



Troubleshooting Commands on Cisco ASR 9000 Series Router

This module describes commands used for troubleshooting routers running Cisco IOS XR software.

The commands in this chapter with the cisco-support task ID are used in the *Cisco IOS XR Troubleshooting Guide* as part of the troubleshooting process. For information about commands with the cisco-support task ID that are not documented in this chapter, please contact Cisco Technical Support. See “[Obtaining Documentation and Submitting a Service Request](#)” section on page iii in the [Preface](#).



Caution

These Cisco support commands are normally reserved for use by Cisco Technical Support personnel only. There is some risk that they may cause performance or other issues that impact products without proper usage, and we highly recommend that you contact Cisco Technical Support prior to using any of these commands.

R3.9 Technical Checkpoint Review – Cisco Confidential

show sysdb connections

To display the client connection information for the system database (SYSDB), use the **show sysdb connections** command in EXEC mode.

show sysdb connections [detail | job | path | location | shared-plane]

Syntax Description	Parameter	Description
	detail	Displays the detailed client connection information.
	job	Specify a Job ID.
	path	Specify a path filter.
	location	Specify a location.
	shared-plane	Displays the shared-plane data

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.7.2	This command was introduced on the Cisco ASR 9000 Series Router.
	Release 3.9.0	No modification.

Usage Guidelines To use this command, your Cisco IOS XR software system administrator must assign you to a user group associated with a task group that includes the corresponding command task IDs. If you need assistance with your task group assignment, contact your system administrator. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	sysmgr	read
	cisco-support	read

Examples The following example shows the output of the **show sysdb connections** command.

```
RP/0/RSP0/CPU0:router# show sysdb connections detail location 0/1/CPU0

SysDB Connections:
  "/debug/node/11/LR/sysdb/client/"
  From:      shmwin_svr (jid 76, nid 0/1/CPU0, tid 1)
  Connid:    00000001 Refcount: 0002 Options: 00000032
  Connected:      Y In trans:  N Verf susp:      N
  Client connid: 00000000
```

R3.9 Technical Checkpoint Review – Cisco Confidential

```
Connected at: Jul 14 19:31:47.304
"/debug/node/11/LR/packet/"
From:      packet (jid 218, nid 0/1/CPU0, tid 1)
Connid:    00000002 Refcount: 0002 Options: 00000032
Connected: Y In trans: N Verf susp: N
Client connid: 00000000
Connected at: Jul 14 19:31:47.305
"/debug/node/11/LR/cdm/qsm/"
From:      qsm (jid 246, nid 0/1/CPU0, tid 4)
Connid:    00000003 Refcount: 0002 Options: 00000032
Connected: Y In trans: N Verf susp: N
Client connid: 00000000
Connected at: Jul 14 19:31:47.305
"/debug/node/11/LR/eem/"
From:      wdsysmon (jid 361, nid 0/1/CPU0, tid 5)
Connid:    00000005 Refcount: 0002 Options: 00000032
Connected: Y In trans: N Verf susp: N
Client connid: 00000000
Connected at: Jul 14 19:31:47.316
"/debug/node/11/LR/sysmgr/"
From:      sysmgr (jid 79, nid 0/1/CPU0, tid 7)
Connid:    00000013 Refcount: 0002 Options: 00000032
...
```

R3.9 Technical Checkpoint Review – Cisco Confidential

show sysdb trace verification location

To display trace verification information for the system database (SYSDB), use the **show sysdb trace verification location** command in EXEC mode.

show sysdb trace verification location *node-id*

Syntax Description	<i>node-id</i>	Specific node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
---------------------------	----------------	--

Defaults	No default behavior or values	
-----------------	-------------------------------	--

Command Modes	EXEC	
----------------------	------	--

Command History	Release	Modification
	Release 3.7.2	This command was introduced on the Cisco ASR 9000 Series Router.
Release 3.9.0	No modification.	

