## CONTENTS

### CHAPTER 1

**debug iapp through debug ip ftp** 1

- debug iapp 3
- debug idmgr 4
- debug if-mgr efp-ext 6
- debug ima 7
- debug installer 9
- debug interface 10
- debug interface counters exceptions 11
- debug interface counters protocol memory 13
- debug interface states 14
- debug interface(vasi) 17
- debug iosd issu 18
- debug ip access-list hash-generation 19
- debug ip access-list intstats 21
- debug ip access-list turboacl 22
- debug ip admission consent 24
- debug ip admission capoudp 25
- debug ip auth-proxy 26
- debug ip auth-proxy ezvpn 29
- debug ip bgp 31
- debug ip bgp groups 34
- debug ip bgp igp-metric ignore 36
- debug ip bgp import 37
- debug ip bgp range 40
- debug ip bgp sso 42
- debug ip bgp updates 44
debug ip bgp vpnv4 checkpoint 46
debug ip bgp vpnv4 nsf 47
debug ip bgp vpnv4 unicast 48
debug ip bgp vpn6 unicast 50
debug ip casa affinities 52
debug ip casa packets 54
debug ip casa wildcards 56
debug ip cef 58
debug ip cef accounting non-recursive 61
debug ip cef fragmentation 64
depugin cef hash 66
depugin cef rhash 68
depugin cef subblock 70
depugin cef table 72
depugin ddns update 75
depugin dfp agent 82
depugin dhcp server 83
depugin dhcp server redundancy 86
depugin dhcp server snmp 87
depugin dns name-list 88
depugin dns view 90
depugin dns view-list 92
depugin domain 94
depugin domain replies 96
depugin drp 98
depugin dvmrp 99
depugin eigrp 102
depugin eigrp notifications 104
depugin error 105
depugin flow cache 108
depugin flow export 110
depugin ftp 112

CHAPTER 2  debug ip http all through debug ip rsvp 115
debug ip ospf database-timer rate-limit 244
debug ip ospf events 245
debug ip ospf lsa-maxage 246
debug ip ospf mpls traffic-eng advertisements 247
debug ip ospf nsf 249
debug ip ospf packet 250
debug ip ospf rib 252
debug ip ospf spf statistic 254
debug ip packet 256
dep bug ip pgm host 262
dep bug ip pgm router 264
dep bug ip pim 266
dep bug ip pim atm 270
dep bug ip pim auto-rp 271
dep bug ip policy 273
dep bug ip rbscp 275
dep bug ip rbscp ack-split 276
dep bug ip rgmp 278
dep bug ip rip 279
dep bug ip routing 281
dep bug ip routing static bfd 283
dep bug ip rsvp 284
dep bug ip rsvp aggregation 289
dep bug ip rsvp authentication 291
dep bug ip rsvp detail 293
dep bug ip rsvp dump-messages 295
dep bug ip rsvp errors 298
dep bug ip rsvp hello 300
dep bug ip rsvp high-availability 302
dep bug ip rsvp p2mp 305
dep bug ip rsvp policy 306
dep bug ip rsvp rate-limit 309
dep bug ip rsvp reliable-msg 311
dep bug ip rsvp sbm 313
debug ip rsvp sso 315
debug ip rsvp summary-refresh 317
debug ip rsvp traffic-control 319
debug ip rsvp wfq 321

CHAPTER 3

dbg ip rtp header-compression through debug ipv6 icmp 323

dbg ip rtp header-compression through debug ipv6 icmp 324
dbg ip rtp header-compression 324
dbg ip rtp packets 324
dbg ip scp 325
dbg ip setp api 326
dbg ip setp congestion 328
dbg ip setp init 330
dbg ip setp multihome 332
dbg ip setp performance 334
dbg ip setp rcvchunks 336
dbg ip setp rto 337
dbg ip setp segments 339
dbg ip setp segmentv 341
dbg ip setp signal 344
dbg ip setp sndchunks 345
dbg ip setp state 348
dbg ip setp timer 350
dbg ip setp warnings 352
dbg ip sd 353
dbg ip sdee 354
dbg ip security 355
dbg ip sla error 357
dbg ip sla ethernet-monitor 358
dbg ip sla monitor error 359
dbg ip sla monitor mpls-lsp-monitor 361
dbg ip sla trace 362
dbg ip sla mpls-lsp-monitor 364
dbg ip sla trace 365
debug ip sla trace mpls-lsp-monitor  367
download ip sla trace twamp  368
download ip slb  369
download ip snat  373
download ip socket  374
download ip ssh  377
download ip subscriber  379
download ip subscriber redundancy  380
download ip tcp congestion  380
download ip tcp driver  382
download ip tcp driver-pak  384
download ip tcp ecn  385
download ip tcp ha  386
download ip tcp intercept  387
download ip tcp packet  389
download ip tcp transactions  390
download ip traffic-export events  392
download ip trigger-authentication  393
download ip trm  395
download ip urd  395
download ip urlfilter  396
download ip verify mib  398
download ip virtual-reassembly  400
download ip wccp  401
download ip  403
download ip acls  404
download ip errors  405
download ip events  406
download ip fragments  407
download ip nacks  410
download ip packets  411
download ip rpc  414
download iphc ip  416
download ipv6 cef drop  417
debug ipv6 cef events 419
d debug ipv6 cef hash 420
d debug ipv6 cef receive 421
d debug ipv6 cef table 423
d debug ipv6 dhcp 424
d debug ipv6 dhcp database 425
d debug ipv6 dhcp redundancy 426
d debug ipv6 dhcp relay 426
d debug ipv6 eigrp 427
d debug ipv6 icmp 428

ddebug ipv6 inspect through debug local-ack state 433
d debug ipv6 inspect 436
d debug ipv6 mfib 438
d debug ipv6 mld 440
d debug ipv6 mld explicit 442
d debug ipv6 mld ssm-map 443
d debug ipv6 mobile 444
d debug ipv6 mobile mag 445
d debug ipv6 mobile networks 449
d debug ipv6 mobile packets 450
d debug ipv6 mobile router 452
d debug ipv6 mrib client 453
d debug ipv6 mrib io 454
d debug ipv6 mrib proxy 455
d debug ipv6 mrib route 456
d debug ipv6 mrib table 457
d debug ipv6 multicast aaa 458
d debug ipv6 multicast rpf 460
d debug ipv6 multicast rwatch 461
d debug ipv6 nat 462
d debug ipv6 nd 464
d debug ipv6 ospf 467
d debug ipv6 ospf database-timer rate-limit 469
debug isis mpls traffic-eng advertisements 549
debug isis mpls traffic-eng events 551
debug isis nsf 552
debug isis rib 554
debug isis rib redistribution 556
debug isis spf statistics 558
debug isis spf-events 560
debug isis update-packets 561
debug iu a as 563
d debug iu a as p 564
d debug kerberos 566
d debug kpml 568
d debug kron 574
d debug l2ctrl 576
d debug l2fib 577
d debug l2relay events 579
d debug l2relay packets 580
d debug l2tp 581
d debug l2tp redundancy 583
d debug l2vpn acircuit 590
d debug l2vpn atom checkpoint 592
d debug l2vpn atom event-trace 594
d debug l2vpn atom fast-failure-detect 595
d debug l2vpn atom signaling 596
d debug l2vpn atom static-oam 598
d debug l2vpn atom vc 599
d debug l2vpn atom vc vccv 602
d debug l2vpn pseudowire 604
d debug l2vpn vfi 605
d debug l2vpn xconnect 606
d debug l3-mgr tunnel 607
d debug l4f 609
d debug lacp 611
d debug lane client 614
debug lane config 623
d debug lane finder 625
d debug lane server 626
 debug lane signaling 629
d debug lapb 631
d debug lapb-ta 636
d debug lat packet 638
 debug ldap 640
d debug lex rcmd 642
 debug license 645
d debug link monitor 647
 debug list 648
d debug llc2 dynwind 651
 debug llc2 errors 652
 debug llc2 packet 653
 debug llc2 state 655
 debug lnm events 656
 debug lnm llc 659
d debug lnm mac 662
 debug local-ack state 664
debug iapp through debug ip ftp

- debug iapp, on page 3
- debug idmgr, on page 4
- debug if-mgr efp-ext, on page 6
- debug ima, on page 7
- debug installer, on page 9
- debug interface, on page 10
- debug interface counters exceptions, on page 11
- debug interface counters protocol memory, on page 13
- debug interface states, on page 14
- debug interface(vasi), on page 17
- debug iosd issu, on page 18
- debug ip access-list hash-generation, on page 19
- debug ip access-list intstats, on page 21
- debug ip access-list turboacl, on page 22
- debug ip admission consent, on page 24
- debug ip admission eapoudp, on page 25
- debug ip auth-proxy, on page 26
- debug ip auth-proxy ezvpn, on page 29
- debug ip bgp, on page 31
- debug ip bgp groups, on page 34
- debug ip bgp igp-metric ignore, on page 36
- debug ip bgp import, on page 37
- debug ip bgp range, on page 40
- debug ip bgp sso, on page 42
- debug ip bgp updates, on page 44
- debug ip bgp vpnv4 checkpoint, on page 46
- debug ip bgp vpnv4 nsf, on page 47
- debug ip bgp vpnv4 unicast, on page 48
- debug ip bgp vpnv6 unicast, on page 50
- debug ip casa affinities, on page 52
- debug ip casa packets, on page 54
- debug ip casa wildcards, on page 56
- debug ip cef, on page 58
• debug ip cef accounting non-recursive, on page 61
• debug ip cef fragmentation, on page 64
• debug ip cef hash, on page 66
• debug ip cef rhash, on page 68
• debug ip cef subblock, on page 70
• debug ip cef table, on page 72
• debug ip ddns update, on page 75
• debug ip dfp agent, on page 82
• debug ip dhcp server, on page 83
• debug ip dhcp server redundancy, on page 86
• debug ip dhcp server snmp, on page 87
• debug ip dns name-list, on page 88
• debug ip dns view, on page 90
• debug ip dns view-list, on page 92
• debug ip domain, on page 94
• debug ip domain replies, on page 96
• debug ip drp, on page 98
• debug ip dvmrp, on page 99
• debug ip eigrp, on page 102
• debug ip eigrp notifications, on page 104
• debug ip error, on page 105
• debug ip flow cache, on page 108
• debug ip flow export, on page 110
• debug ip ftp, on page 112
debug iapp

Use the debug iapp privileged EXEC command to begin debugging of IAPP operations. Use the no form of this command to stop the debug operation.

[no] debug iapp {packets | event | error}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>packets</td>
<td>Displays IAPP packets sent and received by the access point. Link test packets are not displayed</td>
</tr>
<tr>
<td>event</td>
<td>Displays significant IAPP events</td>
</tr>
<tr>
<td>error</td>
<td>Displays IAPP software and protocol errors</td>
</tr>
</tbody>
</table>

Command Default

This command has no default setting.

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(11)JA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

Examples

This example shows how to begin debugging of IAPP packets:

SOAP-AP# debug iapp packet

This example shows how to begin debugging of IAPP events:

SOAP-AP# debug iapp events

This example shows how to begin debugging of IAPP errors:

SOAP-AP# debug iapp errors

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show debugging</td>
<td>Displays all debug settings</td>
</tr>
</tbody>
</table>
To enable debugging for the identity manager (IDMGR), use the `debug idmgr` command in privileged EXEC mode. To disable debugging for the IDMGR, use the `no` form of this command.

```
debug idmgr {core | data | db | elog | flow local}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>core</td>
<td>Specifies debugging for the Layer 2 (L2) access core process flow.</td>
</tr>
<tr>
<td>data</td>
<td>Specifies debugging for data handling.</td>
</tr>
<tr>
<td>db</td>
<td>Specifies debugging for database interaction.</td>
</tr>
<tr>
<td>elog</td>
<td>Specifies debugging for event logging.</td>
</tr>
<tr>
<td>flow</td>
<td>Specifies debugging for remote and local interaction.</td>
</tr>
<tr>
<td>local</td>
<td></td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(2)S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

You can use the `debug idmgr` command to debug errors such as missing or incorrect attributes in a session or Accounting, Authentication, and Authorization (AAA) records.

### Usage Guidelines

The following is sample output from the `debug idmgr` command:

```
Router# debug idmgr core
IDMGR core process flow debugging is on
Router# debug idmgr data
IDMGR data handling debugging is on
Router# debug idmgr db
IDMGR database interaction debugging is on
R1# debug idmgr elog
IDMGR event logging debugging is on
R1# debug idmgr flow local
IDMGR local process flow debugging is on
2w6d: %SYS-5-CONFIG_I: Configured from console by console
2w6d: IDMGR: Enabled core flow debugging
2w6d: IDMGR: Enabled local flow debugging
2w6d: IDMGR: Enabled DB interaction debugging
2w6d: IDMGR: (07EC4890) got an Session Assert Request
2w6d: IDMGR: (07EC4890) Local processing Session Assert Request
2w6d: IDMGR: Set field session-handle 2281701385(88000009) in idmgr db record
2w6d: IDMGR: Set field aaa-unique-id 16(00000010) in idmgr db record
2w6d: IDMGR: Set field composite-key in idmgr db record
2w6d: IDMGR: Set field idmgr-data in idmgr db record
2w6d: IDMGR: (07EC4890) Adding new record 07640138 for session handle 88000009 to Session DB
2w6d: IDMGR: Enabled core flow debugging
2w6d: IDMGR: Enabled local flow debugging
2w6d: IDMGR: Enabled DB interaction debugging
```
2w6d: IDMGR:(07EC4890) got an Session Update Event
2w6d: IDMGR:(07EC4890) Local processing Session Update Event
2w6d: IDMGR:(07EC4890) Search for session record
2w6d: IDMGR: Set field session-handle 2281701385(88000009) in search record
2w6d: IDMGR:(07EC4890) Found match for session handle 88000009
2w6d: IDMGR:(07EC4890) Found record in search get, returning 07640138
2w6d: IDMGR: releasing memory for search record field with type session-handle
2w6d: IDMGR: Set field idmgr-mask 4294967295(FFFFFFFF) in search record
2w6d: IDMGR: releasing memory for search record field with type idmgr-mask
Router#
2w6d: IDMGR:(07EC4890) Updating attribute authen-status in datalist
2w6d: IDMGR:(07EC4890) Updated record 07640138 for 88000009 to Session DB

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show subscriber session</td>
<td>Displays information about subscriber sessions on an ISG.</td>
</tr>
</tbody>
</table>
debug if-mgr efp-ext

To enable debugging for the interface manager (IF-MGR) Ethernet flow point (EFP) extension, use the `debug if-mgr efp-ext` command in privileged EXEC mode. To turn off debugging for the IF-MGR EFP extension, use the `no` form of this command.

```
diff debug if-mgr {errors | trace} efp-ext
no debug if-mgr {errors | trace} efp-ext
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>errors</code></td>
<td>Specifies debugging for IF-MGR EFP extension errors.</td>
</tr>
<tr>
<td><code>trace</code></td>
<td>Specifies debugging for IF-MGR EFP extension traces.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRD1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before you issue the `debug if-mgr efp-ext` command, consider the high volume of output that debug commands usually generate and the amount of time the debugging operation may take.

