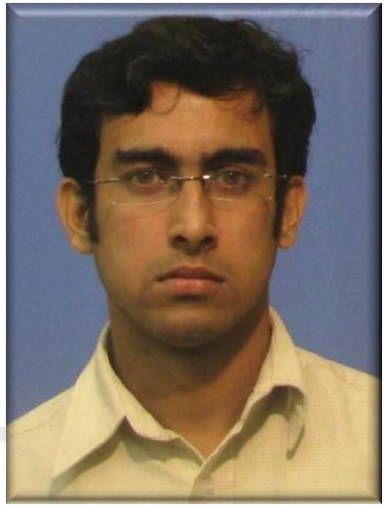
Troubleshooting Tools to Analyze High CPU Utilization Issues on Cisco Catalyst 6500 Series Switches

Souvik Ghosh, Customer Support Engineer

Cisco Support Community – Expert Series Webcast

- Today's featured expert is Cisco Support Engineer **Souvik Ghosh**
- Ask him questions now about **Troubleshooting Tools to Analyze High CPU Utilization Issues on Cisco Catalyst 6500 Series Switches**



Souvik Ghosh

Thank You for Joining Us Today

Today’s presentation will include audience polling questions

We encourage you to participate!

Thank You for Joining Us Today

If you would like a copy of the presentation slides, click the link in the chat box on the right or go to

https://supportforums.cisco.com/docs/DOC-21945

Or,

https://supportforums.cisco.com/community/netpro/network-infrastructure/switching

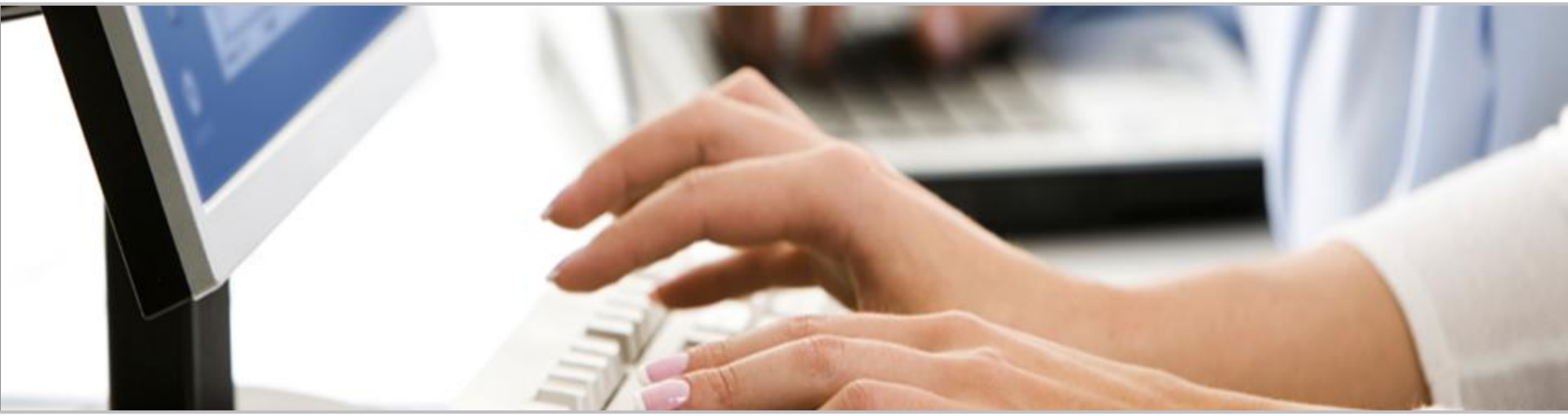
Polling Question 1

What is your level of experience in troubleshooting high CPU utilization on 6500?

a) I have seen the 6500 switch but rarely work with it for troubleshooting purpose.

b) I know basic 6500 troubleshooting, but no idea about high cpu utilization specific troubleshooting.

c) I know most of the 6500 concepts and know what to collect and when.



Submit Your Questions Now

Use the Q&A text box to submit your questions

Troubleshooting Tools to Analyze High CPU Utilization Issues on Cisco Catalyst 6500 Series Switches

Souvik Ghosh, Customer Support Engineer

Agenda

- **How to spot CPU utilization issues**
- **Architecture Introduction**
- **Forwarding Lifecycle**
- **Inspection Tools on:**
  - SUP1/SUP2 running in Hybrid Mode
  - SUP2 running in Native Mode
  - SUP720/SUP32 running in Native Mode
- **Summary**

Spot CPU utilization issues

How to spot the high CPU issue

- Usually this one is noticed by its effects:
  - ✓ Routing Protocol Neighbors Flapping
  - ✓ Sluggish Device Response
  - ✓ Packet Loss etc.