Usage Guidelines

To use this command, your Cisco IOS XR software system administrator must assign you to a user group associated with a task group that includes the corresponding command task IDs. If you need assistance with your task group assignment, contact your system administrator. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of *Cisco IOS XR System Security Configuration Guide*.

Use the **show sysdb trace verification shared-plane location** command to display details of recent verification sysDB transactions and changes on local plane configurations. The command output allows you to confirm that configuration were verified and accepted.

Task ID	Task ID	Operations
	sysmgr	read
	cisco-support	read

Examples

The following example shows the output of the **show sysdb trace verification shared-plane location** command. The output shows that changes to the SysDB local plane were verified and accepted.

```
RP/0/RSP0/CPU0:router# show sysdb trace verification location 0/3/CPU0

Timestamp          path          jid          tid  reg handle  connid  action
-----
323 wrapping entries (4096 possible, 299 filtered, 622 total)
Jul  7 20:10:36.212 260          1    90         8782    apply reply
Jul  7 20:10:35.476 260          1    90         4912    Apply/abort called
```

R3.9 Technical Checkpoint Review – Cisco Confidential

```

'cfg/if/act/GigabitEthernet0_3_4_0.1/a/sub_vlan/0x2/_____/Gigab
itEthernet0_3_4_0/_____'
Jul  7 20:10:35.475      260      1      90      4912      verify reply: accep
t      '---'
Jul  7 20:10:35.471      260      1      90      4912      Verify called
'cfg/if/act/GigabitEthernet0_3_4_0.1/a/sub_vlan/0x2/_____/Gigab
itEthernet0_3_4_0/_____'
Jul  7 20:10:35.471      144      1      4      8782      apply reply
'---'
Jul  7 20:10:35.471      144      1      4      8782      apply reply
'---'
Jul  7 20:10:35.471      144      1      4      8782      apply reply
'---'
Jul  7 20:10:35.471      144      1      4      8782      apply reply
'---'
Jul  7 20:10:35.471      144      1      4      8782      apply reply
'---'
Jul  7 20:10:35.471      144      1      4      8782      apply reply
'---'
Jul  7 20:10:35.471      144      1      4      8782      apply reply
'---'
Jul  7 20:10:35.470      144      1      4      474      Apply/abort batch e
nded
Jul  7 20:10:35.470      144      1      4      474      Apply/abort called
'cfg/if/act/GigabitEthernet0_3_4_0/ord_x/im/shutdown'
Jul  7 20:10:35.470      144      1      4      474      Apply/abort called
'cfg/if/act/GigabitEthernet0_3_4_1/ord_x/im/shutdown'
Jul  7 20:10:35.470      144      1      4      474      Apply/abort called
'cfg/if/act/GigabitEthernet0_3_4_2/ord_x/im/shutdown'
Jul  7 20:10:35.470      144      1      4      474      Apply/abort called
'cfg/if/act/GigabitEthernet0_3_4_3/ord_x/im/shutdown'
Jul  7 20:10:35.470      144      1      4      474      Apply/abort called
'cfg/if/act/GigabitEthernet0_3_4_4/ord_x/im/shutdown'
Jul  7 20:10:35.469      144      1      4      474      Apply/abort called
'cfg/if/act/GigabitEthernet0_3_4_5/ord_x/im/shutdown'
Jul  7 20:10:35.469      144      1      4      474      Apply/abort called
'cfg/if/act/GigabitEthernet0_3_4_6/ord_x/im/shutdown'
Jul  7 20:10:35.469      144      1      4      474      Apply/abort called
'cfg/if/act/GigabitEthernet0_3_4_7/ord_x/im/shutdown'
Jul  7 20:10:35.469      144      1      4      474      Apply/abort batch s
tarted
Jul  7 20:10:35.469      144      1      4      474      verify reply: accep
t      '---'
Jul  7 20:10:35.469      144      1      4      474      verify reply: accep
t      '---'
Jul  7 20:10:35.469      144      1      4      474      verify reply: accep
t      '---'
!
!
!

