %)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Used</th>
<th>Free</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Security</td>
<td>(160)</td>
<td>8 (0 %)</td>
<td>2040 (100%)</td>
</tr>
<tr>
<td>Output Security</td>
<td>(320)</td>
<td>12 (0 %)</td>
<td>2036 (100%)</td>
</tr>
<tr>
<td>Output Unallocated</td>
<td>(160)</td>
<td>0 (0 %)</td>
<td>61440 (100%)</td>
</tr>
</tbody>
</table>

Input Profiles (logical): used 1 / 32
Input Profiles (physical): used 4 / 32

Output Profiles (logical): used 1 / 32
Output Profiles (physical): used 4 / 32

interface Gi1/1
switchport access vlan 10
switchport mode access
ip access-group 100 in
access-list 100 deny tcp
192.168.100.0 0.0.0.255
192.168.200.0 0.0.0.255 eq telnet
access-list 100 permit ip any any
### 3. Verify ACL is programmed in hardware (Optional)

<table>
<thead>
<tr>
<th>Path</th>
<th>Current Label</th>
<th>Next Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>(in :29, null)</td>
<td>(NQ:3, Q:16382/NoPolicing)</td>
<td>NotPresent</td>
</tr>
</tbody>
</table>

**SUP6-E#**

**show platform software acl input path interface gigabitEthernet 1/30**

**show platform hardware acl input entries interface g1/30 all**

**Notes:** You can check port mapping using the command "show platform mapping port" under PimPhyport

- **CAM Entries for path: (in :29, null)**
  - **Input Acl Cam Table**
    - **Idx: 63529 Hit: false**
      - **<snip>**
      - **IP Src**: 192.168.100.0 / 255.255.255.0
      - **IP Dst**: 192.168.200.0 / 255.255.255.0
      - **IP Protocol**: tcp / IpProtocolMask
      - **TCP Src Port**: 0 / 0
      - **TCP Dst Port**: 23 / 65535
      - **<snip>**
      - **ActIdx: 254 StatsIdx: 0 FwdIdx: (None, rep: 0)**
    - **Idx: 63530 Hit: true**
      - **<snip>**
      - **access-list 100 deny tcp**
      - **192.168.100.0 0.0.0.255**
      - **192.168.200.0 0.0.0.255 eq telnet**
      - **<snip>**
      - **access-list 100 permit ip any any**
      - **ActIdx: 255 StatsIdx: 0 FwdIdx: (None, rep: 0)**

**PACL Port Mapping**

- Not associated with a VLAN

**Non-QoS label**

- Not Present
Security Features Overview
Hardening Your Switch

- **Port Security**
  Limits the number of MAC addresses learned and allowed on a port
  Prevents MAC address flooding attacks

- **DHCP Snooping**
  Intercepts, rate-limits, and selectively forwards DHCP packets from hosts connected to untrusted ports
  Prevents DHCP packet flooding, rogue DHCP servers

- **IP Source Guard**
  Allows untrusted hosts’ traffic as per DHCP snooping or static binding table
  Prevents IP address spoofing

- **Dynamic ARP Inspection**
  Allows untrusted hosts’ ARP traffic as per DHCP snooping or static binding table
  Prevents ARP cache poisoning attacks

- **802.1X**
  User-based authentication
  Prevents unauthorized access to the network

1. 12.2(53)SG latest maintenance (SG4) release recommended for security features.
2. For more information, please attend BRKSEC-2005 Deploying Wired 802.1X.
Troubleshooting Security Features

- **Symptom:** Host cannot access the network

- **Gather Facts**
  - Verify port security configuration and status
  - Verify DHCP snooping configuration and status
  - Verify IP source guard configuration and status
  - Verify DAI configuration and status

- **Consider possibilities**
  - Configuration Issue?
  - Security Violation?