- Sign #1: Sustained high CPU utilization. (Utilization>80%)

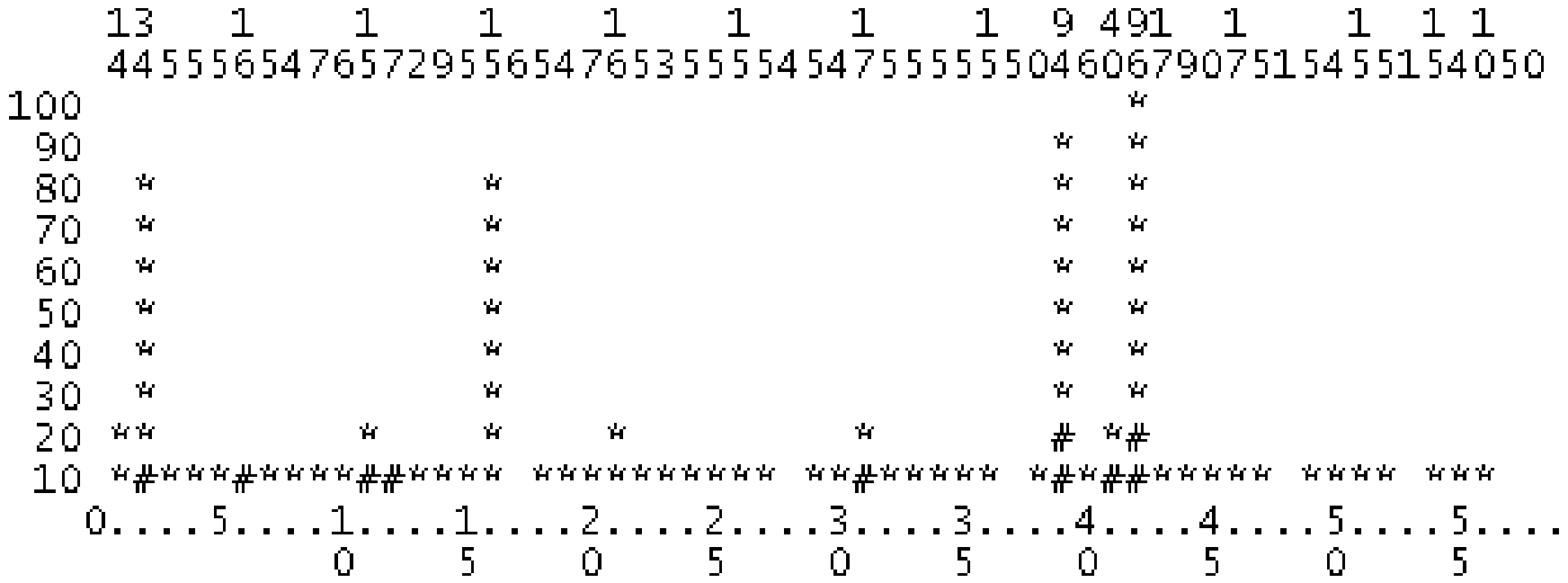
- Sign #2: Sustained high level of CPU-bound traffic.

How to spot the issue: CPU utilization

```
switch#sh process cpu sorted
CPU utilization for five seconds: 100%/82%; one minute: 36%; five minutes: 9%
  PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   12       53228    132347        402 16.62%  5.83%  1.40%   0 ARP Input
   24      146560   1889104         77  0.23%  0.07%  0.07%   0 IPC Seat Manager
  262       98024  12538027          7  0.23%  0.08%  0.02%   0 CDP Protocol
  118        2376      1107       2146  0.15%  0.54%  0.16%   1 Virtual Exec
  480       62520    734741         85  0.15%  0.06%  0.07%   0 Port manager per
...
switch#sh process cpu history
                                1111           11111     11111
    9999999999999999999999990000999999999900000999990000099999
    9999999999999999999999990000999999999900000999990000099999
100 ************************************************************
 80 ************************************************************
 60 ************************************************************
 40 ************************************************************
 20 ************************************************************
 10 ************************************************************
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per second (last 60 seconds)
    1111                                111111
    0000                           1    7000000
    0000655455665555554658958695055555540000006587875477685555
100 ###*                                #####*
 80 ###*                                #####*
 60 ###*                               *#####*
 40 ###*                               *#####*
 20 ####                               *######
 10 ######** ********** ********************#######******** ********
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
CPU% per minute (last 60 minutes) * = maximum CPU%   # = average CPU%
...
```

- Busiest process
- %CPU time spent in interrupt handling
- Total CPU utilization
- How long ago has the issue started

Spikes in CPU utilization



CPU% per second (last 60 seconds)