**Examples**

The following example shows how to enable debugging for IF-MGR EFP extension errors:

```
Router> enable
Router# debug if-mgr errors efp-ext
Router#
```
debug ima

To display debugging messages for inverse multiplexing over AMT (IMA) groups and links, use the `debug ima` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ima
no debug ima
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging for IMA groups is not enabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(5)XK</td>
<td>This command was modified.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows output when you enter the `debug ima` command while adding two ATM links to an IMA group. Notice that the group has not yet been created with the `interface atm slot /ima group-number` command, so the links are not activated yet as group members. However, the individual ATM links are deactivated.

```
Router# debug ima

IMA network interface debugging is on

Router# config terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# interface atm1/0

Router(config-if)# ima-group 1

Router(config-if)#

01:35:08:IMA shutdown atm layer of link ATM1/0
01:35:08:ima_clear_atm_layer_if ATM1/0
01:35:08:IMA Link ATM1/0 removed in firmware
01:35:08:ima_release_channel:ATM1/0 released channel 0.
01:35:08:Bring up ATM1/4 that had been waiting for a free channel.
01:35:08:IMA:no shut the ATM interface.
01:35:08:IMA allocate_channel:ATM1/4 using channel 0.
01:35:08:IMA config_restart ATM1/4
01:35:08:IMA

adding link 0 to Group ATM1/IMA1ATM1/0 is down waiting for IMA group 1 to be activated
01:35:08:Link 0 was added to Group ATM1/IMA1
01:35:08:ATM1/0 is down waiting for IMA group 1 to be created.
01:35:08:IMA send AIS on link ATM1/0
01:35:08:IMA Link up/down Alarm:port 0, new status 0x10, old status 0x1.
01:35:10:%LINK-3-UPDOWN:Interface ATM1/4, changed state to up
01:35:10:%LINK-3-UPDOWN:Interface ATM1/0, changed state to down
01:35:11:%LINEPROTO-5-UPDOWN:Line protocol on Interface ATM1/4, changed state to up
01:35:11:%LINEPROTO-5-UPDOWN:Line protocol on Interface ATM1/0, changed state to down
```
Router(config-if)# int atm1/1
Router(config-if)# ima-group 1
Router(config-if)#
01:37:19:IMA shutdown atm layer of link ATM1/1
01:37:19:ima_clear_atm_layer_if ATM1/1
01:37:19:IMA link ATM1/1 removed in firmware
01:37:19:ima_release_channel:ATM1/1 released channel 1.
01:37:19:Bring up ATM1/5 that had been waiting for a free channel.
01:37:19:IMA:no shut the ATM interface.
01:37:19:IMA allocate_channel:ATM1/5 using channel 1.
01:37:19:IMA config_restart ATM1/5
01:37:19:IMA adding link 1 to Group ATM1/IMA ATM1/1 is down waiting for IMA group 1 to be activated
01:37:19:Link 1 was added to Group ATM1/IMA
01:37:19:ATM1/1 is down waiting for IMA group 1 to be created.
01:37:19:IMA send AIS on link ATM1/1
01:37:19:IMA Link up/down Alarm:port 1, new status 0x10, old_status 0x1.
Router(config-if)#
01:37:21:%LINK-3-UPDOWN:Interface ATM1/5, changed state to up
01:37:21:%LINK-3-UPDOWN:Interface ATM1/1, changed state to down
01:37:22:%LINEPROTO-5-UPDOWN:Line protocol on Interface ATM1/5, changed state to up
01:37:22:%LINEPROTO-5-UPDOWN:Line protocol on Interface ATM1/1, changed state to down

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug backhaul-session-manager set</td>
<td>Displays debugging messages for ATM errors, and reports specific problems such as encapsulation errors and errors related to OAM cells.</td>
</tr>
<tr>
<td>debug events</td>
<td>Displays debugging messages for ATM events, and reports specific events such as PVC setup completion, changes in carrier states, and interface rates.</td>
</tr>
</tbody>
</table>
debug installer

To enable debugs in the installer, use the `debug installer` command in Privileged EXEC mode. To disable debugging use the `no` form of the command.

```
deploy installer [ { all | process | issu | common } ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>process</th>
<th>issu</th>
<th>common</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enables all installer debugs</td>
<td>Enables all the debugs inside Installer process</td>
<td>Enables all the debugs inside the installer's Bash provisioning scripts</td>
<td>Enables all the debugs inside the installer common code</td>
</tr>
<tr>
<td>process</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>issu</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>common</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

No debugs enabled

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS XE 3.2.0 SE</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The debug output for the above commands is displayed to the console and/or the IOS logging buffer. It's always a good idea to turn on `debug installer all` when troubleshooting installer related problems.

**Examples**

To enable all installer debugs, perform the following:

```
infra-p2-3#debug installer all
All installer debugging is on
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show version</td>
<td>To display information about the currently loaded software along with hardware and device information, use the <code>show version</code> command.</td>
</tr>
</tbody>
</table>
debug interface

To display interface descriptor block debugging messages, use the `debug interface` command in privileged EXEC mode. To disable the debugging messages, use the `no` form of this command.

`debug interface type number`
`no debug interface type number`

**Syntax Description**

| type number | Interface type and number. In the case of an ATM interface, you get the following options once you enter the interface type and number:
| --- | --- |
| • vc | Displays information about the virtual circuit.
| • [vpi /]vci | Specifies the virtual channel identifier (VCI) or virtual path identifier/virtual channel identifier (VPI/VCI) pair, if the interface to be debugged is an ATM-encapsulated interface. Valid values for vpi are 0 to 255. Valid values for vci are 1 to 65535.

**Command Default**

By default, debugging messages are not enabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(26)S.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug interface` command:

```
Router# debug interface ATM 1/0 vc 0/5
Condition 1 set
*Jan 31 19:36:38.399: ATM VC Debug: Condition 1, atm-vc 0/5 AT1/0 triggered, count 1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug interface counters exceptions</code></td>
<td>Displays a message when a recoverable exceptional condition happens during the computation of the interface packet and data rate statistics.</td>
</tr>
<tr>
<td><code>debug interface counters protocol memory</code></td>
<td>Displays the memory operations (create and free) of protocol counters on interfaces and debugging messages during memory operations.</td>
</tr>
</tbody>
</table>
debug interface counters exceptions

To display a message when a recoverable exceptional condition happens during the computation of the interface packet and data rate statistics, use the **debug interface counters exceptions** command in privileged EXEC mode. To disable debugging output, use the no form of this command.

```
depbug interface counters exceptions
no debug interface counters exceptions
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

By default, the debugging messages are not enabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(26)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **debug interface counters exceptions** command to debug problems where the packet counter values or rates have unexpected values. The command helps to flag interfaces whose packet counter values have decreased in number. This condition can occur if a packet is counted and then dropped. This command helps you to determine if the input and output rate statistics are adjusted to display a zero value versus an unexpected value. It is also possible for zero values to be displayed if an interface is running at or close to its maximum capacity due to interface statistics being viewed as negative values.

This message is rate limited to one message per minute. If multiple interfaces are having unexpected counter statistic issues, then a message is displayed only for the first interface that experiences a problem within a minute.

**Examples**

The following is sample output from the **debug interface counters exceptions** command when backward-going counters are detected. The output is self-explanatory.

```
Router# debug interface counters exceptions
IF-4-BACKWARD_COUNTERS: Corrected for backward rx_bytes counters (561759 -> 526385) on Multilink1
IF-4-BACKWARD_COUNTERS: Corrected for backward tx_bytes counters (288114 -> 268710) on Multilink1
IF-4-BACKWARD_COUNTERS: Corrected for backward tx_bytes counters (2220 -> 0) on Virtual-Access4
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug interface</td>
<td>Displays the interface descriptor block debugging messages.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>debug interface counters protocol memory</code></td>
<td>Displays the memory operations (create and free) of protocol counters on interfaces and debugging messages during memory operations.</td>
</tr>
</tbody>
</table>
debug interface counters protocol memory

To display the memory operations (create and free) of protocol counters on interfaces and debugging messages during memory operations, use the **debug interface counters protocol memory** command in privileged EXEC mode. To disable the debugging output, use the **no** form of this command.

```
default interface counters protocol memory
no debug interface counters protocol memory
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

By default, the debugging messages are not enabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(26)S.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the **debug interface counters protocol memory** command. The output is self-explanatory.

```
Router# debug interface counters protocol memory
interface counter protocol memory operations debugging is on
*Jan 11 11:34:08.154: IDB_PROTO: Ethernet0/0 created CDP
*Jan 11 11:35:08.154: IDB_PROTO: Ethernet0/0 reset CDP
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug interface</td>
<td>Displays the interface descriptor block debugging messages.</td>
</tr>
<tr>
<td>debug interface counters exceptions</td>
<td>Displays a message when a recoverable exceptional condition happens during the computation of the interface packet and data rate statistics.</td>
</tr>
</tbody>
</table>
**debug interface states**

To display intermediary messages when an interface's state transitions, use the `debug interface states` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug interface states
no debug interface states
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Debugging is disabled.

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(44)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(44)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command helps to debug interface state transition problems and includes the following interface state related message outputs:

- BRIDGE_ADJ--bridging database and Spanning tree protocol (STP) port state adjustment
- CSTATE_REQ--carrier state change request
- CSTATE_TMR--carrier timer state change
- LSTATE_REQ--line protocol state change request
- LSTATE_TMR--line protocol timer state change
- ROUTE_ADJ--route adjustment
- TRANS_ADJ--state transition adjustment

The debug information can be restricted to display state transitions on an interface basis using the `debug condition interface` command.

**Caution**
Because the `debug interface states` command is a global debug command for all the interfaces in the router, in some cases such as with online insertion and removal (OIR) this command generates a substantial amount of output, depending on the number of interfaces hosted on the shared port adapter (SPA) or the line card. Use the `debug condition interface` command instead for debugging an interface state transition problem.

**Examples**
The following is sample output from the `debug interface states` command when the `shutdown` command is executed on an interface. The output is self-explanatory.
Router# debug interface states
interface state transitions debugging is on
Router# debug condition interface fast0/0
Condition 1 set
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
  *Sep 1 12:24:46.294: [IDB Fa0/0 UARUYY] LSTATE_REQ: Entry
  *Sep 1 12:24:46.294: [IDB Fa0/0 UARUYY] LSTATE_REQ: timers not running
  *Sep 1 12:24:46.294: [IDB Fa0/0 UARUYY] LSTATE_REQ: Exit
Router(config)# interface fast0/0
Router(config-if)# shut
Router(config-if)#
  *Sep 1 12:24:56.294: [IDB Fa0/0 UARUYY] LSTATE_REQ: Entry
  *Sep 1 12:24:56.294: [IDB Fa0/0 UARUYY] LSTATE_REQ: timers not running
  *Sep 1 12:24:56.294: [IDB Fa0/0 UARUYY] LSTATE_REQ: Exit
  *Sep 1 12:24:57.162: [IDB Fa0/0 UARUYY] CSTATE_REQ: Entry, requested
  state: A
  *Sep 1 12:24:57.162: [IDB Fa0/0 UARUYY] CSTATE_REQ: state assign
  *Sep 1 12:24:57.162: [IDB Fa0/0 UARUYY] LSTATE_REQ: Entry
  *Sep 1 12:24:57.162: [IDB Fa0/0 UARUYY] LSTATE_REQ: Exit
  *Sep 1 12:24:57.162: [IDB Fa0/0 UARUYY] CSTATE_REQ: Exit
  *Sep 1 12:24:57.162: [IDB Fa0/0 UARUYY] CSTATE_REQ: Entry, requested
  state: A
  *Sep 1 12:24:57.162: [IDB Fa0/0 UARUYY] CSTATE_REQ: state assign
  *Sep 1 12:24:57.162: [IDB Fa0/0 UARUYY] LSTATE_REQ: Entry
  *Sep 1 12:24:57.162: [IDB Fa0/0 UARUYY] LSTATE_REQ: Exit
  *Sep 1 12:24:57.162: [IDB Fa0/0 UARUYY] CSTATE_REQ: Exit
  *Sep 1 12:24:57.166: [IDB Fa0/0 AURUYY] TRANS_ADJ: Entry
  *Sep 1 12:24:57.166: [IDB Fa0/0 AURUYY] TRANS_ADJ: propagating change
to subifs
  *Sep 1 12:24:57.170: [IDB Fa0/0 AURUYY] TRANS_ADJ: Exit
  *Sep 1 12:24:57.170: [IDB Fa0/0 AURUYY] ROUTE_ADJ: Entry
  *Sep 1 12:24:57.170: [IDB Fa0/0 AURUYY] BRIDGE_ADJ: Entry
  *Sep 1 12:24:57.170: [IDB Fa0/0 AURUYY] BRIDGE_ADJ: Exit
  *Sep 1 12:24:59.162: [IDB Fa0/0 AURUYY] CSTATE_TMP: Entry
  *Sep 1 12:24:59.162: [IDB Fa0/0 AURUyy] CSTATE_TMP: netidb=Fa0/0,
linestate: n
  *Sep 1 12:24:59.162: [IDB Fa0/0 AURUyy] LSTATE_REQ: Entry
  *Sep 1 12:24:59.162: [IDB Fa0/0 AURUyy] LSTATE_REQ: timers not running
  *Sep 1 12:24:59.162: [IDB Fa0/0 AURUyy] LSTATE_REQ: starting lineproto
timer
  *Sep 1 12:24:59.162: [IDB Fa0/0 AURUyy] LSTATE_REQ: Exit
  *Sep 1 12:24:59.162: [IDB Fa0/0 AURUyy] CSTATE_TMP: transition detected
  *Sep 1 12:24:59.162: ENTITY_ALARM-6-INFO: ASSERT INFO Fa0/0 Physical
Port Administrative State Down
  *Sep 1 12:24:59.162: [IDB Fa0/0 AURUyy] TRANS_ADJ: Entry
  *Sep 1 12:24:59.162: [IDB Fa0/0 AURUyy] TRANS_ADJ: Exit
  *Sep 1 12:24:59.162: [IDB Fa0/0 AURUyy] CSTATE_TMP: Exit
  *Sep 1 12:25:00.162: [IDB Fa0/0 AURUyy] LSTATE_TMP: Entry
  *Sep 1 12:25:00.162: [IDB Fa0/0 AURUyy] CSTATE_TMP: not spoofing,
current state: n
  *Sep 1 12:25:00.162: [IDB Fa0/0 AURUyy] LSTATE_TMP: informing line
state transitions
  *Sep 1 12:25:00.162: [IDB Fa0/0 AURUyy] TRANS_ADJ: Entry
  *Sep 1 12:25:00.162: [IDB Fa0/0 AURUyy] TRANS_ADJ: Exit
  *Sep 1 12:25:00.162: [IDB Fa0/0 AURUyy] ROUTE_ADJ: Entry
  *Sep 1 12:25:00.162: [IDB Fa0/0 AURUyy] ROUTE_ADJ: Exit
  *Sep 1 12:25:00.162: [IDB Fa0/0 AURUyy] LSTATE_TMP: Exit

Cisco IOS Debug Command Reference - Commands I through L
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>debug condition interface</strong></td>
<td>Limits output for some debug commands on the basis of the interface, VC, or VLAN.</td>
</tr>
</tbody>
</table>
### debug interface(vasi)

To display debugging information for the VRF-Aware Service Infrastructure (VASI) interface descriptor block, use the `debug interface` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

**debug interface {vasileft | vasiright} number**

**no debug interface {vasileft | vasiright} number**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vasileft</code></td>
<td>Displays information about vasileft interface.</td>
</tr>
<tr>
<td><code>vasiright</code></td>
<td>Displays information about vasiright interface.</td>
</tr>
<tr>
<td><code>number</code></td>
<td>Identifier of the VASI interface. The range is from 1 to 256.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.6</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug interface` command:

```
Router# debug interface vasileft 100
Condition 1 set
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface (vasi)</code></td>
<td>Configures a VASI virtual interface.</td>
</tr>
<tr>
<td><code>debug adjacency (vasi)</code></td>
<td>Displays debugging information for the VASI adjacency.</td>
</tr>
<tr>
<td><code>debug vasi</code></td>
<td>Displays debugging information for the VASI.</td>
</tr>
<tr>
<td><code>show vasi pair</code></td>
<td>Displays the status of a VASI pair.</td>
</tr>
</tbody>
</table>
**debug iosd issu**

To enable all the debugging for the IOS issu iosd and iosvrp issu_upgrades subsystems, use the `debug iosd issu` command in Privileged EXEC mode. To disable debugging use the `no` form of the command.