- **Create and execute action plan**

- **Observe results**

1. Dynamic ARP Inspection
Verify Port Security Configuration
Is the Configuration Correct?

NOTE: Default violation mode is to shutdown the port. Violation mode “restrict” drops unsecured MAC addresses in software, which may increase CPU utilization.

interface GigabitEthernet2/1
description Phone_Host_Connection
switchport access vlan 10
switchport mode access
switchport voice vlan 20
switchport port-security maximum 5
switchport port-security
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security limit rate invalid-source-mac 100
ip arp inspection limit rate 50
auto qos voip cisco-phone
qos trust device cisco-phone
spanning-tree portfast
spanning-tree bpduguard enable
service-policy input AutoQos-VoIP-Input-Cos-Policy
service-policy output AutoQos-VoIP-Output-Policy
ip verify source vlan dhcp-snooping port-security
ip dhcp snooping limit rate 50
### Verify Port Security Status

**What is the Port Status?**

#### Sup6E-4503E# `show port-security interface g2/1`

<table>
<thead>
<tr>
<th>Port Security</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Status</td>
<td>Secure-up</td>
</tr>
<tr>
<td>Violation Mode</td>
<td>Shutdown</td>
</tr>
<tr>
<td>Aging Time</td>
<td>2 mins</td>
</tr>
<tr>
<td>Aging Type</td>
<td>Inactivity</td>
</tr>
<tr>
<td>SecureStatic Address Aging</td>
<td>Disabled</td>
</tr>
<tr>
<td>Maximum MAC Addresses</td>
<td>5</td>
</tr>
<tr>
<td>Total MAC Addresses</td>
<td>2</td>
</tr>
<tr>
<td>Configured MAC Addresses</td>
<td>0</td>
</tr>
<tr>
<td>Sticky MAC Addresses</td>
<td>0</td>
</tr>
<tr>
<td>Last Source Address:Vlan</td>
<td>0091.0000.0000:10</td>
</tr>
<tr>
<td>Security Violation Count</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Sup6E-4503E# `show port-security interface g2/1 address`

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
<th>Remaining Age (mins)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0091.0000.0000</td>
<td>SecureDynamic</td>
<td>Gi2/1</td>
<td>2 (I)</td>
</tr>
<tr>
<td>20</td>
<td>000f.2322.ddd0</td>
<td>SecureDynamic</td>
<td>Gi2/1</td>
<td>2 (I)</td>
</tr>
</tbody>
</table>

**If port is Secure-down, port security violation occurred**

**Ensure phone and host MAC address are secured**

---

**Total Addresses: 2**
Verify Port Security Status

Host MAC Address Learned and Programmed?

Sup6E-4503E# show mac address-table static

<table>
<thead>
<tr>
<th>vlan</th>
<th>mac address</th>
<th>type</th>
<th>protocols</th>
<th>port</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0091.0000.0000</td>
<td>static</td>
<td>ip,ipx,assigned,other</td>
<td>GigabitEthernet2/1</td>
</tr>
<tr>
<td>20</td>
<td>000f.2322.ddd0</td>
<td>static</td>
<td>ip,ipx,assigned,other</td>
<td>GigabitEthernet2/1</td>
</tr>
</tbody>
</table>

Sup6E-4503E# show platform software host-access-table interface g2/1

Host Access Table for Gi2/1

Current features: Port Security

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Vlan</th>
<th>Access Mode</th>
<th>Inactive(Sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0F:23:22:DD:D0</td>
<td>20</td>
<td>Permit</td>
<td>17</td>
</tr>
<tr>
<td>00:91:00:00:00:00</td>
<td>10</td>
<td>Permit</td>
<td>6</td>
</tr>
<tr>
<td>Default</td>
<td></td>
<td>Ask</td>
<td></td>
</tr>
</tbody>
</table>

%PM-4-ERR_DISABLE: psecure-violation error detected on Gi2/1, putting Gi2/1 in err-disable state

%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0091.0000.0004 on port GigabitEthernet2/1.