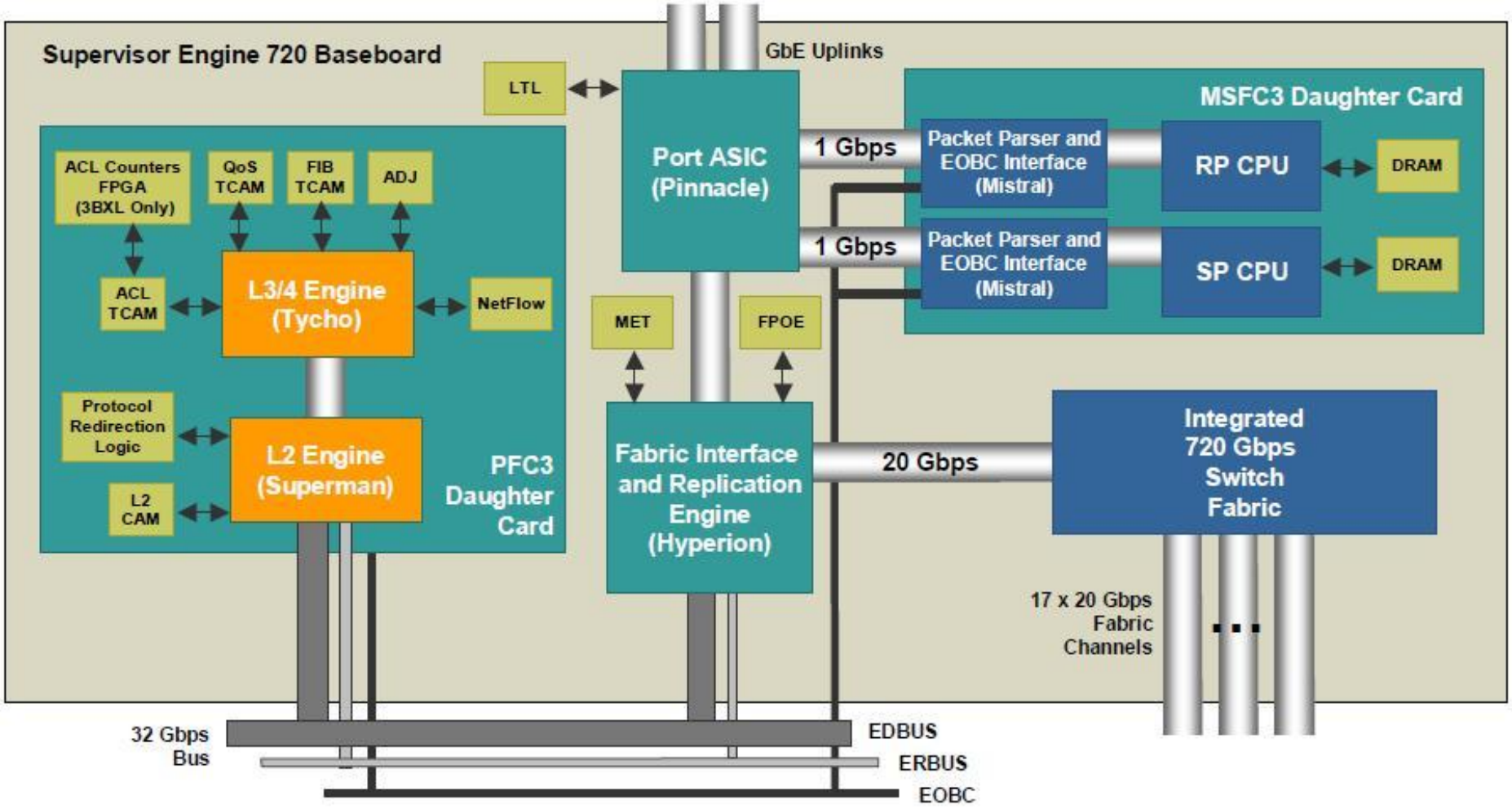
* = maximum CPU% # = average CPU%

Causes for punting traffic to CPU

- Fragmentation
- Same interface forwarding (to generate ICMP redirects)
- ACL log
- ACL deny – no route packet (to generate ICMP unreachable)
- Forwarding exception (out of TCAM/adj space)
- Feature exception (out of TCAM space / conflict)
- SW-supported feature (crypto, nbar, GRE)
- TTL=1
- IP options
- Multicast path setup
- Multicast RPF drops
- Platform-specific traffic handling
- Forwarding path issues – requires troubleshooting
- Glean (Packets requiring ARP resolution) / Receive(Packets falling in the Receive case)