**debug iosd issu**

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Deblogs not enabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command Modes</strong></td>
<td>Privileged EXEC</td>
</tr>
<tr>
<td><strong>Command History</strong></td>
<td>Release</td>
</tr>
<tr>
<td></td>
<td>IOS XE 3.2.0 SE</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No command variables

It's always a good idea to turn on `debug iosd issu` when troubleshooting installer related problems

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show version</td>
<td>To display information about the currently loaded software along with hardware and device information, use the <code>show version</code> command.</td>
</tr>
</tbody>
</table>
debug ip access-list hash-generation

To display debugging information about access control list (ACL) hash-value generation (for ACL Syslog entries), use the `debug ip access-list hash-generation` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
depbug ip access-list hash-generation
no debug ip access-list hash-generation
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
This command is disabled.

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(22)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use this command when configuring an access control entry (ACE) to view the router-generated hash values for the ACE.

This command displays the input and output for the hash-generation mechanism. The input is the ACE text and ACL name. The output is an MD5 algorithm-derived, 4-byte value.

**Examples**

The following example shows sample debug output displayed when configuring ACL hash-value generation.

```
Router# debug ip access-list hash-generation
Syslog hash code generation debugging is on
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip access-list logging hash-generation
Router(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log
Router(config)#
*Aug 9 00:25:31.661: %IPACL-HASHGEN: Hash Input: 101 extended permit 6 host 20.1.1.1 host 20.1.1.2 Hash Output: 0xA363BB54
Router(config)# exit
Router# exit
```

**Note**
The example in this section shows sample output for a numbered access list. However, you can configure ACL hash-value generation for both numbered and named access lists, and for both standard and extended access lists.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list logging hash-generation</td>
<td>Enables the generation of hash-values for access control entries in the system messaging logs.</td>
</tr>
<tr>
<td>show ip access-list</td>
<td>Displays the contents of all current access lists.</td>
</tr>
</tbody>
</table>
debug ip access-list intstats

To display information about whether or not the interface-level statistics of an access list were created, updated, cleared or deleted successfully, use the `debug ip access-list intstats` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
default ip access-list intstats
no default ip access-list intstats
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behaviors or values

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip access-list intstats` command:

```
Router# debug ip access-list intstats
Router# enable
Router# configure terminal
Router(config)# interface e0/0
Router(config-if)# ip access-group 100 in
*Oct 29 08:52:16.763: IPACL-INTSTATS: ACL swsb created
*Oct 29 08:52:16.763: IPACL-INTSTATS: ACL header stats structure created
*Oct 29 08:52:16.763: IPACL-INTSTATS: I/P stats table created
*Oct 29 08:52:16.763: IPACL-INTSTATS: Statsid bitmap created
*Oct 29 08:52:16.763: IPACL-INTSTATS: Done with static ACEs
Router(config-if)# ip access-group 100 out
*Oct 29 08:52:19.435: IPACL-INTSTATS: O/P stats table created
*Oct 29 08:52:19.435: IPACL-INTSTATS: Done with static ACEs
```
debug ip access-list turboacl

To display debugging information about turbo access control lists (ACLs), use the `debug ip access-list turboacl` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip access-list turboacl
no debug ip access-list turboacl
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
No default behaviors or values

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(3)T</td>
<td>This command was modified to include support for turbo ACLs.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `debug ip access-list turboacl` command is useful for debugging problems associated with turbo ACLs. Turbo ACLs compile the ACLs into a set of lookup tables, while maintaining the first packet matching requirements. Packet headers are used to access these tables in a small, fixed, number of lookups, independent of the existing number of ACL entries.

**Examples**
The following is sample output from the `debug ip access-list turboacl` command:

```
Router# debug ip access-list turboacl
*Aug 20 00:41:17.843 UTC:Miss at index 73, 19
*Aug 20 00:41:17.843 UTC:Adding dynamic entry, update = 1
*Aug 20 00:41:17.843 UTC:Miss at index 21, 39
*Aug 20 00:41:17.847 UTC:Adding dynamic entry, update = 1
*Aug 20 00:41:17.847 UTC:Miss at index 116, 42
*Aug 20 00:41:17.851 UTC:Adding dynamic entry, update = 1
*Aug 20 00:41:17.851 UTC:Miss at index 119, 28
*Aug 20 00:41:17.851 UTC:Adding dynamic entry, update = 1
*Aug 20 00:41:17.851 UTC:Miss at index 119, 28
*Aug 20 00:41:17.851 UTC:Adding dynamic entry, update = 1
*Aug 20 00:41:17.855 UTC:Adding dynamic entry, update = 1
*Aug 20 00:41:17.855 UTC:Miss at index 92, 20
*Aug 20 00:41:17.855 UTC:Adding dynamic entry, update = 1
*Aug 20 00:41:17.855 UTC:Miss at index 119, 28
*Aug 20 00:41:17.855 UTC:Adding dynamic entry, update = 1
*Aug 20 00:41:17.855 UTC:Miss at index 56, 29
*Aug 20 00:41:17.859 UTC:Adding dynamic entry, update = 1
*Aug 20 00:41:17.859trv, update = 1
*Aug 20 00:41:19.959 UTC:Miss at index 29, 41
```
The table below describes the significant fields shown in the display.

### Table 1: debug ip access-list turboacl Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 20 00:41:17.843 UTC</td>
<td>Date and Coordinated Universal Time (UTC) the command was used to debug the turbo ACL.</td>
</tr>
<tr>
<td>Miss at index 73, 19</td>
<td>Location in the compiled access list tables where a new packet lookup does not match an existing entry.</td>
</tr>
<tr>
<td>Adding dynamic entry, update = 1</td>
<td>Action taken to add a new entry in the compiled access list tables as a result of a packet being processed.</td>
</tr>
</tbody>
</table>
debug ip admission consent

To display authentication proxy consent page information on the router, use the `debug ip admission consent` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip admission consent [{events | errors | messages}]
no debug ip admission consent
```

**Syntax Description**

- `errors` *(Optional)* Displays only error messages.
- `events` *(Optional)* Displays only event-related messages.
- `messages` *(Optional)* Displays only packet-related messages.

**Command Default**

If an option is not selected, all debug messages are displayed.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Examples**

Router# `debug ip admission consent errors`

IP Admission Consent Errors debugging is on

Router# `debug ip admission consent events`

IP Admission Consent Events debugging is on

Router# `debug ip admission consent messages`

IP Admission Consent Messages debugging is on

Router# `show debugging`

IP Admission Consent:
IP Admission Consent Errors debugging is on
IP Admission Consent Events debugging is on
IP Admission Consent Messages debugging is on
debug ip admission eapoudp

To display information about Extensible Authentication Protocol over User Datagram Protocol (UDP) (EAPoUDP) network admission control events, use the debug ip admission eapoudp command in privileged EXEC mode. To disable debugging output, use the no form of this command.

```
debug ip admission eapoudp
no debug ip admission eapoudp
```

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging is not enabled.

Command Modes

Privileged EXEC #

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

Examples

The following sample output from the debug ip admission eapoudp command shows information about network admission control using EAPoUDP. In the command output, the term “posture” refers to the credentials (for example, antivirus state or version of Cisco IOS software) of the host system.

```
Router# debug ip admission eapoudp
Posture validation session created for client mac= 0001.027c.f364 ip= 10.0.0.1
Total Posture sessions= 1 Total Posture Init sessions= 1
*Apr 9 19:39:45.684: %AP-6-POSTURE_START_VALIDATION: IP=10.0.0.1| Interface=FastEthernet0/0.420
*Apr 9 19:40:42.292: %AP-6-POSTURE_STATE_CHANGE: IP=10.0.0.1| STATE=POSTURE ESTAB
*Apr 9 19:40:42.292: auth_proxy_posture_parse_aaa_attributes:
CiscoDefined-ACL name= #ACSACL#-IP-HealthyACL-40921e54
Apr 9 19:40:42.957: %AP-6-POSTURE_POLICY: Apply access control list (xACSACLx-IP-HealthyACL-40921e54) policy for host (10.0.0.1)
```

The fields in the display are self-explanatory.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip admission</td>
<td>Displays IP admission control cache entries or the running admission control configuration.</td>
</tr>
</tbody>
</table>
debug ip auth-proxy

To display the authentication proxy configuration information on the router, use the `debug ip auth-proxy` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```plaintext
debug ip auth-proxy {detailed | ftp | function-trace | object-creation | object-deletion | telnet | timers}
no debug ip auth-proxy
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detailed</td>
<td>Displays details of the TCP events during an authentication proxy process. The details are generic to all FTP, HTTP, and Telnet protocols.</td>
</tr>
<tr>
<td>ftp</td>
<td>Displays FTP events related to the authentication proxy.</td>
</tr>
<tr>
<td>function-trace</td>
<td>Displays the authentication proxy functions.</td>
</tr>
<tr>
<td>object-creation</td>
<td>Displays additional entries to the authentication proxy cache.</td>
</tr>
<tr>
<td>object-deletion</td>
<td>Displays deletion of cache entries for the authentication proxy.</td>
</tr>
<tr>
<td>telnet</td>
<td>Displays Telnet-related authentication proxy events.</td>
</tr>
<tr>
<td>timers</td>
<td>Displays authentication proxy timer-related events.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(1)</td>
<td>The <code>detailed</code> keyword was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `debug ip auth-proxy` command to display authentication proxy activity.

#### Note

The `function-trace` debugging information provides low-level software information for Cisco technical support representatives. No output examples are provided for this keyword option.

### Examples

The following examples illustrate the output of the `debug ip auth-proxy` command. In these examples, debugging is on for object creations, object deletions, HTTP, and TCP.

In this example, the client host at 192.168.201.1 is attempting to make an HTTP connection to the web server located at 192.168.21.1. The HTTP debugging information is on for the authentication proxy. The output shows that the router is setting up an authentication proxy entry for the login request:
Following a successful login attempt, the debugging information shows the authentication proxy entries created for the client. In this example, the client is authorized for SMTP (port 25), FTP data (port 20), FTP control (port 21), and Telnet (port 23) traffic. The dynamic access control list (ACL) entries are included in the display.

The next example shows the debug output following a `clear ip auth-proxy cache` command to clear the authentication entries from the router. The dynamic ACL entries are removed from the router.

The following example shows the timer information for a dynamic ACL entry. All times are expressed in milliseconds. The `first laststart` is the time that the ACL entry is created relative to the startup time of the router. The `lastref` is the time of the last packet to hit the dynamic ACL relative to the startup time of the router. The `expetime` is the next expected expiration time for the dynamic ACL. The `delta` indicates the remaining time before the dynamic ACL expires. After the timer expires, the debugging information includes a message indicating that the ACL and associated authentication proxy information for the client have been removed.

The following example is sample output with the `detailed` keyword enabled:

```
00:12:36:AUTH-PROXY OBJ_DELETE:delete auth_proxy cache 61AD6298
00:12:36:AUTH-PROXY OBJ_DELETE:delete create acl wrapper 6151C7C8 -- acl item 61AD60CC
00:12:36:AUTH-PROXY OBJ_DELETE:delete create acl wrapper 6187A060 -- acl item 6151C908
00:12:36:AUTH-PROXY OBJ_DELETE:delete create acl wrapper 6187A0D4 -- acl item 61879550
00:12:36:AUTH-PROXY OBJ_DELETE:delete create acl wrapper 61879644 -- acl item 61879550
00:12:36:AUTH-PROXY OBJ_DELETE:delete create acl wrapper 61A40B88

The following example shows the timer information for a dynamic ACL entry. All times are expressed in milliseconds. The `first laststart` is the time that the ACL entry is created relative to the startup time of the router. The `lastref` is the time of the last packet to hit the dynamic ACL relative to the startup time of the router. The `expetime` is the next expected expiration time for the dynamic ACL. The `delta` indicates the remaining time before the dynamic ACL expires. After the timer expires, the debugging information includes a message indicating that the ACL and associated authentication proxy information for the client have been removed.

00:19:51:first laststart 1191112
00:20:51:AUTH-PROXY:delta 54220 lastref 1245332 expetime 1251112
00:21:45:AUTH-PROXY:ACL and cache are removed

The following example is sample output with the `detailed` keyword enabled:

```
00:37:50:AUTH-PROXY:proto_flag=5, dstport_index=1
00:37:50: SYN SEQ 245972 LEN 0
00:37:50:dst_addr 192.168.127.2 src_addr 192.168.27.1 dst_port 21 src_port 4347
```
00:37:50: AUTH-PROXY:auth_proxy_half_open_count++ 1
00:37:50: AUTH-PROXY:proto_flag=5, dstport_index=1
00:37:50: ACK 1820245643 SEQ 245973 LEN 0
00:37:50: dst_addr 192.168.127.2 src_addr 192.168.27.1 dst_port 21 src_port 4347
00:37:50: clientport 4347 state 0
00:37:50: AUTH-PROXY:incremented proxy_proc_count=1
00:37:50: AUTH-PROXY:proto_flag=5, dstport_index=1
00:37:50: ACK 1820245674 SEQ 245973 LEN 0
00:37:50: dst_addr 192.168.127.2 src_addr 192.168.27.1 dst_port 21 src_port 4347
00:37:50: clientport 4347 state 0
00:37:57: AUTH-PROXY:proto_flag=5, dstport_index=1
00:37:57: PSH ACK 1820245674 SEQ 245973 LEN 16
00:37:57: dst_addr 192.168.127.2 src_addr 192.168.27.1 dst_port 21 src_port 4347
00:37:57: clientport 4347 state 0
00:37:57: AUTH-PROXY:proto_flag=5, dstport_index=1
00:37:57: ACK 1820245699 SEQ 245989 LEN 0
00:37:57: dst_addr 192.168.127.2 src_addr 192.168.27.1 dst_port 21 src_port 4347
00:37:57: clientport 4347 state 0
00:38:01: AUTH-PROXY:proto_flag=5, dstport_index=1
00:38:01: PSH ACK 1820245699 SEQ 245989 LEN 16
00:38:01: dst_addr 192.168.127.2 src_addr 192.168.27.1 dst_port 21 src_port 4347
00:38:01: clientport 4347 state 0
00:38:01: AUTH-PROXY:Authenticating user ryan
00:38:01: AUTH-PROXY:Session state is INIT. Not updating stats
00:38:01: AUTH-PROXY:Sent AAA request successfully
00:38:01: AUTH-PROXY:Sent password successfully
00:38:01: AUTH-PROXY:processing authorization data
00:38:01: AUTH-PROXY:Sending accounting start.unique-id 2
00:38:01: AUTH-PROXY:Session state is INIT. Not updating stats
00:38:01: AUTH-PROXY:Session state is INIT. Not updating stats
00:38:01: AUTH-PROXY:wait complete on watched boolean stat=0
00:38:01: AUTH-PROXY:src ip addr is 192.168.127.2, dstaddr=192.168.27.1
00:38:01: AUTH-PROXY:src ip addr is 192.168.127.2, dstaddr=192.168.27.1
00:38:01: PSH ACK 2072458992 SEQ 4051022445 LEN 49
00:38:02: AUTH-PROXY:src ip addr is 192.168.127.2, dstaddr=192.168.27.1
00:38:02: ACK 2072459003 SEQ 4051022495 LEN 0
00:38:02: AUTH-PROXY:src ip addr is 192.168.127.2, dstaddr=192.168.27.1
00:38:02: PSH ACK 2072459003 SEQ 4051022495 LEN 33
00:38:02: AUTH-PROXY:src ip addr is 192.168.127.2, dstaddr=192.168.27.1
00:38:02: ACK 2072459014 SEQ 4051022528 LEN 26
00:38:03: AUTH-PROXY:proto_flag=5, dstport_index=1
00:38:03: ACK 1820245725 SEQ 246005 LEN 0
00:38:03: dst_addr 192.168.127.2 src_addr 192.168.27.1 dst_port 21 src_port 4347
00:38:03: clientport 4347 state 3

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show debug</td>
<td>Displays the debug options set on the router.</td>
</tr>
</tbody>
</table>
**debug ip auth-proxy ezvpn**

To display information related to proxy authentication behavior for web-based activation, use the `debug ip auth-proxy ezvpn` command in privileged EXEC mode. To turn off debugging, use the `no` form of this command.

```
dep in auth-proxy ezvpn
no debug ip auth-proxy ezvpn
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Debugging is not turned on.

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

⚠️ **Caution**

Using this command may result in considerable output if simultaneous authentications are taking place.

**Examples**

The following is output from the `debug ip auth-proxy ezvpn` command. The output displays the proxy authentication behavior of a web-based activation.