NOTE: Port security “consumes” the first packet sent from the host to program the host access table. Catalyst 4500 review process subsequently programs host access table entries into the MAC address table for hardware switching.
Verify DHCP Snooping Configuration

- Is the configuration correct?

```plaintext
ip dhcp snooping vlan 10
ip dhcp snooping

interface GigabitEthernet2/1
  description Phone_Host_Connection
  switchport access vlan 10

ip dhcp snooping limit rate 50

interface TenGigabitEthernet1/1
  switchport mode dynamic desirable
  ip dhcp snooping trust
```

- Any system messages?

```
%DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE WARNING: DHCP Snooping received 50 DHCP packets on interface Gi2/1

%DHCP_SNOOPING-4-DHCP_SNOOPING_RATE_LIMIT_EXCEEDED: The interface Gi2/1 is receiving more than the threshold set

%PM-4-ERR_DISABLE: dhcp-rate-limit error detected on Gi2/1, putting Gi2/1 in err-disable state
```

1. Redundant uplink has same configuration as TenGigabitEthernet1/1.
Verify DHCP Snooping Status

DHCP Snooping Operational and Binding Present?

Sup6E-4503E# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10

DHCP snooping is operational on following VLANs:
10
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled

DHCP snooping trust/rate is configured on the following Interfaces:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
<th>Allow option</th>
<th>Rate limit (pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGigabitEthernet1/1</td>
<td>yes</td>
<td>yes</td>
<td>unlimited</td>
</tr>
<tr>
<td>Custom circuit-ids:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TenGigabitEthernet1/2</td>
<td>yes</td>
<td>yes</td>
<td>unlimited</td>
</tr>
<tr>
<td>Custom circuit-ids:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GigabitEthernet2/1</td>
<td>no</td>
<td>no</td>
<td>50</td>
</tr>
<tr>
<td>Custom circuit-ids:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sup6E-4503E# show ip dhcp snooping binding interface g2/1
MacAddress      IpAddress  Lease(sec) Type     VLAN  Interface
------------------------------------------------------------
00:91:00:00:00:00 172.16.1.1  3600  dhcp-snooping  10    G12/1

Total number of bindings: 1

Ensure uplink ports are configured as trusted
Verify DHCP Snooping Status

- **DHCP static ACL counters incrementing?**

  ```
  Sup6E-4503E# show platform hardware acl input entries static
  ```

  BlockId: 30, LookupType: Security, BlockWidth: 320Bit

<table>
<thead>
<tr>
<th>CamIndex</th>
<th>Entry Type</th>
<th>Active</th>
<th>Hit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>63518</td>
<td>CaptureDhcpClientToServer</td>
<td>Y</td>
<td>11506</td>
</tr>
<tr>
<td>63519</td>
<td>CaptureDhcpServerToClient</td>
<td>Y</td>
<td>439</td>
</tr>
<tr>
<td>63520</td>
<td>CaptureDhcpServerToServer</td>
<td>Y</td>
<td>0</td>
</tr>
</tbody>
</table>

  Should increment with DHCP handshake

- **Is the CPU dropping DHCP packets?**

  ```
  Sup6E-4503E# show platform cpu packet statistics | begin Dropped
  ```

  Packets Dropped In Processing by CPU event

<table>
<thead>
<tr>
<th>Event</th>
<th>Total</th>
<th>5 sec avg</th>
<th>1 min avg</th>
<th>5 min avg</th>
<th>1 hour avg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sa Miss</td>
<td>6900</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Input Acl Fwd</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

  Incrementing? CPU could be dropping DHCP packets
ip dhcp snooping vlan 10
ip dhcp snooping
!
interface GigabitEthernet2/1
description Phone_Host_Connection
switchport access vlan 10
switchport mode access
switchport voice vlan 20
switchport port-security maximum 2
  switchport port-security
  switchport port-security aging time 2
  switchport port-security aging type inactivity
  switchport port-security limit rate invalid-source-mac 100
  switchport port-security mac-address 000f.2322.ddd0 vlan voice
  ip arp inspection limit rate 50
  <snip>
  ip verify source vlan dhcp-snooping port-security
  ip dhcp snooping limit rate 50
 !
interface TenGigabitEthernet1/1
  switchport mode dynamic desirable
  ip dhcp snooping trust
  !
interface TenGigabitEthernet1/2
  switchport mode dynamic desirable
  ip dhcp snooping trust
Verify IP Source Guard Status