Sup 720 Architecture

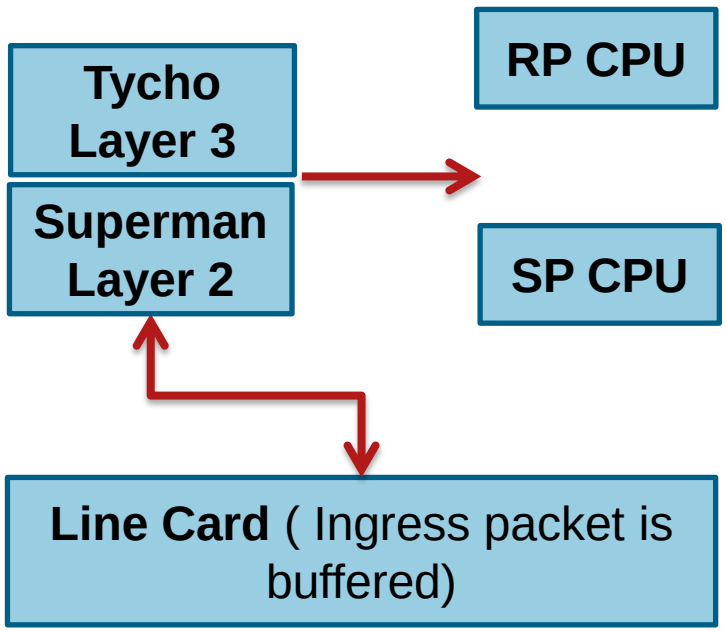
Sup720 Architecture



Sup720 Architecture

- Centralised or Distributed forwarding decisions
- Packet is buffered at ingress linecard
- Lookup decision completed by PFC giving destination port
- Important info in lookup result:
  - ✓ Src/Dest port
  - ✓ VLAN (src/dest vlan)
  - ✓ Rewrite info (any header change to packet)

Simplified diagram



Path of the packet is as follows:

Ingress LC

↓

Bus

↓

PFC (If PFC cannot switch the packet)

↓

Inband Pinnacle

↓

Mistral/Driver—>SW-Queues

↓

CPU

Polling Question 2

What is the first thing you do when you encounter issues with high cpu utilization on 6500?

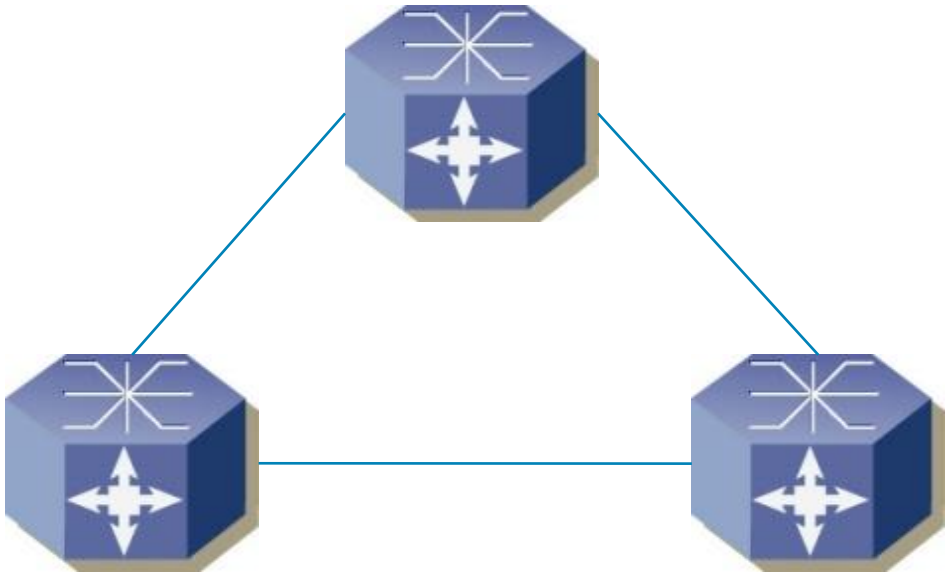
a) **Try to understand the problem yourself or Google around.**

b) **Ask for help from a 6500 expert person in your group.**

c) **Look at 'show tech' output and alarms.**

d) **Open TAC case with Cisco.**

LAB Topology



VLAN10 – 10.10.10.0/24

Tools on Hybrid setup

- ✓ We need to capture the packets which are hitting the CPU.
- ✓ If high cpu utilization is observed in the RP CPU then SPAN capture of port 15/1 is required.
- ✓ If high CPU utilization is observed in the SP CPU then SPAN capture of port SC0 is required.

SPAN on Port 15 and SC0

```
SUP1-HYBRID> (enable) show module

Mod Slot Ports Module-Type                Model                Sub Status
--- ---- ----- ------------------------- -------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE     yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC2         no  ok


SUP1-HYBRID> (enable) set span 15/1 1/1

--------------FOR HIGH CPU on SP CPU---------------------

SUP1-HYBRID> (enable) show interface

sc0: flags=63<UP,BROADCAST,RUNNING>

     vlan 10 inet 10.10.10.4 netmask 255.255.255.0 broadcast 10.10.10.255


SUP1-HYBRID> (enable) set span sc0 1/1
```

Tools on Sup2 running in native mode

- **What it shows:**
  - Packets in input-queue
  - Packet data
  - Src/Dest: MAC, IP, VLAN, TTL, TCP/ UDP, LTL (src)

- **When to use:**
  - High CPU
  - Oversubscribed input queue
  - Find source of punted packets (SVI's usually)