```
Router# debug ip auth-proxy ezvpn
*Dec 20 20:25:11.006: AUTH-PROXY: New request received by EzVPN WebIntercept from
10.4.205.205
*Dec 20 20:25:17.150: AUTH-PROXY:GET request received
*Dec 20 20:25:17.150: AUTH-PROXY:Authentication scheme is 401
*Dec 20 20:25:17.362: AUTH-PROXY:Allocated on credinfo for connect at 0x81EF1A84
*Dec 20 20:25:17.362: AUTH-PROXY:Posting CONNECT request to EzVPN
Dec 20 20:25:17.362: EZVPN(tunnel22): Received CONNECT from 10.4.205.205!
```

The output in the display is self-explanatory.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xauth userid mode</td>
<td>Specifies how the Cisco Easy VPN Client handles Xauth requests or prompts from the server.</td>
</tr>
</tbody>
</table>
**debug ip bgp**

To display information related to processing of the Border Gateway Protocol (BGP), use the `debug ip bgp` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip bgp [{ip-address | addpath | dampening | events | in | keepalives | out | updates | vpnv4 | mpls}]
no debug ip bgp [{ip-address | addpath | dampening | events | in | keepalives | out | updates | vpnv4 | mpls}]
```

**Cisco 10000 Series Router**

```
debug ip bgp [{ip-address | dampening | events | in | keepalives | out | updates | vpnv4 | mpls | all | groups | import | ipv4 | ipv6}]
no debug ip bgp [{ip-address | dampening | events | in | keepalives | out | updates | vpnv4 | mpls | all | groups | import | ipv4 | ipv6}]
```

### Syntax Description

<table>
<thead>
<tr>
<th><strong>Syntax</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>(Optional) The BGP neighbor IP address.</td>
</tr>
<tr>
<td><code>addpath</code></td>
<td>(Optional) Displays BGP additional path events.</td>
</tr>
<tr>
<td><code>dampening</code></td>
<td>(Optional) Displays BGP dampening.</td>
</tr>
<tr>
<td><code>events</code></td>
<td>(Optional) Displays BGP events.</td>
</tr>
<tr>
<td><code>in</code></td>
<td>(Optional) Displays BGP inbound information.</td>
</tr>
<tr>
<td><code>keepalives</code></td>
<td>(Optional) Displays BGP keepalives.</td>
</tr>
<tr>
<td><code>out</code></td>
<td>(Optional) Displays BGP outbound information.</td>
</tr>
<tr>
<td><code>updates</code></td>
<td>(Optional) Displays BGP updates.</td>
</tr>
<tr>
<td><code>mpls</code></td>
<td>(Optional) Displays Multiprotocol Label Switching (MPLS) information.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>(Optional) Displays all address family information.</td>
</tr>
<tr>
<td><code>groups</code></td>
<td>(Optional) Displays BGP configuration and update groups information.</td>
</tr>
<tr>
<td><code>import</code></td>
<td>(Optional) Displays BGP import routes to a VPN routing and forwarding (VRF) instance across address family information.</td>
</tr>
<tr>
<td><code>ipv4</code></td>
<td>(Optional) Displays BGP IPv4 address family information.</td>
</tr>
<tr>
<td><code>ipv6</code></td>
<td>(Optional) Displays BGP IPv6 address family information.</td>
</tr>
</tbody>
</table>

### Command Modes

- Privileged EXEC(#)
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(21)ST</td>
<td>This command was integrated into Cisco IOS Release 12.0(21)ST. The mpls keyword was added.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(22)S.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>The mpls keyword was added.</td>
</tr>
<tr>
<td>12.2(17b)SXA</td>
<td>This command was integrated into Cisco IOS Release 12.2(17b)SXA.</td>
</tr>
<tr>
<td>12.0(27)S</td>
<td>The command output was modified to show explicit-null label information.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was modified. The addpath keyword was added.</td>
</tr>
<tr>
<td>12.2(33)XNE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)XNE.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.5</td>
<td>This command was integrated into Cisco IOS XE Release 2.5.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command with the updates and mpls keywords to display explicit-null label information. The optional arguments in, out, keepalives, updates, and events provide verbose output to the debug ip bgp command. The sequence in which the optional arguments are provided affects the behavior of the command. The non peer specific commands override the peer-specific commands.

Examples

Following is the sample output from the `debug ip bgp` command used with vpnv4 keyword:

```
Router# debug ip bgp vpnv4
03:47:14:vpn:bgp_vpnv4_bnetinit:100:2:10.0.0.0/8
03:47:14:vpn:bnettable add:100:2:10.0.0.0/8
03:47:14:vpn:bestpath_hook route_tag_change for vpn2:10.0.0.0/255.0.0.0 (ok)
03:47:14:vpn:bgp_vpnv4_bnetinit:100:2:10.0.0.0/8
03:47:14:vpn:bnettable add:100:2:10.0.0.0/8
03:47:14:vpn:bestpath_hook route_tag_change for vpn2:10.0.0.0/255.0.0.0 (ok)
03:47:14:vpn:bgp_vpnv4_bnetinit:100:2:10.0.0.0/8
03:47:14:vpn:bnettable add:100:2:10.0.0.0/8
03:47:14:vpn:bestpath_hook route_tag_change for vpn2:10.0.0.0/255.0.0.0 (ok)
```

The following example shows sample output, including the explicit-null label, from the `debug ip bgp updates` and the `debug ip bgp mpls` commands:

```
Router# debug ip bgp updates
BGP updates debugging is on
Router# debug ip bgp mpls
BGP MPLS labels debugging is on
```

Router#
01:33:53: BGP(0): route 10.10.10.10/32 up
01:33:53: BGP(0): nettable_walker 10.10.10.10/32 route sourced locally
01:33:53: BGP: adding MPLS label to 10.10.10.10/32
01:33:53: BGP: check on 10.10.10.10/8 in LDP - ok
01:33:53: BGP: label imp-null allocated via LDP
01:33:53: BGP-IPv4: send exp-null label for 10.10.10.10/32
01:33:53: BGP-IPv4: Send prefix 10.10.10.10/32, label exp-null !explicit-null label being sent
01:33:53: BGP(0): 10.10.10.11 send UPDATE (format) 10.10.10.10/32, next 10.10.10.12, metric 0, path , mpls label 0 !label value is 0
01:33:53: BGP(0): updgrp 1 - 10.10.10.12 enqueued 1 updates, average/maximum size (bytes) 61/61

Following example shows a sample output from the debug ip bgp command when various arguments are provided in a particular sequence:

```
Router# debug ip bgp 209.165.200.225
Router# debug ip bgp 209.165.200.225 updates
Router# debug ip bgp keepalives
Router# debug ip bgp events
Router# debug ip bgp in
Router# debug ip bgp out

Router# show debug
IP routing:
 BGP debugging is on (outbound) for address family: IPv4 Unicast
 BGP events debugging is on
 BGP keepalives debugging is on
 BGP updates debugging is on (outbound) for address family: IPv4 Unicast

The behavior of the command changes when the arguments are provided in a different sequence:

```
Router# debug ip bgp keepalives
Router# debug ip bgp events
Router# debug ip bgp in
Router# debug ip bgp out
Router# debug ip bgp 209.165.200.225
Router# debug ip bgp 209.165.200.225 updates

Router# show debug
IP routing:
 BGP debugging is on for neighbor 209.165.200.225 for address family: IPv4 Unicast
 BGP events debugging is on for neighbor 209.165.200.225
 BGP keepalives debugging is on for neighbor 209.165.200.225 for address family: IPv4 Unicast
 BGP updates debugging is on for neighbor 209.165.200.225 for address family: IPv4 Unicast
```
### debug ip bgp groups

To display information related to the processing of Border Gateway Protocol (BGP) update-groups, use the `debug ip bgp update` privileged EXEC mode. To disable debugging output, use the `no` form of this command.

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ip bgp groups</code> [ `{index-group</td>
<td>ip-address}` ]</td>
</tr>
<tr>
<td><code>no debug ip bgp groups</code></td>
<td>(Optional) Specifies that update-group debugging information for a single peer will be displayed.</td>
</tr>
</tbody>
</table>

#### Command Default

No information about BGP update-groups is displayed.

#### Command Modes

Privileged EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(24)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

The output of this command displays information about update-group calculations and the addition and removal of update-group members. Information about peer-groups, peer-policy, and peer-session templates will also be displayed in the output of this command as neighbor configurations change.

#### Note

The output of this command can be very verbose. This command should not be deployed in a production network unless you are troubleshooting a problem.

When a change to outbound policy occurs, the router automatically recalculates update-group memberships and applies the changes by triggering an outbound soft reset after a 1-minute timer expires. This behavior is designed to provide the network operator with time to change the configuration if a mistake is made. You can manually enable an outbound soft reset before the timer expires by entering the `clear ip bgp ip-address soft out` command.

#### Note

In Cisco IOS Release 12.0(25)S, 12.3(2)T, and prior releases the update group recalculation delay timer is set to 3 minutes.
Examples

The following sample output from the `debug ip bgp groups` command shows that peering has been established with neighbor 10.4.9.8 and update-group calculations are occurring for this member:

```
Router# debug ip bgp groups
5w4d: BGP-DYN(0): Comparing neighbor 10.4.9.8 flags 0x0 cap 0x0 and updgrp 1 f10
5w4d: BGP-DYN(0): Created update-group(0) flags 0x0 cap 0x0 from neighbor 10.4.0
5w4d: BGP-DYN(0): Adding neighbor 10.4.9.8 flags 0x0 cap 0x0, to update-group 0
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.8 Up
```

The following sample output from the `debug ip bgp groups` command shows the recalculation of update-groups after the `clear ip bgp groups` command was issued:

```
Router# debug ip bgp groups
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.5 Down User reset
5w4d: BGP-DYN(0): Comparing neighbor 10.4.9.5 flags 0x0 cap 0x0 and updgrp 2 f10
5w4d: BGP-DYN(0): Update-group 2 flags 0x0 cap 0x0 policies same as 10.4.9.5 f10
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.8 Down User reset
5w4d: BGP-DYN(0): Comparing neighbor 10.4.9.8 flags 0x0 cap 0x0 and updgrp 2 f10
5w4d: BGP-DYN(0): Update-group 2 flags 0x0 cap 0x0 policies same as 10.4.9.8 f10
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.21 Down User reset
5w4d: BGP-DYN(0): Comparing neighbor 10.4.9.21 flags 0x0 cap 0x0 and updgrp 1 f0
5w4d: BGP-DYN(0): Update-group 1 flags 0x0 cap 0x0 policies same as 10.4.9.21 f0
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.5 Up
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.21 Up
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.8 Up
```

The table below describes the significant fields shown in the display.

**Table 2: debug ip bgp groups Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%BGP-5-ADJCHANGE:</td>
<td>A BGP neighbor has come Up or gone Down. The IP address of the neighbor is</td>
</tr>
<tr>
<td></td>
<td>specified in the output string.</td>
</tr>
<tr>
<td>BGP-DYN(0):</td>
<td>This line is displayed when a neighbor adjacency is established. The BGP</td>
</tr>
<tr>
<td></td>
<td>dynamic update group algorithm analyzes the policies of the new neighbor</td>
</tr>
<tr>
<td></td>
<td>and then adds the neighbor to the appropriate BGP update group.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip bgp</td>
<td>Resets a BGP connection or session.</td>
</tr>
<tr>
<td>clear ip bgp update-group</td>
<td>Clears BGP update-group member sessions.</td>
</tr>
<tr>
<td>show ip bgp replication</td>
<td>Displays BGP update-group replication statistics.</td>
</tr>
<tr>
<td>show ip bgp update-group</td>
<td>Displays information about BGP update-groups.</td>
</tr>
</tbody>
</table>
debug ip bgp igp-metric ignore

To display information related to the system ignoring the Interior Gateway Protocol (IGP) metric during best path selection, use the debug ip bgp igp-metric ignore command in privileged EXEC mode. To disable such debugging output, use the no form of the command.

debug ip bgp igp-metric ignore
no debug ip bgp igp-metric ignore

Syntax Description
This command has no arguments or keywords.

Command Modes
Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.4S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
You might use this command if the path you expected to be chosen as the best path at the shadow RR was not chosen as such. That could be because the bgp bestpath igp-metric ignore command makes the best path algorithm choose the same best path as the primary RR if they are not co-located.

Examples
The following example turns on debugging of events related to the system ignoring the IGP metric during bestpath selection:

Router# debug ip bgp igp-metric ignore

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp bestpath igp-metric ignore</td>
<td>Specifies that the system ignore the Interior Gateway Protocol (IGP) metric during best path selection.</td>
</tr>
</tbody>
</table>
### debug ip bgp import

To display debugging information related to importing IPv4 prefixes from the BGP global routing table into a VRF table or exporting from a VRF table into the BGP global table, use the `debug ip bgp import` command in privileged EXEC mode. To disable the display of such debugging information, use the `no` form of this command.

**Syntax**

```
debug ip bgp import {events | updates} [{access-list|expanded-access-list}]
no debug ip bgp import {events | updates} [{access-list|expanded-access-list}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>events</code></td>
<td>Displays messages related to IPv4 prefix import events.</td>
</tr>
<tr>
<td><code>updates</code></td>
<td>Displays messages related to IPv4 prefix import updates.</td>
</tr>
<tr>
<td><code>access-list</code></td>
<td>(Optional) Number of the access list used to filter debugging messages. The range is from 1 to 199.</td>
</tr>
<tr>
<td><code>expanded-access-list</code></td>
<td>(Optional) Number of the expanded access list used to filter debugging messages. The range is from 1300 to 2699.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(29)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(14)T.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was modified. The output now includes information for the BGP Support for IP Prefix Export from a VRF to the Global Table feature.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was modified. The output now includes information for the BGP Support for IP Prefix Export from a VRF to the Global Table feature.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to display debugging information related to the BGP Support for IP Prefix Import from Global Table into a VRF Table feature or the BGP Support for IP Prefix Export from a VRF Table into Global Table feature. The former feature provides the capability to import IPv4 unicast prefixes from the global routing table into a Virtual Private Network (VPN) routing/forwarding (VRF) instance table using an import route map. The latter feature provides the capability to export IPv4 or IPv6 prefixes from a VRF table into the global table using an export route map.
The following example configures IPv4 prefix import debugging messages for both import events and import updates to be displayed on the console of the router:

```
Router# debug ip bgp import events
BGP import events debugging is on
Router# debug ip bgp import updates
BGP import updates debugging is on for access list 3
00:00:50: %BGP-5-ADJCHANGE: neighbor 10.2.2.2 Up
00:01:06: BGP: reevaluate IPv4 Unicast routes in VRF academic
00:01:06: BGP: 0 routes available (limit: 1000)
00:01:06: BGP: import IPv4 Unicast routes to VRF academic
00:01:06: BGP(2)-VRF(academic): import prefix 100:1:10.30.1.0/24 via 10.2.2.2
00:01:06: BGP: accepted 8 routes (limit: 1000)
00:01:06: BGP: reevaluate IPv4 Multicast routes in VRF multicast
00:01:06: BGP: 0 routes available (limit: 2)
00:01:06: BGP: import IPv4 Multicast routes to VRF multicast
00:01:06: %BGP-4-AFIMPORT: IPv4 Multicast prefixes imported to multicast vrf reached the limit 2
00:01:06: BGP: accepted 2 routes (limit: 2)
00:01:06: BGP: reevaluate IPv4 Unicast routes in VRF BLUE
00:01:06: BGP: 0 routes available (limit: 1000)
00:01:06: BGP: import IPv4 Unicast routes to VRF BLUE
00:01:06: BGP: accepted 3 routes (limit: 1000)
```

The table below describes the significant fields shown in the display.