- DHCP snooping binding present?

```
Sup6E-4503E# show ip dhcp snooping binding interface g2/1
MacAddress          IpAddress  Lease(sec)  Type           VLAN  Interface
----------------- -------------------------- --------------- ----------- ----- -------
00:91:00:00:00:00  172.16.1.1  3600        dhcp-snooping  10   Gi2/1
Total number of bindings: 1
```

- Per port per VLAN ACL present?

```
Sup6E-4503E# show ip verify source interface g2/1
Interface  Filter-type  Filter-mode  IP-address  Mac-address  Vlan
--------- --------- ------- ---------- --------- ------
Gi2/1      ip-mac    active    172.16.1.1  00:91:00:00:00:00  10

%PM-4-ERR_DISABLE: psecure-violation error detected on Gi2/1, putting Gi2/1 in err-disable state

%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0091.0000.0001 on port GigabitEthernet2/1.
```

```
Sup6E-4503E# show ip verify source interface g2/1
Interface  Filter-type  Filter-mode  IP-address  Mac-address  Vlan
--------- --------- ------- ---------- --------- ------
Gi2/1      ip-mac    inactive-no-snooping-vlan
```
Verify IP Source Guard Status

- TCAM resources available?

<table>
<thead>
<tr>
<th></th>
<th>Used</th>
<th>Free</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Security</td>
<td>46</td>
<td>1984</td>
<td>2048</td>
</tr>
<tr>
<td>Output Security</td>
<td>8</td>
<td>2040</td>
<td>2048</td>
</tr>
</tbody>
</table>

Only allow packets from 172.16.1.1 to any destination

- Per port per VLAN ACL programmed in hardware?
Verify DAI Configuration

- Is the configuration correct?

```plaintext
ip arp inspection vlan 10
ip arp inspection validate src-mac dst-mac ip
ip arp inspection log-buffer entries 1024
ip arp inspection log-buffer logs 100 interval 10
ip dhcp snooping vlan 10
ip dhcp snooping
!
interface GigabitEthernet2/1
  description Phone_Host_Connection
  switchport access vlan 10
  <snip>
  ip arp inspection limit rate 50
  <snip>
end
```

- Any system message?

```
%SW_DAI-4-PACKET_RATE_EXCEEDED: 339 packets received in 0 milliseconds on Gi2/1.
.May 13 14:35:39.386 DST: %PM-4-ERR_DISABLE: arp-inspection error detected on Gi2/1, putting Gi2/1 in err-disable state
```
Verify DAI Status

- DAI operational?

```plaintext
Sup6E-4503E# show ip arp inspection vlan 10

Source Mac Validation : Enabled
Destination Mac Validation : Enabled
IP Address Validation : Enabled

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Configuration</th>
<th>Operation</th>
<th>ACL Match</th>
<th>Static ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Enabled</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vlan</th>
<th>ACL Logging</th>
<th>DHCP Logging</th>
<th>Probe Logging</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Deny</td>
<td>Deny</td>
<td>Off</td>
</tr>
</tbody>
</table>
```

- DHCP snooping binding present?

```plaintext
Sup6E-4503E# show ip dhcp snooping binding interface g2/1

MacAddress          IpAddress  Lease(sec)  Type           VLAN  Interface
--------------       ---------   -----------  ------------    ----  ---------
00:91:00:00:00:00  172.16.1.1  3600     dhcp-snooping  10   Gi2/1

Total number of bindings: 1
```

1. Verify static binding if DHCP snooping is not used with `show ip source binding`.

1. Verify DAI status

- DAI operational?