Show Buffer

```
SUP2-NATIVE#show buffer input-interface vl10 header

Buffer information for Medium buffer at 0x425D8648
  data_area 0x6F7A144, refcount 1, next 0x425D88F4, flags 0x280
  linktype 7 (IP), enctype 1 (ARPA), encsize 14, rxtype 1
  if_input 0x436E1A3C (Vlan10), if_output 0x0 (None)
  inputtime 00:00:00.000 (elapsed never)
  outputtime 00:00:00.000 (elapsed never), oqnumber 65535
  datagramstart 0x6F7A1BA, datagramsize 114, maximum size 460
  mac_start 0x6F7A1BA, addr_start 0x6F7A1BA, info_start 0x0
  network_start 0x6F7A1C8, transport_start 0x0, caller_pc 0x4026DE4C

  source: 10.10.10.3, destination: 10.10.10.1, id: 0x00DE, ttl: 255, prot: 1

Buffer information for Medium buffer at 0x425F3C78
  data_area 0x6F8E944, refcount 1, next 0x425F3F24, flags 0x280
  linktype 7 (IP), enctype 1 (ARPA), encsize 14, rxtype 1
  if_input 0x436E1A3C (Vlan10), if_output 0x0 (None)
  inputtime 00:00:00.000 (elapsed never)
  outputtime 00:00:00.000 (elapsed never), oqnumber 65535
  datagramstart 0x6F8E9BA, datagramsize 114, maximum size 460
  mac_start 0x6F8E9BA, addr_start 0x6F8E9BA, info_start 0x0
  network_start 0x6F8E9C8, transport_start 0x0, caller_pc 0x4026DE4C

  source: 10.10.10.3, destination: 10.10.10.1, id: 0x01C7, ttl: 255, prot: 1
```

Tools on Sup720/Sup32 in native mode

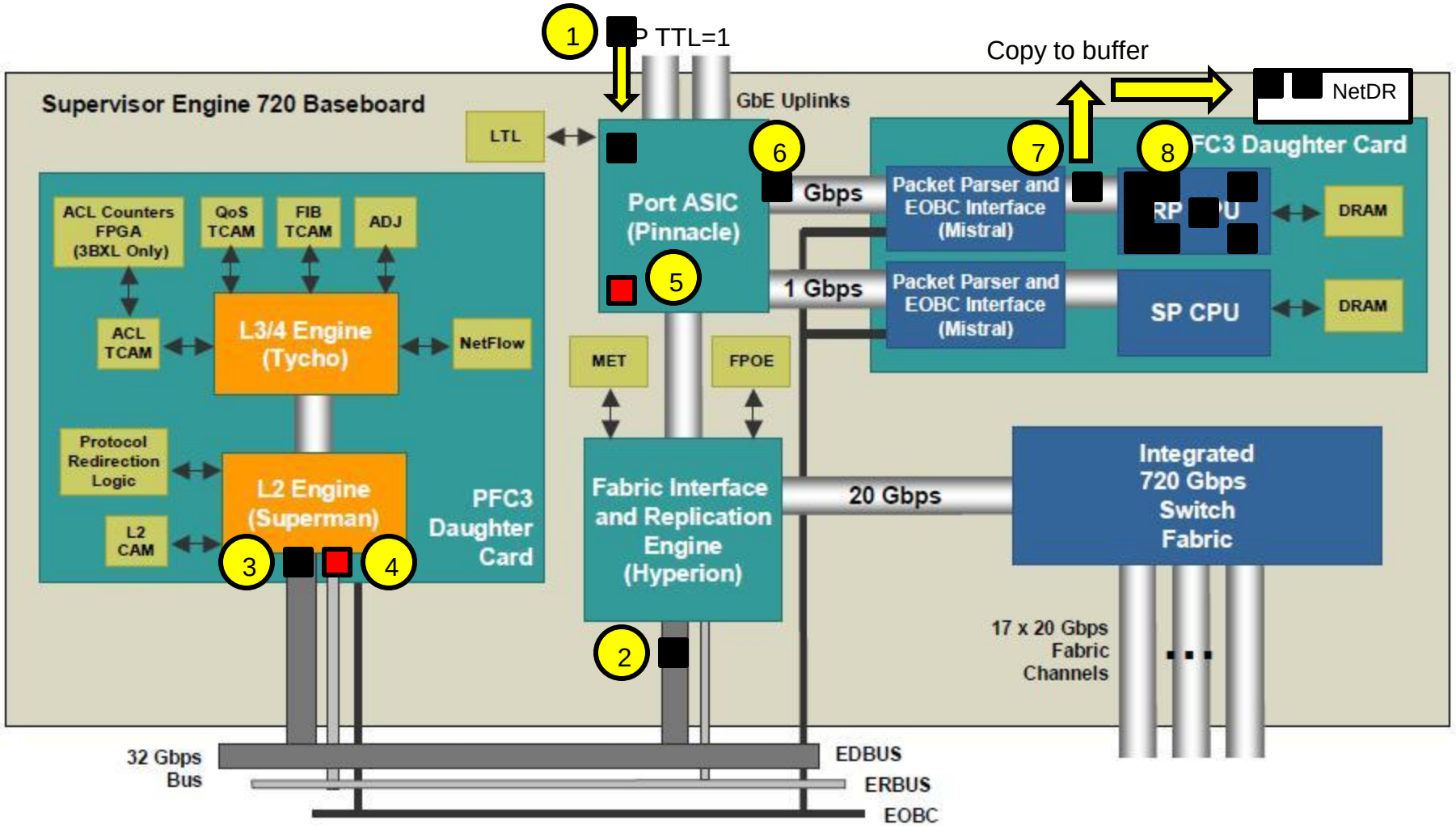
Netdriver

Capture packets being received and sent by RP to buffer space

- **What it shows:**
  - Packets received or sent on RP net interface.
  - SRC/DEST: IP, MAC, VLAN, EtherType etc.