### Table 3: debug ip bgp import Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP: accepted 2 routes (limit: 2)</td>
<td>Number of routes imported into the VRF, and the default or user-defined prefix import limit.</td>
</tr>
<tr>
<td>BGP: reevaluate IPv4 Unicast routes in VRF BLUE</td>
<td>Prefix was imported during BGP convergence and is being reevaluated for the next scan cycle.</td>
</tr>
<tr>
<td>BGP: 0 routes available (limit: 1000)</td>
<td>Number of routes available from the import source, and the default or user-defined prefix import limit.</td>
</tr>
<tr>
<td>BGP: import IPv4 Unicast routes to VRF BLUE</td>
<td>Import map and prefix type (unicast or multicast) that is being imported into the specified VRF.</td>
</tr>
</tbody>
</table>

The following is a sample debug message for the IP prefix export from a VRF table to global table:

```
Device# debug ip bgp import events
-> global:IPv4 Unicast:base Creating importing net.
  4.4.4.4 (metric 11) from 4.4.4.4 (4.4.4.4)
  Origin IGP, metric 0, localpref 100, valid, internal, best
  Extended Community: RT:1:1
  mpls labels in/out nolabel/16
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip bgp</td>
<td>Resets a BGP connection.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>export map (VRF table to global table)</td>
<td>Exports IP prefixes from a VRF table to the global routing table based on a route map.</td>
</tr>
<tr>
<td>import map</td>
<td>Imports IP prefixes from the global routing table to a VRF table based on a route map.</td>
</tr>
</tbody>
</table>
**debug ip bgp range**

To display debugging information related to Border Gateway Protocol (BGP) dynamic subnet range neighbors, use the `debug ip bgp range` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
default ip bgp range [detail]
no debug ip bgp range
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>detail</strong></td>
<td>(Optional) Specifies that detailed debugging information about BGP dynamic subnet range neighbors will be displayed.</td>
</tr>
</tbody>
</table>

**Command Default**

No debugging information about BGP dynamic subnet range neighbors is displayed.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXH</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)S</td>
<td>This command was integrated into Release 15.0(1)S.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.1S</td>
<td>This command was integrated into Cisco IOS XE Release 3.1S.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output of this command displays information about the identification and creation of BGP dynamic subnet range neighbors. BGP dynamic neighbors are configured using a range of IP addresses and BGP peer groups. After a subnet range is configured for a BGP peer group, and a TCP session is initiated for an IP address in the subnet range, a new BGP neighbor is dynamically created as a member of that group. The new BGP neighbor will inherit any configuration or templates for the group.

**Examples**

The following output shows that the `debug ip bgp range` command has been entered and a BGP neighbor at 192.168.3.2 has been dynamically created using the subnet range 192.168.0.0/16. This new neighbor is a member of the peer group named group192.

```
Router# debug ip bgp range
bgprange_debug = 1, sense = 1
BGP dynamic Range debugging is on
!
*Mar 26 20:05:13.251: BGP:DN: Created a new neighbor *192.168.3.2
in range 192.168.0.0/16, peer-group group192,count = 1
```

The following sample output from the `debug ip bgp range detail` command shows more detailed debugging of the addition of dynamic BGP neighbors:

```
Router# debug ip bgp range detail
bgprange_debug = 1, sense = 1
BGP dynamic Range debugging is on with detail (Dynamic Range neighbors details only)
```
The table below describes the significant field shown in the display.

Table 4: debug ip bgp range Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP:DN:</td>
<td>A potential dynamic BGP neighbor has been identified as opening a TCP session with an IP address in a subnet associated with a BGP peer group. BGP accepts the session and creates a new neighbor. The new neighbor becomes a member of the peer group associated with its subnet range.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp listen</td>
<td>Configures BGP dynamic neighbor parameters.</td>
</tr>
<tr>
<td>clear ip bgp peer-group</td>
<td>Clears BGP peer group member sessions.</td>
</tr>
<tr>
<td>show ip bgp peer-group</td>
<td>Displays information about BGP peer groups.</td>
</tr>
</tbody>
</table>
debug ip bgp sso

To display Border Gateway Protocol (BGP)-related stateful switchover (SSO) events or debugging information for BGP-related interactions between the active Route Processor (RP) and the standby RP, use the debug ip bgp sso command in privileged EXEC mode. To disable debugging output, use the no form of this command.

dep debug ip bgp sso {events | transactions} [detail]  
no debug ip bgp sso {events | transactions} [detail]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>Displays BGP-related SSO failures.</td>
</tr>
<tr>
<td>transactions</td>
<td>Displays debugging information for failed BGP-related interactions between</td>
</tr>
<tr>
<td></td>
<td>the active RP and the standby RP.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed debugging information about successful BGP-</td>
</tr>
<tr>
<td></td>
<td>related SSO operations and successful BGP-related interactions between the</td>
</tr>
<tr>
<td></td>
<td>active and the standby RP.</td>
</tr>
</tbody>
</table>

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(28)SB</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRB1</td>
<td>This command was integrated into Cisco IOS Release</td>
</tr>
<tr>
<td>15.0(1)S</td>
<td>This command was integrated into Cisco IOS Release</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRB1.</td>
</tr>
<tr>
<td></td>
<td>15.0(1)S.</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE 3.1S.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The debug ip bgp sso command is used to display BGP-related SSO events or debugging information for BGP-related interactions between the active RP and the standby RP. This command is useful for monitoring or troubleshooting BGP sessions on a provider edge (PE) router during an RP switchover or during a planned In-Service Software Upgrade (ISSU).

Examples

The following is sample output from the debug ip bgp sso command with the events keyword. The following output indicates that the 10.34.32.154 BGP session is no longer SSO capable.

*Mar 28 02:29:43.526: BGPSSO: 10.34.32.154 reset SSO and decrement count

Tip

Use the show ip bgp vpnv4 all neighbors command to display the reason that the SSO-capable BGP session has been disabled.

The following is sample output from the debug ip bgp sso command with the transactions keyword. The following output shows an SSO notification indicating that the SSO capability is pending for 602 BGP neighbors. This notification is generated as the state between the active and standby RP is being synchronized during the bulk synchronization phase of SSO initialization. During this phase,
the Transmission Control Blocks (TCBs) must be synchronized with the TCBs on the standby RP before SSO initialization is complete.

*Mar 28 02:32:12.102: BGPSSO: tcp sso notify pending for 602 nbrs
**debug ip bgp updates**

To display information about the processing of Border Gateway Protocol (BGP) updates, use the `debug ip bgp updates` command in privileged EXEC mode. To disable the display of BGP update information, use the `no` form of this command.

```
debug ip bgp updates [access-list expanded-access-list] [in|out] [events] [refresh]
no debug ip bgp updates [access-list expanded-access-list] [in|out] [events] [refresh]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list</td>
<td>(Optional) Number of access list used to filter debugging messages. The range that can be specified is from 1 to 199.</td>
</tr>
<tr>
<td>expanded-access-list</td>
<td>(Optional) Number of expanded access lists used to filter debugging messages. The range that can be specified is from 1300 to 2699.</td>
</tr>
<tr>
<td>in</td>
<td>(Optional) Specifies debugging messages for inbound BGP update information.</td>
</tr>
<tr>
<td>out</td>
<td>(Optional) Specifies debugging messages for outbound BGP update information.</td>
</tr>
<tr>
<td>events</td>
<td>(Optional) Specifies debugging messages for BGP update events.</td>
</tr>
<tr>
<td>refresh</td>
<td>(Optional) Specifies debugging messages for BGP update refresh.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(31)SB</td>
<td>This command was modified. The <code>refresh</code> keyword was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip bgp updates` command. The output shows that the BGP session was cleared between neighbor 10.4.9.21 and the local router 10.4.9.4. There are no field description tables for this command because the debugging output from this command depends on the subsequent commands that are entered.

```
Router# debug ip bgp updates
5w2d: %SYS-5-CONFIG_I: Configured from console by console
5w2d: BGP: 10.4.9.21 went from Idle to Active
5w2d: BGP: 10.4.9.21 open active, delay 7032ms
5w2d: BGP: 10.4.9.21 open active, local address 10.4.9.4
5w2d: BGP: 10.4.9.21 went from Active to OpenSent
5w2d: BGP: 10.4.9.21 sending OPEN, version 4, my as: 101
5w2d: BGP: 10.4.9.21 send message type 1, length (incl. header) 45
```
5w2d: BGP: 10.4.9.21 rcv message type 1, length (excl. header) 26
5w2d: BGP: 10.4.9.21 rcv OPEN, version 4
5w2d: BGP: 10.4.9.21 rcv OPEN w/ OPTION parameter len: 16
5w2d: BGP: 10.4.9.21 rcvd OPEN w/ optional parameter type 2 (Capability) len 6
5w2d: BGP: 10.4.9.21 OPEN has CAPABILITY code: 1, length 4
5w2d: BGP: 10.4.9.21 OPEN has MP_EXT CAP for afi/safi: 1/1
5w2d: BGP: 10.4.9.21 rcvd OPEN w/ optional parameter type 2 (Capability) len 2
5w2d: BGP: 10.4.9.21 OPEN has CAPABILITY code: 128, length 0
5w2d: BGP: 10.4.9.21 OPEN has ROUTE-REFRESH capability(old) for all address-fams
5w2d: BGP: 10.4.9.21 rcvd OPEN w/ optional parameter type 2 (Capability) len 2
5w2d: BGP: 10.4.9.21 OPEN has CAPABILITY code: 2, length 0
5w2d: BGP: 10.4.9.21 OPEN has ROUTE-REFRESH capability for all address-families
5w2d: BGP: 10.4.9.21 went from OpenSent to OpenConfirm
5w2d: BGP: 10.4.9.21 went from OpenConfirm to Established
5w2d: %BGP-5-ADJCHANGE: neighbor 10.4.9.21 Up
5w2d: BGP(0): 10.4.9.21 computing updates, afi 0, neighbor version 0, table ver0
5w2d: BGP(0): 10.4.9.21 update run completed, afi 0, ran for 0ms, neighbor vers1
5w2d: BGP(0): 10.4.9.21 initial update completed

The following is sample output from the debug ip bgp updates out command. The output shows that the local router is sending updates with the cost community:

Router# debug ip bgp updates out
*Mar 15 01:41:23.515:BGP(0):10.0.0.5 computing updates, afi 0, neighbor version 0, table version 64, starting at 0.0.0.0
*Mar 15 01:41:23.515:BGP(0):10.0.0.5 send UPDATE (format) 0.0.0.0/0, next 10.0.0.2, metric 0, path , extended community Cost:igp:1:100
*Mar 15 01:41:23.515:BGP(0):10.0.0.5 send UPDATE (format) 10.2.2.0/24, next 10.20.20.10, metric 0, path 10, extended community Cost:igp:8:22
*Mar 15 01:41:23.515:BGP(0):10.0.0.5 send UPDATE (format) 10.13.13.0/24, next 10.0.0.8, metric 0, path

The following is sample output from the debug ip bgp updates in command. The output shows that the local router is receiving updates with the cost community:

Router# debug ip bgp updates in
*Jan 6 01:27:09.111:BGP(2):10.0.0.8 rcvd UPDATE w/ attr:nexthop 10.0.0.8, origin ?, localpref 100, metric 0, path 10, extended community RT:100:1 Cost:igp:10:10 Cost:igp:11:11
debug ip bgp vpnv4 checkpoint

To display the events for the Virtual Routing and Forwarding (VRF) checkpointing system between the active and standby Route Processors, use the debug ip bgp vpnv4 checkpoint command in privileged EXEC mode. To disable the display of these events, use the no form of this command.

debug ip bgp vpnv4 checkpoint
no debug ip bgp vpnv4 checkpoint

Syntax Description
This command has no arguments or keywords.

Command Default
Debugging is not enabled.

Command Modes
Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(25)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

Examples

The following example shows command output on the active Route Processor:

Router# debug ip bgp vpnv4 checkpoint
3d18h: %HA-5-SYNC_NOTICE: Config sync started.
3d18h: vrf-nsf: vrf vpn2 tableid 1 send OK
3d18h: vrf-nsf: vrf tableid bulk sync complete msg send OK
3d18h: vrf-nsf: CF send ok
3d18h: vrf-nsf: CF send ok
3d18h: %HA-5-SYNC_NOTICE: Config sync completed.
3d18h: %HA-5-SYNC_NOTICE: Standby has restarted.
3d18h: %HA-5-MODE: Operating mode is sso, configured mode is sso.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip bgp vpnv4 nsf</td>
<td>Displays the nonstop forwarding events for the VRF table-id synchronization subsystem between the active and standby route processors.</td>
</tr>
</tbody>
</table>
debug ip bgp vpnv4 nsf

To display the nonstop forwarding events for the VRF table-id synchronization subsystem between the active and standby Route Processors, use the debug ip bgp vpnv4 nsf command in privileged EXEC mode. To disable the display of these events, use the no form of this command.

```
debug ip bgp vpnv4 nsf
no debug ip bgp vpnv4 nsf
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Debugging is not enabled.

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(25)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the command output on the active Route Processor:

```
Router# debug ip bgp vpnv4 nsf
MPLS VPN NSF Processing debugging is on
Router(config)# ip vrf vpn3
3d18h: vrf-nsf: vrf vpn3 tableid 2 send rpc OK
Router(config-vrf)# no ip vrf vpn3
% IP addresses from all interfaces in VRF vpn3 have been removed
3d18h: vrf-nsf: rx vrf tableid delete complete msg, tid = 2, name = vpn3
```

The following example shows the command output on the standby Route Processor:

```
Router# debug ip bgp vpnv4 nsf
MPLS VPN NSF Processing debugging is on
00:05:21: vrf-nsf: rx vrf tableid rpc msg, tid = 2, name = vpn3
% IP addresses from all interfaces in VRF vpn3 have been removed
00:06:22: vrf-nsf: vrf vpn3 tableid 2 , delete complete, send OK
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip bgp vpnv4 checkpoint</td>
<td>Display the events for the VRF checkpointing system between the active and standby Route Processors.</td>
</tr>
</tbody>
</table>
**debug ip bgp vpnv4 unicast**

To display debugging messages for Virtual Private Network version 4 (VPNv4) unicast routes, use the `debug ip bgp vpnv4 unicast` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip bgp vpnv4 unicast \{checkpoint | csc | import | keepalives | labelmode | updates\}
no debug ip bgp vpnv4 unicast \{checkpoint | csc | import | keepalives | labelmode | updates\}
```

**Syntax Description**

- **checkpoint**: Displays virtual routing and forwarding (VRF) nonstop forwarding (NSF) checkpoint messages and events.
- **csc**: Displays VRF processing messages for a Carrier Supporting Carrier (CSC) VPN.
- **import**: Displays VRF import processing messages.
- **keepalives**: Displays Border Gateway Protocol (BGP) keepalives.
- **labelmode**: Displays VRF label mode processing.
- **updates**: Displays BGP updates processing for Unicast VPNv4 address family.

**Command Default**

Debugging of VPNv4 unicast routes is not enabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>XE Release 2.2</td>
<td>The <strong>labelmode</strong> keyword was added.</td>
</tr>
<tr>
<td>12.2(33)SRD</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRD.</td>
</tr>
</tbody>
</table>

**Examples**

The following example enables debugging of MPLS VPN label mode processing:

```
Router# debug ip bgp vpnv4 unicast labelmode
MPLS VPN Label mode processing debugging is on
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf % This command is an unreleased and unsupported feature
Router(config)#
*Oct 18 11:35:01.159: vpn: changing the label mode (Enable: per-vrf) for all-vrfs
*Oct 18 11:35:01.459: BGP: VPNv4 Unicast label mode changed
Router(config)#^Z
Router# *Oct 18 11:35:21.995: %SYS-5-CONFIG_I: Configured from console by console
Router# show debug
```

*SYS-5-CONFIG_I: Configured from console by console
Tag VPN:

  MPLS VPN Label mode processing debugging is on

Router#

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip vrf detail</td>
<td>Displays assigned label mode for the VRF.</td>
</tr>
</tbody>
</table>
debug ip bgp vpnv6 unicast

To display debugging messages for Virtual Private Network version 6 (VPNv6) unicast routes, use the **debug ip bgp vpnv6 unicast** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip bgp vpnv6 unicast {csc import keepalives labelmode topology updates}
no debug ip bgp vpnv6 unicast {csc import keepalives labelmode topology updates}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>csc</td>
<td>Displays VPN routing and forwarding (VRF) processing messages for a Carrier Supporting Carrier (CSC) VPN.</td>
</tr>
<tr>
<td>import</td>
<td>Displays VRF import processing messages.</td>
</tr>
<tr>
<td>keepalives</td>
<td>Displays Border Gateway Protocol (BGP) keepalives.</td>
</tr>
<tr>
<td>labelmode</td>
<td>Displays VRF label mode processing.</td>
</tr>
<tr>
<td>topology</td>
<td>Displays the routing topology instance.</td>
</tr>
<tr>
<td>updates</td>
<td>Displays BGP updates processing for the unicast VPNv6 address family.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging of VPNv6 unicast routes is not enabled.

**Command Modes**

- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRD</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example enables debugging of MPLS VPN label mode processing:

```
Router# debug ip bgp vpnv6 unicast labelmode
MPLS VPN Label mode processing debugging is on
Router(config)#
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mpls label mode vrf vpn1 protocol bgp-vpnv6 per-vrf
% Command accepted but obsolete, unreleased or unsupported; see documentation.
Router(config)#

6d03h: vpn: changing the label mode (Enable: per-vrf) for vrf vpn1, address family ipv6
6d03h: vpn: setting pervrfaggr label 18 for vrf vpn1:2001:DB8:1::/96
6d03h: vpn: setting pervrfaggr label 18 for vrf vpn1:2001:DB8:2::1/128
6d03h: vpn: pervrfaggr, withdraw and free local label 19 for vpn1:2001:DB8:CE1::1/128
6d03h: vpn: setting pervrfaggr label 18 for vrf vpn1:2001:DB8:CE1::1/128
6d03h: vpn: label mode change, bnet walk complete.
6d03h: BGP: VPNv6 Unicast label mode changed
Router(config)# end
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vrf detail</td>
<td>Displays assigned label mode for the VRF.</td>
</tr>
</tbody>
</table>
debug ip casa affinities

To display debugging messages for affinities, use the `debug ip casa affinities` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip casa affinities
no debug ip casa affinities
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging for affinities is not enabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip casa affinities` command:

```
Router# debug ip casa affinities
16:15:36: Adding fixed affinity: 10.10.1.1:54787 -> 10.10.10.23 proto = 6
16:15:36: Updating fixed affinity: 10.10.1.1:54787 -> 10.10.10.23 proto = 6
16:15:36: flags = 0x2, appl addr = 10.10.3.2, interest = 0x5/0x100
16:15:36: int ip:port = 10.10.2.2:1638, sequence delta = 0/0/0/0
16:15:36: Adding fixed affinity: 10.10.10.23 -> 10.10.1.1:54787 proto = 6
16:15:36: Updating fixed affinity: 10.10.10.23 -> 10.10.1.1:54787 proto = 6
16:15:36: flags = 0x2, appl addr = 0.0.0.0, interest = 0x3/0x104
16:15:36: int ip:port = 10.10.2.2:1638, sequence delta = 0/0/0/0
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding fixed affinity</td>
<td>Adding a fixed affinity to affinity table.</td>
</tr>
<tr>
<td>Updating fixed affinity</td>
<td>Modifying a fixed affinity table with information from the services manager.</td>
</tr>
<tr>
<td>flags</td>
<td>Bit field indicating actions to be taken on this affinity.</td>
</tr>
<tr>
<td>fwd addr</td>
<td>Address to which packets will be directed.</td>
</tr>
<tr>
<td>interest</td>
<td>Services manager that is interested in packets for this affinity.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>int ip:port</td>
<td>Services manager port to which interest packets are sent.</td>
</tr>
<tr>
<td>sequence delta</td>
<td>Used to adjust TCP sequence numbers for this affinity.</td>
</tr>
</tbody>
</table>
debug ip casa packets

To display debugging messages for packets, use the `debug ip casa packets` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip casa packets
no debug ip casa packets
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging for packets is not enabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip casa packets` command:

```
Router# debug ip casa packets
16:15:36:Routing CASA packet - TO_MGR:
16:15:36: 10.10.1.1:55299 -> 10.10.10.23 proto = 6
16:15:36: Interest Addr:10.10.2.2 Port:1638
16:15:36:Routing CASA packet - FWD_PKT:
16:15:36: 10.10.1.1:55299 -> 10.10.10.23 proto = 6
16:15:36: Fwd Addr:10.10.3.2
16:15:36:Routing CASA packet - TO_MGR:
16:15:36: 10.10.10.23 -> 10.10.1.1:55299 proto = 6
16:15:36: Interest Addr:10.10.2.2 Port:1638
16:15:36:Routing CASA packet - FWD_PKT:
16:15:36: 10.10.10.23 -> 10.10.1.1:55299 proto = 6
16:15:36: Fwd Addr:0.0.0.0
16:15:36:Routing CASA packet - TICKLE:
16:15:36: 10.10.10.23 -> 10.10.1.1:55299 proto = 6
16:15:36: Interest Addr:10.10.2.2 Port:1638 Interest Mask:SYN
16:15:36:Routing CASA packet - FWD_PKT:
16:15:36: 10.10.10.23 -> 10.10.1.1:55299 proto = 6
16:15:36: Fwd Addr:10.10.3.2
```

The table below describes the significant fields shown in the display.

**Table 6: debug ip casa packets Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing CASA packet - TO_MGR</td>
<td>Forwarding Agent is routing a packet to the services manager.</td>
</tr>
<tr>
<td>Routing CASA packet - FWD_PKT</td>
<td>Forwarding Agent is routing a packet to the forwarding address.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Routing CASA packet - TICKLE</td>
<td>Forwarding Agent is signaling services manager while allowing the packet in question to take the appropriate action.</td>
</tr>
<tr>
<td>Interest Addr</td>
<td>Services manager address.</td>
</tr>
<tr>
<td>Interest Port</td>
<td>Port on the services manager where packet is sent.</td>
</tr>
<tr>
<td>Fwd Addr</td>
<td>Address to which packets matching the affinity are sent.</td>
</tr>
<tr>
<td>Interest Mask</td>
<td>Services manager that is interested in packets for this affinity.</td>
</tr>
</tbody>
</table>
**debug ip casa wildcards**

To display debugging messages for wildcards, use the `debug ip casa wildcards` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
default ip casa wildcards
no debug ip casa wildcards
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging for wildcards is not enabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip casa wildcards` command:

```
Router# debug ip casa wildcards
16:13:23: Updating wildcard affinity:
16:13:23: 10.10.10.10 -> 0.0.0.0:0 proto = 6
16:13:23: src mask = 255.255.255.255, dest mask = 0.0.0.0
16:13:23: no frag, not advertising
16:13:23: flags = 0x0, appl addr = 0.0.0.0, interest = 0x8107/0x8104
16:13:23: int ip:port = 10.10.2.2:1638, sequence delta = 0/0/0/0
16:13:23: Updating wildcard affinity:
16:13:23: 0.0.0.0:0 -> 10.10.10.10:0 proto = 6
16:13:23: src mask = 0.0.0.0, dest mask = 255.255.255.255
16:13:23: no frag, advertising
16:13:23: flags = 0x0, appl addr = 0.0.0.0, interest = 0x8107/0x8102
16:13:23: int ip:port = 10.10.2.2:1638, sequence delta = 0/0/0/0
```

The table below describes the significant fields shown in the display.

**Table 7: debug ip casa wildcards Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>src mask</td>
<td>Source of connection.</td>
</tr>
<tr>
<td>dest mask</td>
<td>Destination of connection.</td>
</tr>
<tr>
<td>no frag, not advertising</td>
<td>Not accepting IP fragments.</td>
</tr>
<tr>
<td>flags</td>
<td>Bit field indicating actions to be taken on this affinity.</td>
</tr>
<tr>
<td>fwd addr</td>
<td>Address to which packets matching the affinity will be directed.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>interest</td>
<td>Services manager that is interested in packets for this affinity.</td>
</tr>
<tr>
<td>int ip: port</td>
<td>Services manager port to which interest packets are sent.</td>
</tr>
<tr>
<td>sequence delta</td>
<td>Used to adjust sequence numbers for this affinity.</td>
</tr>
</tbody>
</table>
debug ip cef

To troubleshoot various Cisco Express Forwarding events, use the **debug ip cef** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip cef {drops [rpf [access-list]] [access-list] | receive [access-list] | events [access-list] | interface | dialer}
no debug ip cef {drops [rpf [access-list]] [access-list] | receive [access-list] | events [access-list] | interface | dialer}
```

**Specific to Interprocess Communication (IPC) Records**
```
debug ip cef {ipc | interface-ipc | prefix-ipc [access-list]}
no debug ip cef {ipc | interface-ipc | prefix-ipc [access-list]}
```

**Cisco 10000 Series Routers Only**
```
debug ip cef {drops [rpf [access-list]] [access-list] | receive [access-list] | events [access-list]}
no debug ip cef {drops [rpf [access-list]] [access-list] | receive [access-list] | events [access-list]}
```

**Cisco 10000 Series Routers Only--Specific to IPC Records**
```
debug ip cef ipc
no debug ip cef ipc
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>drops</td>
<td>Records dropped packets.</td>
</tr>
<tr>
<td>rpf</td>
<td>(Optional) Records the result of the Reverse Path Forwarding (RPF) check for packets.</td>
</tr>
<tr>
<td>access-list</td>
<td>(Optional) Limits debugging collection to packets that match the list.</td>
</tr>
<tr>
<td>receive</td>
<td>Records packets that are ultimately destined to the router and packets destined to a tunnel endpoint on the router. If the decapsulated tunnel is IP, the packets are Cisco Express Forwarding switched; otherwise the packets are process switched.</td>
</tr>
<tr>
<td>events</td>
<td>Records general Cisco Express Forwarding events.</td>
</tr>
<tr>
<td>interface</td>
<td>Records IP Cisco Express Forwarding interface events.</td>
</tr>
<tr>
<td>dialer</td>
<td>Records IP Cisco Express Forwarding interface events for dialer interfaces.</td>
</tr>
<tr>
<td>ipc</td>
<td>Records information related to IPC in Cisco Express Forwarding. Possible types of events are the following:</td>
</tr>
<tr>
<td></td>
<td>• IPC messages received out of sequence</td>
</tr>
<tr>
<td></td>
<td>• Status of resequenced messages</td>
</tr>
<tr>
<td></td>
<td>• Status of buffer space for IPC messages</td>
</tr>
<tr>
<td></td>
<td>• Transmission status of IPC messages</td>
</tr>
<tr>
<td></td>
<td>• Throttle requests sent from a line card to the Route Processor</td>
</tr>
</tbody>
</table>
### debug ip cef

**interface-ipc**

Records IPC updates related to interfaces. Possible reporting includes an interface coming up or going down and updates to fibhwidb and fibidb.

**prefix-ipc**

Records updates related to IP prefix information. Possible updates include the following:

- Debugging of IP routing updates in a line card
- Reloading of a line card with a new table
- Updates related to exceeding the maximum number of routes
- Control messages related to Forwarding Information Base (FIB) table prefixes

### Command Default

This command is disabled.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2GS</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.1CC</td>
<td>Support for multiple platforms was added.</td>
</tr>
<tr>
<td>12.0(5)T</td>
<td>The rpf keyword was added.</td>
</tr>
<tr>
<td>12.2(4)T</td>
<td>The dialer keyword was added.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command gathers additional information for the handling of Cisco Express Forwarding interface, IPC, or packet events.

**Note**

For packet events, we recommend that you use an access control list (ACL) to limit the messages recorded.

### Examples

The following is sample output from the `debug ip cef rpf` command for a packet that is dropped when it fails the RPF check. IP address 172.17.249.252 is the source address, and Ethernet 2/0/0 is the input interface.

```
Router# debug ip cef drops rpf
```
IP CEF drops for RPF debugging is on
00:42:02:CEF-Drop:Packet from 172.17.249.252 via Ethernet2/0/0 -- unicast rpf check

The following is sample output for Cisco Express Forwarding packets that are not switched using information from the FIB table but are received and sent to the next switching layer:

Router# debug ip cef receive
IP CEF received packets debugging is on
00:47:52:CEF-receive:Receive packet for 10.1.104.13

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEF-Drop:Packet from 172.17.249.252 via Ethernet2/0/0 -- unicast rpf check</td>
<td>A packet from IP address 172.17.249.252 is dropped because it failed the RPF check.</td>
</tr>
<tr>
<td>CEF-receive:Receive packet for 10.1.104.13</td>
<td>Cisco Express Forwarding has received a packet addressed to the router.</td>
</tr>
</tbody>
</table>

The following is sample output from the `debug ip cef dialer` command for a legacy dialer:

Router# debug ip cef dialer
00:19:50:CEF-Dialer (legacy):add link to 10.10.10.2 via Dialer1 through BR10/0:1
00:19:50:CEF-Dialer:adjacency added:0x81164850
00:19:50:CEF-Dialer:adjacency found:0x81164850; fib->count:1
00:19:50:CEF-Dialer:setup loadinfo with 1 paths

The following is sample output from the `debug ip cef dialer` command for a dialer profile:

Router# debug ip cef dialer
00:31:44:CEF-Dialer (profile dynamic encap (not MLP)):add link to 10.10.10.2 via Dialer1 through Dialer1
00:31:44:CEF-Dialer:adjacency added:0x81164850
00:31:44:CEF-Dialer:adjacency found:0x81164850; fib->count:1

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEF-Dialer (legacy):add link to 10.10.10.2 via Dialer1 through BR10/0:1</td>
<td>A link was added to IP address 10.10.10.2 for legacy Dialer1 through physical interface BR10/0:1.</td>
</tr>
<tr>
<td>CEF-Dialer (profile dynamic encap (not MLP)):add link to 10.10.10.2 via Dialer1 through Dialer1</td>
<td>A link was added to IP address 10.10.10.2 for dialer profile Dialer1 through Dialer1.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip cef</td>
<td>Enables Cisco Express Forwarding on the RPC card.</td>
</tr>
<tr>
<td>show ip cef</td>
<td>Displays entries in the FIB or displays a summary of the FIB.</td>
</tr>
</tbody>
</table>
debug ip cef accounting non-recursive

To troubleshoot Cisco Express Forwarding accounting records, use the `debug ip cef accounting non-recursive` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
d debug ip cef accounting non-recursive
no debug ip cef accounting non-recursive
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
This command is disabled.

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1CC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command records accounting events for nonrecursive prefixes when the `ip cef accounting non-recursive` command is enabled in global configuration mode.

**Examples**
The following is sample output from the `debug ip cef accounting non-recursive` command:

```
Router# debug ip cef accounting non-recursive
03:50:19:CEF-Acct:tmstats_binary:Beginning generation of tmstats ephemeral file (mode binary)
03:50:19:CEF-Acct:snaphosting loadinfo 0x63FF2000
03:50:19:CEF-Acct:snaphosting loadinfo 0x63FF1EA0
03:50:19:CEF-Acct:snaphosting loadinfo 0x63FF17C0
03:50:19:CEF-Acct:snaphosting loadinfo 0x63FF1D40
03:50:19:CEF-Acct:snaphosting loadinfo 0x63FF1A80
03:50:19:CEF-Acct:snaphosting loadinfo 0x63FF0740
03:50:19:CEF-Acct:snaphosting loadinfo 0x63FF08A0
03:50:19:CEF-Acct:snaphosting loadinfo 0x63FF0B60
03:50:19:CEF-Acct:snaphosting loadinfo 0x63FF0CC0
03:50:19:CEF-Acct:snaphosting loadinfo 0x63FF0F80
03:50:19:CEF-Acct:snaphosting loadinfo 0x63FF10E0
03:50:19:CEF-Acct:snaphosting loadinfo 0x63FF1240
03:50:19:CEF-Acct:snaphosting loadinfo 0x63FF13A0
03:50:19:CEF-Acct:snaphosting loadinfo 0x63FF1500
```
The table below describes the significant fields shown in the display.

### Table 10: debug ip cef accounting non-recursive Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tmstats file is being created.</td>
<td>Beginning generation of tmstats ephemeral file (mode binary)</td>
</tr>
<tr>
<td>Baseline counters are being written to the tmstats file for each nonrecursive prefix.</td>
<td>CEF-Acct: tmstats_binary: aggregation complete, duration 0 seconds</td>
</tr>
<tr>
<td>Tmstats file creation is complete.</td>
<td>CEF-Acct: tmstats_binary: writing 45 bytes</td>
</tr>
<tr>
<td>Nonrecursive accounting statistics are being updated to the tmstats file.</td>
<td>CEF-Acct: tmstats_binary: writing 45 bytes</td>
</tr>
<tr>
<td>Update of the tmstats file is complete.</td>
<td>CEF-Acct: tmstats_binary: writing 45 bytes</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip cef</td>
<td>Troubleshoots various Cisco Express Forwarding events.</td>
</tr>
<tr>
<td>ip cef accounting</td>
<td>Enables Cisco Express Forwarding network accounting.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td><code>show ip cef</code></td>
<td>Displays entries or a summary of the FIB table.</td>
</tr>
</tbody>
</table>
**debug ip cef fragmentation**

To report fragmented IP packets when Cisco Express Forwarding is enabled, use the `debug ip cef fragmentation` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command:

```bash
debug ip cef fragmentation
no debug ip cef fragmentation
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

This command is disabled.