- DHCP snooping binding present?
Verify DAI Statistics and Log

- Which DAI statistics are [not] incrementing?

```
Sup6E-4503E# show ip arp inspection statistics

Vlan Forwarded Dropped DHCP Drops ACL Drops
---- --------- -------- ------- ------- -------
 10     80       40       40       0

Vlan DHCP Permits ACL Permits Probe Permits Source MAC Failures
---- ----------- ----------- ----------- -------------------
 10     80       0          0          0

Vlan Dest MAC Failures IP Validation Failures Invalid Protocol Data
---- -------------- -------------- --------------
 10       0           0                0
```

Example: source IP in ARP message does not match DHCP snooping binding

```
Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
---- --------- -------- ------- ------- ------- ------- ------- -------
 10     80       40       40       0
```

- What do the logs indicate?

```
Sup6E-4503E# show logging
*Jun 15 01:44:32.115 DST: %SW_DAI-4-DHCP_SNOOPING_DENY: 40 Invalid ARPs (Req) on Gi2/1, vlan 10.[00b2.0000.0001/172.16.1.10/ffff.ffff.ffff/172.16.1.2/01:44:31 DST Mon Jun 15 2009])
Sup6E-4503E# show ip arp inspection log

Interface   Vlan  Sender MAC  Sender IP  Num Pkts  Reason       Time
----------- ---- -------------- ---------- ---------- --------- -------
Gi2/1       10   00b2.0000.0001 172.16.1.10  40  DHCP Deny <snip>
```

DHCP snooping binding has 0091.0000.0000/172.16.1.1 for Gi2/1!
## Troubleshooting Security Features

### Command Summary

<table>
<thead>
<tr>
<th>Troubleshooting Steps</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global and port configuration</td>
<td>show running-config&lt;br&gt;show running-config interface &lt;interface&gt;</td>
</tr>
<tr>
<td>Verify port security status</td>
<td>show port-security interface&lt;br&gt;show port-security interface address&lt;br&gt;show mac address-table static&lt;br&gt;show platform software host-access-table interface</td>
</tr>
<tr>
<td>Verify DHCP snooping status</td>
<td>show ip dhcp snooping&lt;br&gt;show ip dhcp snooping interface &lt;interface&gt;&lt;br&gt;show platform hardware acl input entries static&lt;br&gt;show platform cpu packet statistics</td>
</tr>
<tr>
<td>Verify IP source guard status</td>
<td>show ip dhcp snooping binding interface &lt;interface&gt;&lt;br&gt;show ip verify source interface &lt;interface&gt;&lt;br&gt;show platform hardware acl input entries interface &lt;interface&gt;&lt;br&gt;all&lt;br&gt;show platform hardware acl statistics utilization brief</td>
</tr>
<tr>
<td>Verify DAI status</td>
<td>show ip arp inspection vlan &lt;vlan&gt;&lt;br&gt;show ip dhcp snooping binding interface &lt;interface&gt;&lt;br&gt;show ip arp inspection [statistics</td>
</tr>
</tbody>
</table>
Sup7-E Licensing Replacing Linecard/Supervisor

Replacing Linecards
- Hot swap (remove the old linecard, and insert the new one)
- No License implications
- Configuration persists if the same type is used

Replacing Supervisor
- Copy the license file from the bootflash of the old supervisor to an external storage device
- Hot swap (remove the old supervisor, and insert the new one)
- Copy the license file to the bootflash of the new supervisor
- Re-install license and reboot
Replacing Chassis

- Customers interact with SWIFT to initiate a license transfer for RMA

1. Customer obtain UDIs of the defective and new devices

2. Enter UDI into the “Register for RMA License Transfer” tool

3. License portal determines licenses associated with defective devices

4. New license sent to customer

5. Customer installs new licenses on the new device
Replacing Chassis Details

License Transfer

Product License Registration

Register for a RMA License
Register here and transfer your license from a faulty source device to a replacement device.
You can also check the status of your submitted RMA license transfer request here
Check Status of Submitted Request
A * denotes a required field
Select an option for finding a product.