- **When to use:**
  - Confirm particular packets are sent or received.
  - Identify type of packet hitting CPU without introducing extra processing.

NetDr - Capture Punted Packets



Debug Netdr Capture – How To

- **Default 4096 packet buffer space, FIFO drop**

```
SUP720-NATIVE#debug netdr cap ?
  and-filter              (3) Apply filters in an and function: all must match
  continuous              (1) Capture packets continuously: cyclic overwrite
  destination-ip-address  Capture all packets matching ip dst address
  dmac                    Capture packets matching destination mac
  dstindex                (7) Capture all packets matching destination index
  ethertype               (8) Capture all packets matching ethertype
  interface               (4) Capture packets related to this interface
  or-filter               (3) Apply filters in an or function: only one must
                          match
  rx                      (2) Capture incoming packets only
  smac                    Capture packets matching source mac
  source-ip-address       (9) Capture all packets matching ip src address
  srcindex                (6) Capture all packets matching source index
  tx                      (2) Capture outgoing packets only
  vlan                    (5) Capture packets matching this vlan number
  <cr>
```

Debug Netdr Capture – How To

```
SUP720-NATIVE#show netdr capture

------- dump of incoming inband packet -------
interface Vl10, routine mistral_process_rx_packet_inlin, timestamp 18:37:37.019
dbus info: src_vlan 0xA(10), src_indx 0x101(257), len 0x5EE(1518)
  bpdu 0, index_dir 0, flood 0, dont_lrn 0, dest_indx 0x380(896)
  C0000400 000A0000 01010005 EE080000 00010A0A 0A010A0A 0A020000 03800000
mistral hdr: req_token 0x0(0), src_index 0x101(257), rx_offset 0x76(118)
  requeue 0, obl_pkt 0, vlan 0xA(10)
destmac 00.27.0D.EF.40.80, srcmac 00.04.27.9C.3D.42, protocol 0800
protocol ip: version 0x04, hlen 0x05, tos 0x00, totlen 1500, identifier 39151
  df 0, mf 0, fo 0, ttl 255, src 10.10.10.2, dst 10.10.10.1
    icmp type 8, code 0

------- dump of incoming inband packet -------
interface Vl10, routine mistral_process_rx_packet_inlin, timestamp 18:37:37.023
dbus info: src_vlan 0xA(10), src_indx 0x101(257), len 0x5EE(1518)
  bpdu 0, index_dir 0, flood 0, dont_lrn 0, dest_indx 0x380(896)
  C8000400 000A0000 01010005 EE080000 00010A0A 0A010A0A 0A020000 03800000
mistral hdr: req_token 0x0(0), src_index 0x101(257), rx_offset 0x76(118)
  requeue 0, obl_pkt 0, vlan 0xA(10)
destmac 00.27.0D.EF.40.80, srcmac 00.04.27.9C.3D.42, protocol 0800
protocol ip: version 0x04, hlen 0x05, tos 0x00, totlen 1500, identifier 39152
  df 0, mf 0, fo 0, ttl 255, src 10.10.10.2, dst 10.10.10.1
    icmp type 8, code 0
```

RP/SP inband span

- The RP-Inband SPAN spans the Inband pinnacle port from the SP to the RP and vice versa

- On and after **SXH** Image

```
Router(config)# monitor session 1 type local
Router(config-mon-local)# source cpu rp /sp tx/rx/both
Router(config-mon-local)# destination int Gi5/2
Router(config-mon-local)# no shut
```