```

Table 2 describes the significant fields shown in the display.

Table 2 show sysdb trace verification location Field Descriptions

Field	Description
Timestamp	Time of the verification.
jid	Job identifier of the verification.
tid	Thread identifier.

R3.9 Technical Checkpoint Review – Cisco Confidential

Table 2 show sysdb trace verification location Field Descriptions (continued)

Field	Description
reg handle	Registration handle.
connid	Connection identifier.
action	Action occurring between the sysDB server and client.
apply reply	SysDB notification that the client that an apply action has occurred.
Apply/abort called	SysDB notification for the client that an apply or abort has been called.
verify reply: accept	Verifier has accepted the verification request.

Related Commands

Command	Description
show sysdb connection path shared-plane	Displays sysDB client connection shared plane data for a specific path.

R3.9 Technical Checkpoint Review – Cisco Confidential

show sysdb trace verification shared-plane

To display trace verification information for the system database (SYSDB), use the **show sysdb trace verification shared-plane** command in EXEC mode.

```
show sysdb trace verification shared-plane [file | hexdump | last | location | reverse | stats | tailf
| unique | verbose | wrapping]
```

Syntax Description	file	(Optional) Specifies the name of a file.
	hexdump	(Optional) Displays the packet contents in hexadecimal format.
	last	(Optional) Specifies the last number of packets in the queue to display.
	location	(Optional) Displays the card location.
	reverse	(Optional) Specifies the new traces as they are added.
	stats	(Optional) Displays trace statistics information.
	tailf	(Optional) Displays new traces as they are added.
	unique	(Optional) Displays a list of unique entries with counts.
	verbose	(Optional) Displays internal debugging information.
	wrapping	(Optional) Displays wrapping entries of all trace information.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.7.2	This command was introduced on the Cisco ASR 9000 Series Router.s.
	Release 3.9.0	No modification.

Usage Guidelines To use this command, your Cisco IOS XR software system administrator must assign you to a user group associated with a task group that includes the corresponding command task IDs. If you need assistance with your task group assignment, contact your system administrator. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of *Cisco IOS XR System Security Configuration Guide*.

Use the **show sysdb trace verification shared-plane** command to display details of recent verification sysDB transactions and changes on the shared plane. The command output allows you to confirm whether the configuration was verified correctly.

Specifying a path using the | include keyword and *path* argument filters the data to display only the sysDB path for the router. Use the **describe** command to determine the path.

R3.9 Technical Checkpoint Review – Cisco Confidential

Task ID	Task ID	Operations
	sysmgr	read
	cisco-support	read

Examples

The following example shows the output of the **show sysdb trace verification shared-plane** command. The output shows that changes to the SysDB shared plane were verified and accepted.

```
RP/0/RSP0/CPU0:router# show sysdb trace verification shared-plane | include gl/a/hostname
May 18 19:16:17.143      340      3      210      962      Apply/abort called
                    'cfg/gl/a/hostname'
May 18 19:16:17.132      340      3      210      962      Verify called
                    'cfg/gl/a/hostname'
May 18 19:16:17.126      340      3      210      962      Apply/abort called
                    'cfg/gl/a/hostname'
May 18 19:16:17.109      340      3      210      962      Verify called
                    'cfg/gl/a/hostname'
May 18 18:43:16.065      340      3      210      962      register
                    'cfg/gl/a/hostname'
May 18 18:41:41.048      340      3      16       362      register
                    'cfg/gl/a/hostname'
```

Related Commands

Command	Description
show sysdb connection path shared-plane	Displays sysDB client connection shared plane data for a specific path.