Select a product from drop-down box:

Catalyst 4500 Series

Goto RMA Portal
Replacing Chassis

License Transfer

Use this page to transfer a license from a faulty device to a replacement device during the Return Material Authorization (RMA) process.

A * denotes a required field
Product Id : *
Serial Number : *
Return Material Authorization Number:

WS-C4510R-E
SPE122200AE

For security purposes, please enter the word as shown above. If you have trouble viewing the word, click on Refresh to view a new word.

fixlers

Fixlers

Refresh

Back

Continue
# Replacing Chassis

## License Transfer

## Product License Registration

1. **RMA License Transfer**
2. **Validate Features**
3. **Designate Licensee**
4. **Review and Submit**

These are all the licenses associated with this UDI: PID: WS-C4510R-E  
SN: SPE122200AE

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Description</th>
<th>Quantity</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>entservices=</td>
<td>For internal purposes only</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

0.89

All licenses will be transferred to the destination/replacement device.

Confirm that the information above is correct and click on the "Continue" button below.  
If the information is incorrect, please open a Service Request using the TAC Service Request Tool. Please have your valid Cisco.com user ID and password available. As an alternative, you may also call our main Technical Assistance Center at 800-553-2447. If you would like to enter a different UDI, click on the "Back" button below to return to the previous page.

[Go Back]  [Continue]
Replacing Chassis License Transfer

Please complete the registration information below to obtain a RMA License

Product Id: MS-C4510R-E
Serial Number: FOX1245GCEP
Replacing Chassis
License Transfer

Product Information

Source: 
Destination: 
Edit Details

RMA Information:
Product Family: CSL Subgroup for Initial Testing

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Feature</th>
<th>Description</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>For Internal purposes only</td>
<td>1</td>
</tr>
</tbody>
</table>

EntServices=

End User Information:
Edit Details

Name
Munia Rahman

Job Title
ENGINEER SOFTWARE ENGINEERING

Company Name
Cisco Systems, Inc.

Company Address
3600 Cisco Way
0
SAN JOSE, CALIFORNIA 95134
UNITED STATES

Phone
+1 408 525 2603

Fax
0

Email Address
murahman@cisco.com

Go Back  Submit  Cancel

BRKCRS-3142  © 2012 Cisco and/or its affiliates. All rights reserved. Cisco Public
Replacing Chassis
License Transfer

Your registration is complete. Your RMA License Key will be sent via email within 1 hour to murahman@cisco.com.

If you have not received an email within 1 hour, please open a Service Request using the TAC Service Request Tool. Please have your valid Cisco.com user Id and password available. As an alternative, you may also call our main Technical Assistance Center at 800-553-2447. Please be sure to check your Junk/Spam email folders for this email from licensing@cisco.com with your license key attached.

Download Your License:
Download License

Optional Next Steps:
Register for another RMA License

Return to the Product License Registration home page
Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Passport points for each session evaluation you complete.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.

Don’t forget to activate your Cisco Live Virtual account for access to all session material, communities, and on-demand and live activities throughout the year. Activate your account at the Cisco booth in the World of Solutions or visit www.ciscolive.com.
Final Thoughts

- Get hands-on experience with the Walk-in Labs located in World of Solutions, booth 1042
- Come see demos of many key solutions and products in the main Cisco booth 2924
- Visit [www.ciscoLive365.com](http://www.ciscoLive365.com) after the event for updated PDFs, on-demand session videos, networking, and more!
- Follow Cisco Live! using social media:
  - Facebook: [https://www.facebook.com/ciscoliveus](https://www.facebook.com/ciscoliveus)
  - Twitter: [https://twitter.com/#!/CiscoLive](https://twitter.com/#!/CiscoLive)
  - LinkedIn Group: [http://linkd.in/CiscoLI](http://linkd.in/CiscoLI)