**Command Modes**

Privileged EXEC (she)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(14)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(2)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(2)T.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is used to troubleshoot fragmentation problems when Cisco Express Forwarding switching is enabled.

**Examples**

The following is sample output from the `debug ip cef fragmentation` command:

```bash
Router# debug ip cef fragmentation
00:59:45:CEF-FRAG:no_fixup path:network_start 0x5397CF8E datagramstart 0x5397CF80 data_start 0x397CF80 data_block 0x397CF40 mtu 1000 datagramsize 1414 data_bytes 1414
00:59:45:CEF-FRAG:send frag:datagramstart 0x397CF80 datagramsize 442 data_bytes 442
00:59:45:CEF-FRAG:send frag:datagramstart 0x38BC266 datagramsize 1006 data_bytes 1006
00:59:45:CEF-FRAG:no_fixup path:network_start 0x5397C60E datagramstart 0x5397C600 data_start 0x397C600 data_block 0x397C5C0 mtu 1000 datagramsize 1414 data_bytes 1414
00:59:45:CEF-FRAG:send frag:datagramstart 0x397C600 datagramsize 442 data_bytes 442
00:59:45:CEF-FRAG:send frag:datagramstart 0x38BC266 datagramsize 1006 data_bytes 1006
```

The table below describes the significant fields shown in the display.
Table 11: debug ip cef fragmentation Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no_fixup path</td>
<td>A packet is being fragmented in the no_fixup path.</td>
</tr>
<tr>
<td>network_start 0x5397CF8E</td>
<td>Memory address of the IP packet.</td>
</tr>
<tr>
<td>datagramstart 0x5397CF80</td>
<td>Memory address of the encapsulated IP packet.</td>
</tr>
<tr>
<td>data_start 0x397CF80</td>
<td>For particle systems, the memory address where data starts for the first packet particle.</td>
</tr>
<tr>
<td>data_block 0x397C5C0</td>
<td>For particle systems, the memory address of the first packet particle data block.</td>
</tr>
<tr>
<td>mtu 1000</td>
<td>Maximum transmission unit of the output interface.</td>
</tr>
<tr>
<td>datagramsiz 1414</td>
<td>Size of the encapsulated IP packet.</td>
</tr>
<tr>
<td>data_bytes 1414</td>
<td>For particle systems, the sum of the particle data bytes that make up the packet.</td>
</tr>
<tr>
<td>send frag</td>
<td>Fragment is being forwarded.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip cef</td>
<td>Troubleshoots various Cisco Express Forwarding events.</td>
</tr>
</tbody>
</table>
**debug ip cef hash**

To record Cisco Express Forwarding load sharing hash algorithm events, use the `debug ip cef hash` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip cef hash
no debug ip cef hash
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

This command is disabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(12)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(5)T</td>
<td>This command was integrated into Cisco IOS Release 12.1(5)T.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB. This command is not supported on the Cisco 10000 series routers.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA. This command is not supported on the Cisco 7600 router.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command when changing the load sharing algorithm to display the hash table details.

**Examples**

The following is sample output from the `debug ip cef hash` command with IP Cisco Express Forwarding load algorithm tunnel information:

```
Router# debug ip cef hash
01:15:06:%CEF:ip cef load-sharing algorithm tunnel 0
01:15:06:%CEF:Load balancing algorithm:tunnel
01:15:06:%CEF:Load balancing unique id:1F2BA5F6
01:15:06:%CEF:Destroyed load sharing hash table
01:15:06:%CEF:Sending hash algorithm id 2, unique id 1F2BA5F6 to slot 255
```

The following lines show IP Cisco Express Forwarding load algorithm universal information:

```
01:15:28:%CEF:ip cef load-sharing algorithm universal 0
01:15:28:%CEF:Load balancing algorithm:universal
01:15:28:%CEF:Load balancing unique id:062063A4
01:15:28:%CEF:Creating load sharing hash table
01:15:28:%CEF:Hash table columns for valid max_index:
```
The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip cef load-sharing algorithm tunnel 0</td>
<td>Echo of the user command.</td>
</tr>
<tr>
<td>Load balancing algorithm: tunnel</td>
<td>Load sharing algorithm is set to tunnel.</td>
</tr>
<tr>
<td>Load balancing unique id: 1F2BA5F6</td>
<td>ID field in the command is usually 0. In this instance, the router chose a pseudo random ID of 1F2BA5F6.</td>
</tr>
<tr>
<td>Destroyed load sharing hash table</td>
<td>Purge the existing hash table.</td>
</tr>
<tr>
<td>Sending hash algorithm id 2, unique id 1F2BA5F6 to slot 255</td>
<td>Algorithm is being distributed.</td>
</tr>
<tr>
<td>Creating load sharing hash table</td>
<td>Hash table is being created.</td>
</tr>
<tr>
<td>Hash table columns for valid max_index:</td>
<td>Generated hash table.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip cef</td>
<td>Troubleshoots various Cisco Express Forwarding events.</td>
</tr>
<tr>
<td>debug ip cef rrhash</td>
<td>Records Cisco Express Forwarding removal of receive hash events.</td>
</tr>
</tbody>
</table>
debug ip cef rrhash

To record Cisco Express Forwarding removal of receive hash events, use the `debug ip cef rrhash` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip cef rrhash
no debug ip cef rrhash
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

This command is disabled.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB. This command is not supported on the Cisco 10000 series routers.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA. This command is not supported on the Cisco 7600 routers.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to verify the removal of receive hash events when you are shutting down or deleting an interface.

### Examples

The following is sample output from the `debug ip cef rrhash` command:

```
Router# debug ip cef rrhash
00:27:15:CEF:rrhash/check:found 10.1.104.7 on down idb [ok to delete]
00:27:15:CEF:rrhash/check:found 10.1.104.0 on down idb [ok to delete]
00:27:15:CEF:rrhash/check:found 10.1.104.255 on down idb [ok to delete]
00:27:15:CEF:rrhash/check:found 10.1.104.7 on down idb [ok to delete]
00:27:15:CEF:rrhash/check:found 10.1.104.7 on down idb [ok to delete]
00:27:15:CEF:rrhash/check:found 10.1.104.0 on down idb [ok to delete]
00:27:15:CEF:rrhash/check:found 10.1.104.255 on down idb [ok to delete]
00:27:15:CEF:rrhash/check:found 10.1.104.7 on down idb [ok to delete]
```

The table below describes the significant fields shown in the display.
### Table 13: debug ip cef rrhash Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rrhash/check</td>
<td>Verify address is on the receive list.</td>
</tr>
<tr>
<td>found 10.1.104.7 on down idb [ok to delete]</td>
<td>Found a valid address on the receive list for a shutdown interface that can be deleted.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip cef</td>
<td>Troubleshoots various Cisco Express Forwarding events.</td>
</tr>
<tr>
<td>debug ip cef hash</td>
<td>Records Cisco Express Forwarding removal of receive hash events.</td>
</tr>
</tbody>
</table>
debug ip cef subblock

To troubleshoot Cisco Express Forwarding subblock events, use the `debug ip cef subblock` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
depug ip cef subblock [id {all | hw hw-id | sw sw-id}] [xdr {all | control | event | none | statistic}]
no debug ip cef subblock [id {all | hw hw-id | sw sw-id}] [xdr {all | control | event | none | statistic}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>(Optional) Subblock types.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) All subblock types.</td>
</tr>
<tr>
<td>hw hw-id</td>
<td>(Optional) Hardware subblock and identifier.</td>
</tr>
<tr>
<td>sw sw-id</td>
<td>(Optional) Software subblock and identifier.</td>
</tr>
<tr>
<td>xdr</td>
<td>(Optional) External Data Representation (XDR) message types.</td>
</tr>
<tr>
<td>control</td>
<td>(Optional) All XDR message types.</td>
</tr>
<tr>
<td>event</td>
<td>(Optional) Event XDR messages only.</td>
</tr>
<tr>
<td>none</td>
<td>(Optional) No XDR messages.</td>
</tr>
<tr>
<td>statistic</td>
<td>(Optional) Statistic XDR messages.</td>
</tr>
</tbody>
</table>

### Command Default

This command is disabled.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(2)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(2)T.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command is used to record Cisco Express Forwarding subblock messages and events.
The following is sample output from the `debug ip cef subblock` command:

Router# debug ip cef subblock
00:28:12:CEF-SB:Creating unicast RPF subblock for FastEthernet6/0
00:28:12:CEF-SB:Linked unicast RPF subblock to FastEthernet6/0.
00:28:12:CEF-SB:Encoded unit of unicast RPF data (length 16) for FastEthernet6/0
00:28:12:CEF-SB:Sent 1 data unit to slot 6 in 1 XDR message

**Cisco 10000 Series Router Example**

The following is sample output from the `debug ip cef subblock` command:

Router# debug ip cef subblock
00:28:12:CEF-SB:Creating unicast RPF subblock for FastEthernet6/0/0
00:28:12:CEF-SB:Linked unicast RPF subblock to FastEthernet6/0/0.
00:28:12:CEF-SB:Encoded unit of unicast RPF data (length 16) for FastEthernet6/0/0
00:28:12:CEF-SB:Sent 1 data unit to slot 6 in 1 XDR message

The table below describes the significant fields shown in the display.

**Table 14: debug ip cef subblock Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating unicast RPF subblock for FastEthernet6/0/0</td>
<td>Creating a Unicast Reverse Path Forwarding (Unicast RPF) interface descriptor subblock.</td>
</tr>
<tr>
<td>Linked unicast RPF subblock to FastEthernet6/0/0</td>
<td>Linked the subblock to the specified interface.</td>
</tr>
<tr>
<td>Encoded unit of unicast RPF data (length 16) for</td>
<td>Encoded the subblock information in an XDR.</td>
</tr>
<tr>
<td>FastEthernet6/0/0</td>
<td></td>
</tr>
<tr>
<td>Sent 1 data unit to slot 6 in 1 XDR message</td>
<td>Sent the XDR message to a line card through the IPC.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip cef</td>
<td>Troubleshoots various Cisco Express Forwarding events.</td>
</tr>
</tbody>
</table>
To enable the collection of events that affect entries in the Cisco Express Forwarding tables, use the **debug ip cef table** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip cef table
no debug ip cef table
```

### Syntax Description

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list</td>
<td>(Optional) Controls collection of consistency checker parameters from specified lists.</td>
</tr>
<tr>
<td>consistency-checkers</td>
<td>(Optional) Sets consistency checking characteristics.</td>
</tr>
</tbody>
</table>

### Command Default

This command is disabled.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2GS</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.1CC</td>
<td>Support was added for multiple platforms.</td>
</tr>
<tr>
<td>12.0(15)S</td>
<td>The <strong>consistency-checkers</strong> keyword was added.</td>
</tr>
<tr>
<td>12.2(2)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(2)T.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command is used to record Cisco Express Forwarding table events related to the Forwarding Information Base (FIB) table. Possible types of events include the following:

- Routing updates that populate the FIB table
- Flushing of the FIB table
- Adding or removing of entries to the FIB table
- Table reloading process

### Examples

The following is sample output from the **debug ip cef table** command:
Cisco 10000 Series Router Example

The following is sample output from the `debug ip cef table` command:

```plaintext
Router# debug ip cef table
01:25:46:CEF-Table:Event up, 10.1.1.1/32 (rdbs:1, flags:1000000)
01:25:46:CEF-IP:Checking dependencies of 0.0.0.0/0
01:25:47:CEF-Table:attempting to resolve 10.1.1.1/32
01:25:47:CEF-IP:resolved 10.1.1.1/32 via 10.1.104.1 to 10.1.104.1 Ethernet2/0/0
01:26:02:CEF-Table:Event up, default, 0.0.0.0/0 (rdbs:1, flags:400001)
01:26:02:CEF-IP:Prefix exists - no-op change
```

The table below describes the significant fields shown in the display.

**Table 15: debug ip cef table Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEF-Table</td>
<td>Indicates a table event.</td>
</tr>
<tr>
<td>Event up, 10.1.1.1/32</td>
<td>IP prefix 10.1.1.1/32 is being added.</td>
</tr>
<tr>
<td>rdbs:1</td>
<td>Event is from routing descriptor block 1.</td>
</tr>
<tr>
<td>flags:100000</td>
<td>Indicates the network descriptor block flags.</td>
</tr>
<tr>
<td>CEF-IP</td>
<td>Indicates a Cisco Express Forwarding IP event.</td>
</tr>
<tr>
<td>Checking dependencies of 0.0.0.0/0</td>
<td>Resolves the next hop dependencies for 0.0.0.0/0.</td>
</tr>
<tr>
<td>attempting to resolve 10.1.1.1/32</td>
<td>Resolves the next hop dependencies.</td>
</tr>
<tr>
<td>resolved 10.1.1.1/32 via 10.1.104.1 to 10.1.104.1 Ethernet2/0/0</td>
<td>Next hop to IP prefix 10.1.1.1/32 is set and is added to the table.</td>
</tr>
<tr>
<td>Event up, default, 0.0.0.0/0 Prefix exists - no-op change</td>
<td>Indicates no table change is necessary for 0.0.0.0/32.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cef table consistency-check</td>
<td>Enables Cisco Express Forwarding consistency checker table values by type and parameter.</td>
</tr>
<tr>
<td>clear cef table</td>
<td>Clears the Cisco Express Forwarding tables.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>clear ip cef inconsistency</td>
<td>Clears Cisco Express Forwarding inconsistency statistics and records found by the Cisco Express Forwarding consistency checkers.</td>
</tr>
<tr>
<td>debug cef</td>
<td>Enables the display of information about Cisco Express Forwarding events.</td>
</tr>
<tr>
<td>debug ip cef</td>
<td>Troubleshoots various Cisco Express Forwarding events.</td>
</tr>
<tr>
<td>show cef table consistency-check</td>
<td>Displays Cisco Express Forwarding consistency checker table values.</td>
</tr>
<tr>
<td>show ip cef inconsistency</td>
<td>Displays Cisco Express Forwarding IP prefix inconsistencies.</td>
</tr>
</tbody>
</table>
debug ip ddns update

To enable debugging for Dynamic Domain Name System (DDNS) updates, use the `debug ip ddns update` command in privileged EXEC mode. To disable the debugging, use the `no` form of this command.