R3.9 Technical Checkpoint Review – Cisco Confidential

show tbm hardware

To displays tree bitmap hardware-related information, use the **show tbm hardware** command in EXEC mode.

```
show tbm hardware {ipv4 | ipv6 | mpls | vpnv4 | table-id | afi-all | sw-only | dual | egress |
  ingress} {unicast | multicast | safi-all} {dual | egress | ingress | sw-only} {brief | detail |
  lookup | prefix {prefix-hex-string}} location node-id
```

Syntax Description	
ipv4	Specifies IP Version 4 address prefixes.
ipv6	Specifies IP Version 6 address prefixes.
mpls	Specifies MPLS-related tree bitmap information.
vpnv4	Specifies VPNv4-related tree bitmap information.
table-id	Specifies tree bitmap information for a specific table ID.
afi-all	Specifies IPv4 and IPv6 commands.
sw-only	Specifies software-only tree bitmap information.
dual	Specifies tree bitmap information for dual, ingress, and egress, modes.
egress	Specifies egress tree bitmap information.
ingress	Specifies ingress tree bitmap information.
unicast	Specifies unicast address prefixes.
multicast	Specifies multicast address prefixes. This option is supported for IPv4 address families.
safi-all	For subaddress family, specifies prefixes for all subaddress families. This option is supported for IPv4 address families.
dual	Specifies ingress and egress tree bitmap information.
brief	Displays brief information.
detail	Displays detailed information.
lookup	Displays key or address information to look up (longest match) in the table.
prefix	Displays prefix-related information.
location <i>node-id</i>	Displays tree bitmap hardware-related information for a specified node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults No default behavior or values

Command Modes EXEC

R3.9 Technical Checkpoint Review – Cisco Confidential

Command History

Release	Modification
Release 3.7.2	This command was introduced on the Cisco ASR 9000 Series Router.
Release 3.9.0	No modification.

Usage Guidelines

To use this command, your Cisco IOS XR software system administrator must assign you to a user group associated with a task group that includes the corresponding command task IDs. If you need assistance with your task group assignment, contact your system administrator. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of *Cisco IOS XR System Security Configuration Guide*.

Use the **show tbm hardware** command to display hardware-related ingress and egress information for the tree bitmap.

Task ID

Task ID	Operations
cisco-support	read

Examples

The following example shows the output of the **show tbm hardware** command:

```
RP/0/RSP0/CPU0:router# show tbm hardware ipv4 unicast dual detail location 0/6/cpu0
```

```
TBM Table Type: IPv4 Unicast
-----
TBM: number of pulses: 71
TBM: number of Err fix attempts: 0
      No current failures
Past failures: leaf(0), mem(0), mipc(0), flush_mipc(0)
               post_compact(0), pre_compact(0)
```

```
PLU Bucket Statistics:
-----
```

```
Bucket 0: 44
Bucket 1: 44
Bucket 2: 327
Bucket 3: 44
Bucket 4: 44
Bucket 5: 43
Bucket 6: 43
Bucket 7: 45
```

```
Ingress PLU Info
-----
```

```
PLU: Num Writes : 3064
PLU: Num Copies : 2197
```

```
PLU Memory Channel Statistics:
-----
```

```
Number of compactions: 0
FCRAM0 Chan:      110 (Pages: 5, 1% used)
FCRAM1 Chan:      125 (Pages: 8, 0% used)
FCRAM2 Chan:      127 (Pages: 8, 0% used)
FCRAM3 Chan:      148 (Pages: 8, 0% used)
FCRAM4 Chan:      124 (Pages: 8, 0% used)
```

```
Egress PLU Info
```

R3.9 Technical Checkpoint Review – Cisco Confidential

```

-----
PLU: Num Writes : 3064
PLU: Num Copies : 2197

PLU Memory Channel Statistics:
-----
Number of compactions: 0
FCRAM0 Chan:      110 (Pages: 5, 1% used)
FCRAM1 Chan:      125 (Pages: 8, 0% used)
FCRAM2 Chan:      127 (Pages: 8, 0% used)
FCRAM3 Chan:      148 (Pages: 8, 0% used)
FCRAM4 Chan:      124 (Pages: 8, 0% used)
    
```

Table 3 describes the significant fields shown in the display.