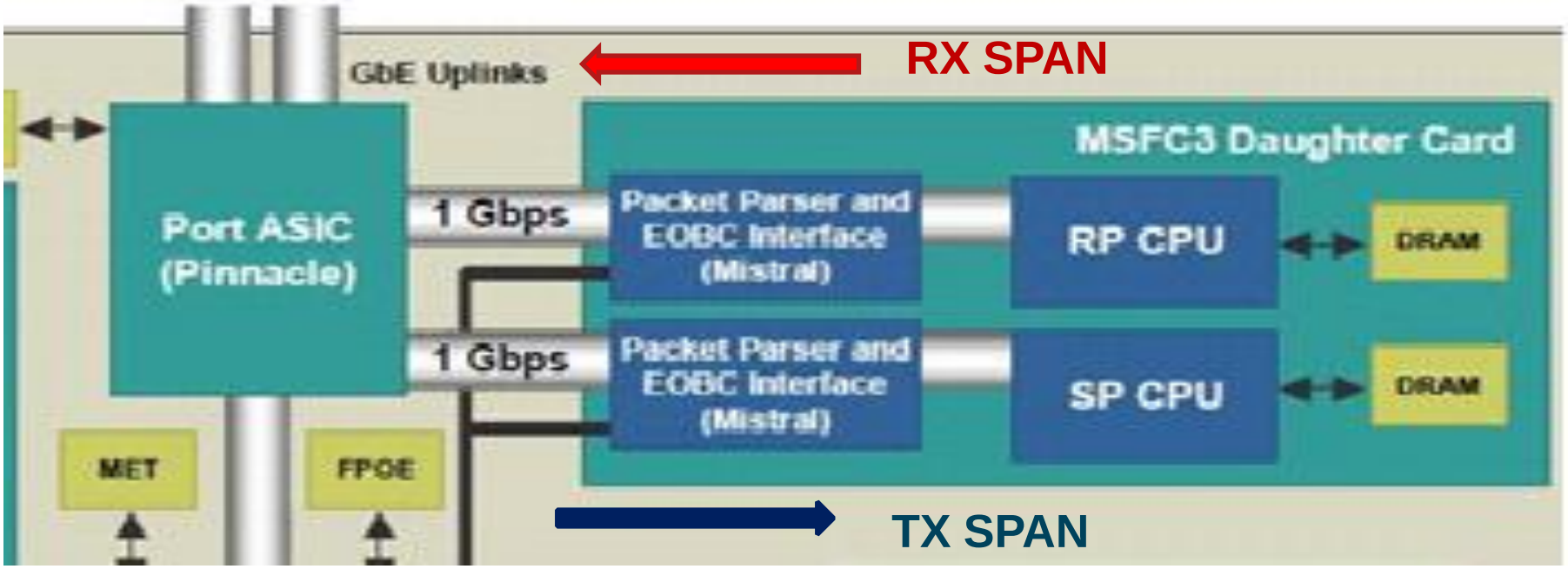
RP/SP inband span

- After 12.1(19)E till SXF

```
Router(config# monitor session 1 source interface <mod/port>
 !--- Use any interface that is administratively shut down.

Router# monitor session 1 destination interface <mod/port>
 !--- Interface with sniffer attached

 Go to the SP console and enter below command:
Router-sp#test monitor session 1 add rp-inband/sp-inband tx
```



TX SPAN

→ For packet from Pinnacle to RP/SP CPU

RX SPAN

← For packet from RP/SP CPU to Pinnacle

Summary

Summary

- Intermittent CPU utilization is not a matter of concern, in networks running SNMP, routing protocols it is expected to see intermittent spike in CPU utilization.
- A constant CPU utilization of more than 70-80% needs troubleshooting.
- The first step of troubleshooting the CPU utilization issue is to identify whether the issue is caused by interrupt or by IOS processes.
- If the CPU utilization is due to an IOS process then further troubleshooting will depend on the process which is pegging the CPU. A detail description is beyond the scope of this presentation.
- If the CPU utilization is majorly contributed by interrupt then it is related network traffic. It is important to find out the traffic which are hitting the CPU, please use the tools described in this presentation to capture the traffic.

Contd…

Summary

- Once we have an understanding of the traffic which are hitting the CPU then next step is to find out the reason behind the punt. The list mentioned in slide 13 are most frequent causes of the punt however the list is not exhaustive.
- If you need to troubleshoot the cause of intermittent high CPU utilization then following script can be configured to capture CPU information:

```
event manager applet highcpu event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.7  get-type exact entry-op gt entry-val "70" exit-op lt exit-val "20" poll-interval 2 maxrun 10

action 0.0 syslog msg "High CPU DETECTED“

action 0.1 cli command "enable"

action 1.1 cli command "show clock | append flash:high_cpu.txt"

action 1.2 cli command "show process cpu sorted | append flash:high_cpu.txt"
```