Table 3 *show tbm hardware Field Descriptions*

Field	Description
Past failures	Number of times there was a failure in programming hardware.
PLU: Num Writes	Number of writes to the PLU portion of the hardware.
PLU: Num Copies	Number of copies to the PLU portion of the hardware.
PLU Memory Channel Statistics	Usage levels of each channel in the PLU memory.

R3.9 Technical Checkpoint Review – Cisco Confidential

show uidb data

To display index data information for the micro-interface descriptor block (uIDB), use the **show uidb data** command in EXEC mode.

show uidb data [**shadow**] [**ingress** | **egress**] [*interface-type interface-instance*] **location node-id**

Syntax Description	shadow	(Optional) Displays uIDB data from shadow copy Route Skill Mapping (RSM) instead of Metro HW.
	ingress	(Optional) Displays ingress PSE-related information.
	egress	(Optional) Displays egress PSE-related information.
	<i>interface-type</i>	Interface type. For more information, use the question mark (?) online help function.
	<i>interface-instance</i>	Either a physical interface instance or a virtual interface instance as follows: <ul style="list-style-type: none"> Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <ul style="list-style-type: none"> <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. <p>Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0.</p> <ul style="list-style-type: none"> Virtual interface instance. Number range varies depending on interface type. <p>For more information about the syntax for the router, use the question mark (?) online help function.</p>
	location node-id	Displays micro-IDB index data information for a specified node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

Defaults No default behavior or values

Command Modes EXEC

R3.9 Technical Checkpoint Review – Cisco Confidential

Command History	Release	Modification
	Release 3.7.2	This command was introduced on the Cisco ASR 9000 Series Router
	Release 3.9.0	No modification.

Usage Guidelines

To use this command, your Cisco IOS XR software system administrator must assign you to a user group associated with a task group that includes the corresponding command task IDs. If you need assistance with your task group assignment, contact your system administrator. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of *Cisco IOS XR System Security Configuration Guide*.

Use the **show uidb index** command to display micro-IDB index data information including, from a software perspective, features that are enabled on a selected interface.

Task ID	Task ID	Operations
	cisco-support	read

Examples

The following example shows the output of the **show uidb data** command:

```
RP/0/RSP0/CPU0:router# sh uidb data shadow ingress gigabitEthernet 0/2/4/4 loc 0/2/CPU0
-----
Location = 0/2/CPU0
Ifname/Ifhandle = GigabitEthernet0_2_4_4 / 0x12800a0
Index = 5
Pse direction = INGRESS
=====
*      (Not programmed in hardware)      *
-----
RSM STATUS: 0x7c000000
-> used: 0x1f
->dirty: 0x00
->badck: 0x00
-> prog: DONE
->count: 0
-----
BUNDLE IFHANDLE: 0
TUNNEL IFHANDLE: 0
L2 ENCAP: 3
=====

General 16 bytes:
-----
IFHANDLE: 0x12800a
STATUS: 1
ISSU State: 0
IPV4 ENABLE: 1
IPV6 ENABLE: 1
MPLS ENABLE: 0
STATS POINTER: 0x7ffd8
SPRAYER QUEUE: 36
IPV4 MULTICAST: 0
IPV6 MULTICAST: 0
USE TABLE ID IPV4: 0
USE TABLE ID IPV6: 0
USE TABLE ID MPLS: 0
```

R3.9 Technical Checkpoint Review – Cisco Confidential

```
TABLE ID: 0
QOS ENABLE: 0
QOS ID: 0
NETFLOW SAMPLING PERIOD: 0
L2 PKT DROP: 0
L2 QOS ENABLE: 0
SRC FWDING: 0
*[CHECKSUM]*: 0xff70f28c
```

Table 4 describes the significant fields shown in the display.

Table 4 show uidb data Field Descriptions

Field	Description
Location	Node in system where the interface resides.
Ifname/Ifhandle	Name associated with the interface.
Pse direction	Direction flag for UIDB data.
INDEX STATUS	Status of the interface.
L2 ENCAP	L2 encap type.
SPRAYER QUEUE LSB	Sprayer queue identifier.
ICMP PUNT FLAG	Flag indicating ICMP punts are enabled for the protocol.

Related Commands

Command	Description
show uidb trace	Displays UIDB trace data debugging information that helps in troubleshooting the problem.
show uidb data-dump	Displays UIDB data information in hexadecimal format.

R3.9 Technical Checkpoint Review – Cisco Confidential

show uidb trace

To display trace data information for the micro-interface descriptor block (IDB), use the **show uidb trace** command in EXEC mode.

show uidb trace {all | errors | events | init | rsm }

Syntax Description	all	Displays all UIDB trace information.
	errors	Displays information related to UIDB errors trace.
	events	Displays information related to UIDB events trace.
	init	Displays information related to UIDB init trace.
	rsm	Displays information related to UIDB rsm trace.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.7.2	This command was introduced on Cisco ASR 9000 Series Router.
	Release 3.9.0	No modification.

Usage Guidelines To use this command, your Cisco IOS XR software system administrator must assign you to a user group associated with a task group that includes the corresponding command task IDs. If you need assistance with your task group assignment, contact your system administrator. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	cisco-support	read

Examples The following example shows the sample output from the **show uidb trace** command:

```
RP/0/RSP0/CPU0:router# sh uidb trace init loc 0/6/CPU0
-----
28 wrapping entries (512 possible, 0 filtered, 28 total)
Mar 31 02:27:35.368 uidb_svr/initlog 0/6/CPU0 t1 Entering : Event manager init
Mar 31 02:27:36.641 uidb_svr/initlog 0/6/CPU0 t1 Successful : Event manager int
Mar 31 02:27:36.641 uidb_svr/initlog 0/6/CPU0 t1 Entering : Debug init
Mar 31 02:27:36.816 uidb_svr/initlog 0/6/CPU0 t1 Successful : Debug init
Mar 31 02:27:36.816 uidb_svr/initlog 0/6/CPU0 t1 Entering : MIPC bund
Mar 31 02:27:51.695 uidb_svr/initlog 0/6/CPU0 t1 Successful : MIPC bind
Mar 31 02:27:51.695 uidb_svr/initlog 0/6/CPU0 t1 PSE RSM : Init - main() : (50s
```

R3.9 Technical Checkpoint Review – Cisco Confidential

```

Mar 31 02:27:51.803 uidb_svr/initlog 0/6/CPU0 t1 Successful : PSE RSM Init succd
Mar 31 02:27:51.803 uidb_svr/initlog 0/6/CPU0 t1 Entering : Metro bind
Mar 31 02:27:51.828 uidb_svr/initlog 0/6/CPU0 t1 Successful : Metro bind
Mar 31 02:27:51.828 uidb_svr/initlog 0/6/CPU0 t1 Entering : PLIM ASIC register
Mar 31 02:27:51.922 uidb_svr/initlog 0/6/CPU0 t1 Successful : PLIM ASIC registr
Mar 31 02:27:51.922 uidb_svr/initlog 0/6/CPU0 t1 Entering : UIDB checkpoint int
Mar 31 02:27:51.944 uidb_svr/initlog 0/6/CPU0 t1 Successful : UIDB checkpoint t
Mar 31 02:27:51.944 uidb_svr/initlog 0/6/CPU0 t1 Entering : UIDB shadow memoryt
Mar 31 02:27:51.944 uidb_svr/initlog 0/6/CPU0 t1 Successful : UIDB shadow memot
Mar 31 02:27:51.944 uidb_svr/initlog 0/6/CPU0 t1 Entering : UIDB EDM init
Mar 31 02:27:51.951 uidb_svr/initlog 0/6/CPU0 t1 Successful : UIDB EDM init
Mar 31 02:27:51.951 uidb_svr/initlog 0/6/CPU0 t1 Entering : Checkpoint ingresse
Mar 31 02:27:51.951 uidb_svr/initlog 0/6/CPU0 t1 Successful : Checkpoint ingree
Mar 31 02:27:51.951 uidb_svr/initlog 0/6/CPU0 t1 Entering : Checkpoint egress e
Mar 31 02:27:51.951 uidb_svr/initlog 0/6/CPU0 t1 Successful : Checkpoint egrese
    
```

Related Commands

Command	Description
show uidb data	Displays UIDB index data information.
show uidb data-dump	Displays UIDB data information in hexadecimal format.