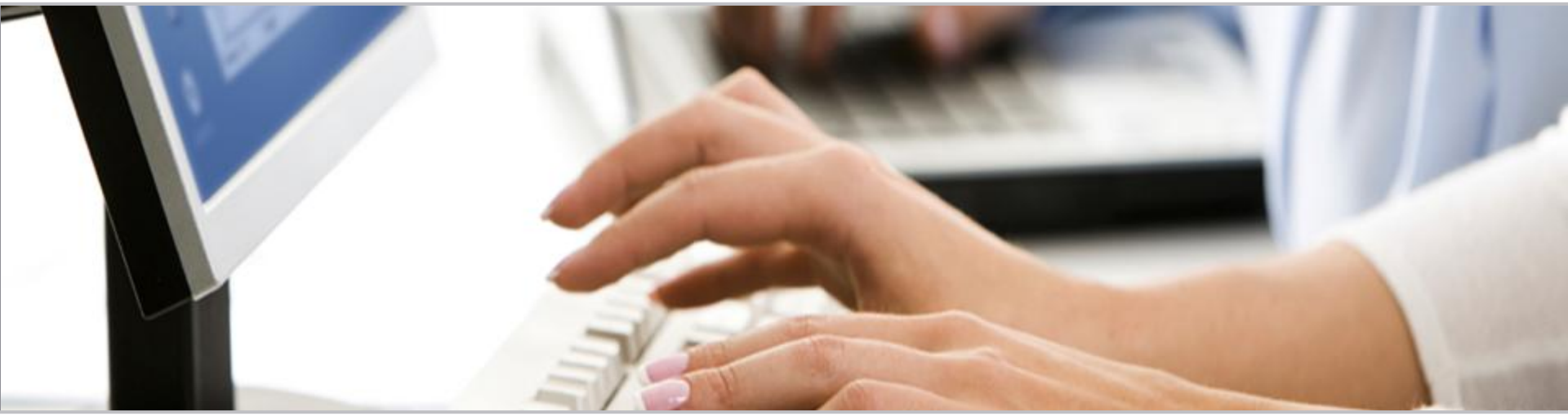
References

❑ Cisco Support Community Documents

- https://supportforums.cisco.com/docs/DOC-12619
- https://supportforums.cisco.com/docs/DOC-15608
- https://supportforums.cisco.com/docs/DOC-14086

❑ Cisco.com or CCO document

- http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a00804916e0.shtml



Submit Your Questions Now

Use the Q&A panel to submit your questions. Experts will start responding those

Polling Question 3

How useful was this presentation?

a) **This was very informative presentation and will help me during my day to day 6500 high cpu utilization issues.**

b) **This presentation needed more in depth details.**

c) **I wanted to see some information on configuration**

d) **This presentation was somewhat useful**

e) **This presentation was not useful to me.**

Q&A

We Appreciate Your Feedback!

The first 5 listeners
who fill out the Evaluation Survey
will receive a free:

$20 USD Gift Certificate

To complete the evaluation, please click on link provided in the chat.

Ask The Experts Event (with Souvik Ghosh)

If you have additional questions, you can ask them to Souvik here:

https://supportforums.cisco.com/community/netpro/ask-the-expert

He will be answering from January 17th to January 27th.

Next CSC Expert Series Webcast in English

Topic: Unified Computing System (UCS) 2.0 – New Hardware & Software Features

Tuesday February 7 at

8:00 a.m. PST San Francisco (UTC -8 hours)
11:00 a.m. EST New York (UTC -5 hours)
4:00 p.m CEST Paris (UTC +1 hours)

Join Cisco Experts and CCIEs

Jose Martinez & Matthew Wronkowski.

They will focus on new features supported on Unified Computing System (UCS) Generation 2 hardware.

During this interactive session you will be able ask all your questions related to this topic.

Register for this live Webcast at

www.CiscoLive.com/ATE

Next CSC Expert Series Webcast in Spanish

Topic: BGP Path Control

Tuesday January 31, at

9:00 a.m. Mexico City time (UTC -6 hours),

7:00 a.m. PST San Francisco (UTC -8 hours),

and 4:00 p.m CEST Madrid (UTC +1 hours).

Join Cisco Support Engineer and CCIE

Ricardo Prado

He will discuss about the techniques for filtering BGP routes using AS PATH and communities attributes, the conditional propagation method

During this interactive session you will be able ask all your questions related to this topic.

Register for this live Webcast at

http://tools.cisco.com/gems/cust/customerSite.do?METHOD=E&LANGUAGE_ID=S&PRIORITY_CODE=4&SEMINAR_CODE=S15924

Next CSC Expert Series Webcast in Portuguese

Topic: Cisco IronPort Email Security Technology

Tuesday February 14, at

1:30 p.m. Rio de Janeiro time (UTC-2 hours)

3:30 p.m WET Lisbon (UTC),

7:30 a.m PST San Francisco (UTC -8 hours)

Join Cisco Support Engineer

Valter Pereira

During the live event you will learn about the features of Cisco IronPort ESA (Cisco IronPort Email Security Appliance), how to manage it and how to troubleshoot most common issues.

During this interactive session you will be able ask all your questions related to this topic.

You'll be able to register at this webcast next week at

https://supportforums.cisco.com/community/portuguese

We have communities in other languages

If you speak Spanish, Portuguese, Japanese, or Polish, we invite you to ask your questions and collaborate in your language.

- Spanish → https://supportforums.cisco.com/community/spanish
- Portuguese: → https://supportforums.cisco.com/community/portuguese
- Japanese → https://supportforums.cisco.com/community/csc-japan
- Polish → https://supportforums.cisco.com/community/etc/netpro-polska

We're also running a pilot for Russian You can register at the following link:

- Russian: (Launching in March, 2012) https://www.ciscofeedback.vovici.com/se.ashx?s=6A5348A712220E19

We invite you to actively collaborate in the Cisco Support Community and social media

https://supportforms.cisco.com

http://www.facebook.com/CiscoSupportCommunity

http://twitter.com/#!/cisco_support

http://www.youtube.com/user/ciscosupportchannel

http://itunes.apple.com/us/app/cisco-technical-support/id398104252?mt=8

http://www.linkedin.com/groups/CSC-Cisco-Support-Community-3210019

Thank You for Your Time

Please Take a Moment to Complete the Evaluation


CISCO