R3.9 Technical Checkpoint Review – Cisco Confidential

show uidb index

To display micro-interface descriptor block (IDB) index information, use the **show uidb index** command in EXEC mode.

show uidb index

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.7.2	This command was introduced on the Cisco ASR 9000 Series Router.
	Release 3.9.0	No modification.

Usage Guidelines To use this command, your Cisco IOS XR software system administrator must assign you to a user group associated with a task group that includes the corresponding command task IDs. If you need assistance with your task group assignment, contact your system administrator. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of *Cisco IOS XR System Security Configuration Guide*.

Use the **show uidb index** command to display the micro-IDB index assigned by the software.

Task ID	Task ID	Operations
	cisco-support	read

Examples The following example shows the output of the **show uidb index** command:

```
RP/0/RP0/CPU0:router# show uidb index
```

```
-----
Location Interface-name Interface-Type Ingress-index Egress-index
-----
0/1/CPU0 0 0
0/1/CPU0 GigabitEthernet0_1_5_0 Main interface 1
1
0/1/CPU0 GigabitEthernet0_1_5_1 Main interface 2
2
0/1/CPU0 GigabitEthernet0_1_5_2 Main interface 3
3
0/1/CPU0 GigabitEthernet0_1_5_3 Main interface 4
4
-----
```

R3.9 Technical Checkpoint Review – Cisco Confidential

```

0/1/CPU0 GigabitEthernet0_1_5_4      Main interface      5
5
0/1/CPU0 GigabitEthernet0_1_5_5      Main interface      6
6
0/1/CPU0 GigabitEthernet0_1_5_6      Main interface      7
7
0/1/CPU0 GigabitEthernet0_1_5_7      Main interface      8
8
0/1/CPU0 POS0_1_0_0                  Main interface      9                9
0/1/CPU0 POS0_1_4_0                  Main interface     10                10
0/1/CPU0 POS0_1_0_1                  Main interface     11                11
0/1/CPU0 POS0_1_4_1                  Main interface     12                12
0/1/CPU0 POS0_1_0_2                  Main interface     13                13
0/1/CPU0 POS0_1_4_2                  Main interface     14                14
0/1/CPU0 POS0_1_0_3                  Main interface     15                15
0/1/CPU0 POS0_1_4_3                  Main interface     16                16
0/1/CPU0 Bundle-POS24                Bundle Interface   17                17
0/1/CPU0 Bundle-Ether28              Bundle Interface18 18
0/1/CPU0 Bundle-Ether28.1            Sub-interface     19                19
0/1/CPU0 Bundle-Ether28.2            Sub-interface     20                20
0/1/CPU0 Bundle-Ether28.3            Sub-interface     21                21
0/6/CPU0 0                            0                0
0/6/CPU0 GigabitEthernet0_6_5_0      Main interface      1
1
0/6/CPU0 GigabitEthernet0_6_5_1      Main interface      2
2
0/6/CPU0 GigabitEthernet0_6_5_2      Main interface      3
3
0/6/CPU0 GigabitEthernet0_6_5_3      Main interface      4
4
0/6/CPU0 GigabitEthernet0_6_5_4      Main interface      5
5
0/6/CPU0 GigabitEthernet0_6_5_5      Main interface      6
6
0/6/CPU0 GigabitEthernet0_6_5_6      Main interface      7
7
0/6/CPU0 GigabitEthernet0_6_5_7      Main interface      8
8
0/6/CPU0 POS0_6_0_0                  Main interface      9                9
0/6/CPU0 POS0_6_4_0                  Main interface     10                10
0/6/CPU0 POS0_6_0_1                  Main interface     11                11
0/6/CPU0 POS0_6_4_1                  Main interface     12                12
0/6/CPU0 POS0_6_0_2                  Main interface     13                13
0/6/CPU0 POS0_6_4_2                  Main interface     14                14
0/6/CPU0 POS0_6_0_3                  Main interface     15                15
0/6/CPU0 POS0_6_4_3                  Main interface     16                16
0/6/CPU0 POS0_6_4_4                  Main interface     17                17
0/6/CPU0 POS0_6_4_5                  Main interface     18                18
0/6/CPU0 POS0_6_4_6                  Main interface     19                19
0/6/CPU0 POS0_6_4_7                  Main interface     20                20

```

Table 5 describes the significant fields shown in the display.

Table 5 show uidb index Field Descriptions

Field	Description
Location	Node where index is located.
Interface-name	Name of the interface.
Interface-Type	Type of interface.

R3.9 Technical Checkpoint Review – Cisco Confidential

Table 5 *show uidb index Field Descriptions (continued)*

Field	Description
Ingress-index	Value associated with ingress processing on the interface.
Egress-index	Value associated with egress processing on the interface.

Related Commands

Command	Description
show uidb data	Displays IDB index data information.
show uidb data-dump	Displays UIDB data information in hexadecimal format.

R3.9 Technical Checkpoint Review – Cisco Confidential

watchdog threshold memory

To configure the value of memory available for each alarm threshold, use the **watchdog threshold memory** command in global configuration or interface configuration mode. To revert to the default threshold memory, use the **no** form of this command.

watchdog memory threshold [**location** *node-id*] **minor** *percentage-memory-available* **severe** *percentage-memory-available* **critical** *percentage-memory-available*

no watchdog memory threshold [**location** *node-id*] **minor** *percentage-memory-available* **severe** *percentage-memory-available* **critical** *percentage-memory-available*

Syntax Description

location <i>node-id</i>	Configures the threshold memory for a specified node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
minor	Specifies the threshold for the minor state.
<i>percentage-memory-available</i>	Memory consumption percentage. Range is from 5 to 40.
severe	Specifies the threshold for the severe state.
critical	Specifies the threshold for the critical state.

Defaults

Use the **show watchdog threshold memory defaults location all** command to display the default memory thresholds.

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced on the Cisco ASR 9000 Series Router.
Release 3.9.0	No modification.

Usage Guidelines

To use this command, your Cisco IOS XR software system administrator must assign you to a user group associated with a task group that includes the corresponding command task IDs. If you need assistance with your task group assignment, contact your system administrator. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of *Cisco IOS XR System Security Configuration Guide*.

Use the **watchdog threshold memory** command to configure the memory thresholds. Threshold values can be applied to all nodes or a specific node using the **location** *node-id* keyword and argument. If the local threshold settings are removed, the local settings return to those set globally. In addition, you can view default and configured thresholds.

[Table 6](#) lists the recommended memory threshold value calculations if the minor threshold is set to 20 percent, the severe threshold is set to 10 percent, and the critical threshold is set to 5 percent.

R3.9 Technical Checkpoint Review – Cisco Confidential

Table 6 Recommended Memory Threshold Values

Total Available Memory (MB)	Minor Threshold (20 percent of available memory)	Severe Threshold (10 percent of available memory)	Critical Threshold (5 percent of available memory)
128	25.6	12.8	6.4
256	51.2	25.6	12.8
512	102.4	51.2	25.6
1024	204.8	102.4	51.2
2048	409.6	204.8	102.4
4096	819.2	409.6	204.8

Task ID	Task ID	Operations
	cisco-support	read, write

Examples

The following example shows how to configure the memory available for each alarm threshold:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# watchdog threshold memory location 0/RP0/CPU0 minor 30
severe 20 critical 10
```

R3.9 Technical Checkpoint Review – Cisco Confidential