```
default ip ddns update
no debug ip ddns update
```

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)YA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(14)T.</td>
</tr>
</tbody>
</table>

### Examples

Use the `debug ip ddns update` command to verify that your configurations are working properly. The following sample configurations are shown for demonstration of possible debug output that could display for each configuration.

#### Sample Configuration for the Client to Update A RRs and the Server to Update PTR RRs

The following scenario has a client configured for IETF DDNS updating of address (A) Resource Records (RRs) during which a Dynamic Host Configuration Protocol (DHCP) server is expected to update the pointer (PTR) RR. The DHCP client discovers the domain name system (DNS) server to update using an Start of Authority (SOA) RR lookup since the IP address to the server to update is not specified. The DHCP client is configured to include an fully qualified domain name (FQDN) DHCP option and notifies the DHCP server that it will be updating the A RRs.

```
!DHCP Client Configuration
ip ddns update method testing
ddns
interface Ethernet1
  ip dhcp client update dns
  ip ddns update testing
  ip address dhcp
end
!DHCP Server Configuration
ip dhcp pool test
  network 10.0.0.0 255.0.0.0
  update dns
!Debug Output Enabled
Router>debug ip ddns update
00:14:39: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1 assigned DHCP address 10.0.0.4, mask 255.0.0.0, hostname canada_reserved
00:14:39: DYNDNSUPD: Adding DNS mapping for canada_reserved.hacks <=> 10.0.0.4
00:14:39: DYNDNSUPD: Sleeping for 3 seconds waiting for interface Ethernet1 configuration to settle
```
00:14:42: DHCPC: Server performed PTR update
00:14:42: DDNS: Enqueuing new DDNS update 'canada_reserved.hacks' <=> 10.0.0.4
00:14:42: DDNS: Zone name for 'canada_reserved.hacks' is 'hacks'
00:14:42: DDNS: Dynamic Update 1: (sending to server 10.19.192.32)
00:14:42: DDNS: Zone - hacks
00:14:42: DDNS: Prerequisite: canada_reserved.hacks not in use
00:14:42: DDNS: Update: add canada_reserved.hacks IN A 10.0.0.4
00:14:42: DDNS: Dynamic DNS Update 1 (A) for host canada_reserved.hacks returned 0 (NOERROR)
00:14:42: DDNS: Update of 'canada_reserved.hacks' <=> 10.0.0.4 finished
00:14:42: DYNDNSUPD: Another update completed (total outstanding=0)

Sample Configuration for the Client to Update Both A and DNS RRs and the Server to Update Neither

The following scenario has the client configured for IETF DDNS updating of both A and DNS RRs and requesting that the DHCP server update neither. The DHCP client discovers the DNS server to update using an SOA RR lookup since the IP address to the server to update is not specified. The DHCP client is configured to include an FQDN DHCP option that instructs the DHCP server to not update either A or PTR RRs.

!DHCP Client Configuration
ip dhcp-client update dns server none
ip ddns update method testing
dns both
interface Ethernet1
  ip ddns update testing
  ip address dhcp
end
!DHCP Server Configuration
ip dhcp pool test
  network 10.0.0.0 255.0.0.0
  update dns
!Debug Output Enabled
Router# debug ip ddns update
00:15:33: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1 assigned DHCP address 10.0.0.5, mask 255.0.0.0, hostname canada_reserved
00:15:33: DYNDNSUPD: Adding DNS mapping for canada_reserved.hacks <=> 10.0.0.5
00:15:33: DYNDNSUPD: Sleeping for 3 seconds waiting for interface Ethernet1 configuration to settle
00:15:36: DDNS: Enqueuing new DDNS update 'canada_reserved.hacks' <=> 10.0.0.5
00:15:36: DDNS: Zone name for '10.0.0.11.in-addr.arpa.' is '10.in-addr.arpa'
00:15:36: DDNS: Dynamic Update 1: (sending to server 10.19.192.32)
00:15:36: DDNS: Zone = 10.in-addr.arpa
00:15:36: DDNS: Prerequisite: 10.0.0.11.in-addr.arpa. not in use
00:15:36: DDNS: Update: add 10.0.0.11.in-addr.arpa. IN PTR canada_reserved.hacks
00:15:36: DDNS: Dynamic DNS Update 1 (PTR) for host canada_reserved.hacks returned 0 (NOERROR)
00:15:36: DDNS: Zone name for 'canada_reserved.hacks' is 'hacks'
00:15:36: DDNS: Dynamic Update 1: (sending to server 10.19.192.32)
00:15:36: DDNS: Zone - hacks
00:15:36: DDNS: Prerequisite: canada_reserved.hacks not in use
00:15:36: DDNS: Update: add canada_reserved.hacks IN A 10.0.0.5
00:15:36: DDNS: Dynamic DNS Update 1 (A) for host canada_reserved.hacks returned 0 (NOERROR)
00:15:36: DDNS: Update of 'canada_reserved.hacks' <=> 10.0.0.5 finished
00:15:36: DYNDNSUPD: Another update completed (total outstanding=0)

Sample Configuration for the Client to Update A and DNS RRs and the Server to Update Neither

The following scenario has the client configured for IETF DDNS updating of both A and DNS RRs and requesting that the DHCP server update neither. The DHCP client explicitly specifies the server
to update. The DHCP client is configured to include an FQDN DHCP option that instructs the DHCP server not to update either A or PTR RRs. The configuration is performed using the **ip dhcp client update dns** command. The DHCP server is configured to override the client request and update both A and PTR RR anyway.

```plaintext
!DHCP Client Configuration
ip dhcp client update dns server none
ip ddns update method testing
ddns both
interface Ethernet1
  ip dhcp client update dns server none
  ip ddns update testing
  ip address dhcp
end

!DHCP Server Configuration
ip dhcp pool test	network 10.0.0.0 255.0.0.0
  update dns both override

!Debug Output Enabled on DHCP Client
Router# debug ip ddns update
00:16:30: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1 assigned DHCP address 10.0.0.6, mask 255.0.0.0, hostname canada_reserved
00:16:30: DYNDNSUPD: Adding DNS mapping for canada_reserved.hacks <=> 10.0.0.6
00:16:30: DYNDNSUPD: Sleeping for 3 seconds waiting for interface Ethernet1 configuration to settle
00:16:33: DHCPC: Server performed both updates
```

### Sample Configuration for the Client to Update A and DNS RRs and the Server to Update Neither

The following scenario has the client configured for IETF DDNS updating of both A and DNS RRs and requesting the DHCP server to update neither. The DHCP client is configured to include an FQDN DHCP option which instructs the DHCP server not to update either A or PTR RRs. The DHCP server is configured to allow the client to update whatever RR it chooses.

```plaintext
!DHCP Client Configuration
ip dhcp client update dns server none
ip ddns update method testing
ddns both
interface Ethernet1
  ip dhcp client update dns server none
  ip ddns update testing host 172.19.192.32
  ip address dhcp
end

!DHCP Server Configuration
ip dhcp pool test
  network 10.0.0.0 255.0.0.0
  update dns

!Debug Output Enabled on DHCP Client
Router# debug ip ddns update
00:17:52: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1 assigned DHCP address 10.0.0.7, mask 255.0.0.0, hostname canada_reserved
00:17:52: DYNDNSUPD: Adding DNS mapping for canada_reserved.hacks <=> 10.0.0.6
00:17:55: DDNS: Enqueuing new DDNS update 'canada_reserved.hacks' <=> 10.0.0.7 server 10.19.192.32
00:17:55: DDNS: Enqueuing new DDNS update 'canada_reserved.hacks' <=> 10.0.0.7 server 10.19.192.32
```
Sample Configuration for Updating the Internal Host Table

In the following scenario, the debug output displays the internal host table updates when the default domain name is hacks. The update method named test specifies that the internal Cisco IOS software host table should be updated. Configuring the update method as “test” should be used when the address on the Ethernet interface 0/0 changes. The hostname is configured for the update on this interface.

```
!Cisco IOS Software Configuration
ip domain name hacks
ip ddns update method test
  internal
interface ethernet0/0
  ip ddns update test hostname test2
  ip addr dhcp
*Debug Output Enabled
Router# debug ip ddns update
  "Jun 4 03:11:10.591: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP address"
```
10.0.0.5, mask 255.0.0.0, hostname test2
*Jun 4 03:11:10.591: DYNDNSUPD: Adding DNS mapping for test2.hacks <=> 10.0.0.5
*Jun 4 03:11:10.591: DYNDNSUPD: Adding internal mapping test2.hacks <=> 10.0.0.5

Using the **show hosts** command displays the newly added host table entry.

```
Router# show hosts
Default domain is hacks
Name/address lookup uses domain service
Name servers are 255.255.255.255
Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
temp - temporary, perm - permanent
NA - Not Applicable None - Not defined
HOST PORT FLAGS AGE TYPE ADDRESS(ES)
test2.hacks None (perm, OK) 0 IP 10.0.0.5
```

Shutting down the interface removes the host table entry.

```
interface ethernet0/0
shutdown
```

*Jun 4 03:14:02.107: DYNDNSUPD: Removing DNS mapping for test2.hacks <=> 10.0.0.5
*Jun 4 03:14:02.107: DYNDNSUPD: Removing mapping test2.hacks <=> 10.0.0.5

Using the **show hosts** command confirms that the entry has been removed.

```
Router# show hosts
Default domain is hacks
Name/address lookup uses domain service
Name servers are 255.255.255.255
Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
temp - temporary, perm - permanent
NA - Not Applicable None - Not defined
HOST PORT FLAGS AGE TYPE ADDRESS(ES)
```

Sample Configuration of HTTP DDNS Updates

In the following scenario, the debug output shows the HTTP-style DDNS updates. The sample configuration defines a new IP DDNS update method named dyndns that configures a URL to use when adding or changing an address. No URL has been defined for use when removing an address since DynDNS.org does not use such a URL for free accounts. A maximum update interval of 28 days has been configured, which specifies that updates should be sent at least every 28 days. Configuring the new “dyndns” update method should be used for Ethernet interface 1.

```
!DHCP Client Configuration
ip ddns update method dyndns
http
    add http://test:test@<s>/nic/update?system=dyndns&hostname=<h>&myip=<a>
        interval max 28 0 0 0
interface ethernet1
ip ddns update hostname test.dyndns.org
ip ddns update dyndns host members.dyndns.org
ip addr dhcp
!Debugging Enabled
```

```
Router# debug ip ddns update
00:04:35: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1 assigned DHCP address 10.32.254.187, mask 255.255.255.240, hostname test.dyndns.org
00:04:35: DYNDNSUPD: Adding DNS mapping for test.dyndns.org <=> 10.32.254.187 server 63.208.196.94
00:04:35: DYNDNSUPD: Sleeping for 3 seconds waiting for interface Ethernet1 configuration
```
to settle
00:04:38: HTTPDNS: Update add called for test.dyndns.org <=> 10.32.254.187
00:04:38: HTTPDNS: Update called for test.dyndns.org <=> 10.32.254.187
00:04:38: HTTPDNS: init
00:04:38: HTTPDNSUPD: Session ID = 0x7
00:04:38: HTTPDNSUPD: URL = 'http://test:test@63.208.196.94/nic/update?system=dyndns&hostname=test.dyndns.org&myip=10.32.254.187'
00:04:38: HTTPDNSUPD: Sending request
00:04:40: HTTPDNSUPD: Response for update test.dyndns.org <=> 10.32.254.187
00:04:40: HTTPDNSUPD: DATA START
good 10.32.254.187
00:04:40: HTTPDNSUPD: DATA END, Status is Response data received, successfully
00:04:40: HTTPDNSUPD: Call returned SUCCESS for update test.dyndns.org <=> 10.32.254.187
00:04:40: HTTPDNSUPD: Freeing response
00:04:40: DYNDNSUPD: Another update completed (outstanding=0, total=0)
00:04:40: HTTPDNSUPD: Clearing all session 7 info
128 days later, the automatic update happens.
00:05:39: DYNDNSUPD: Adding DNS mapping for test.dyndns.org <=> 10.32.254.187 server 63.208.196.94
00:05:39: HTTPDNS: Update add called for test.dyndns.org <=> 10.32.254.187
00:05:39: HTTPDNS: Update called for test.dyndns.org <=> 10.32.254.187
00:05:39: HTTPDNS: init
00:05:39: HTTPDNSUPD: Session ID = 0x8
00:05:39: HTTPDNSUPD: URL = 'http://test:test@63.208.196.94/nic/update?system=dyndns&hostname=test.dyndns.org&myip=10.32.254.187'
00:05:39: HTTPDNSUPD: Sending request
00:05:39: HTTPDNSUPD: Response for update test.dyndns.org <=> 10.32.254.187
00:05:39: HTTPDNSUPD: DATA START
nochg 10.32.254.187
00:05:39: HTTPDNSUPD: DATA END, Status is Response data received, successfully
00:05:39: HTTPDNSUPD: Call returned SUCCESS for update test.dyndns.org <=> 10.32.254.187
00:05:39: HTTPDNSUPD: Freeing response
00:05:39: DYNDNSUPD: Another update completed (outstanding=0, total=0)
00:05:39: HTTPDNSUPD: Clearing all session 8 info

The table below describes the significant fields shown in the output.

Table 16: debug ip ddns update Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPDNSUPD</td>
<td>Reflects the method of update. In this case, the update method is HTTP.</td>
</tr>
<tr>
<td>HTTPDNSUPD: URL =</td>
<td>URL that is used to update the DNS.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug dhcp</td>
<td>Displays debugging information about the DHCP client and monitors the status of DHCP packets.</td>
</tr>
<tr>
<td>debug ip dhcp server</td>
<td>Enables DHCP server debugging.</td>
</tr>
<tr>
<td>host (host-list)</td>
<td>Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.</td>
</tr>
<tr>
<td>ip ddns update hostname</td>
<td>Enables a host to be used for DDNS updates of A and PTR RRs.</td>
</tr>
<tr>
<td>ip ddns update method</td>
<td>Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ip dhcp client update dns</td>
<td>Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.</td>
</tr>
<tr>
<td>ip dhcp-client update dns</td>
<td>Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.</td>
</tr>
<tr>
<td>ip dhcp update dns</td>
<td>Enables DDNS updates of A and PTR RRs for most address pools.</td>
</tr>
<tr>
<td>ip host-list</td>
<td>Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.</td>
</tr>
<tr>
<td>show ip ddns update</td>
<td>Displays information about the DDNS updates.</td>
</tr>
<tr>
<td>show ip ddns update method</td>
<td>Displays information about the DDNS update method.</td>
</tr>
<tr>
<td>show ip dhcp server pool</td>
<td>Displays DHCP server pool statistics.</td>
</tr>
<tr>
<td>show ip host-list</td>
<td>Displays the assigned hosts in a list.</td>
</tr>
<tr>
<td>update dns</td>
<td>Dynamically updates a DNS with A and PTR RRs for some address pools.</td>
</tr>
</tbody>
</table>
**debug ip dfp agent**

To display debugging messages for the Dynamic Feedback Protocol (DFP) agent subsystem, use the `debug ip dfp` command in user EXEC or privileged EXEC mode. To stop debugging output, use the `no` form of this command.

```
debug ip dfp agent
no debug ip dfp agent
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

User EXEC or privileged EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(8a)E</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXD.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays debugging messages for the DFP agent subsystem.

See the following caution before using debug commands:

⚠️ **Caution**

Because debugging output is assigned a high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network flows and fewer users. Debugging during these periods reduces the effect these commands have on other users on the system.

**Examples**

The following example configures a DFP agent debugging session:

```
Router# debug ip dfp agent
DFP debugging is on
```

The following example stops all debugging:

```
Router# no debug all
All possible debugging has been turned off
```
**debug ip dhcp server**

To enable Cisco IOS Dynamic Host Configuration Protocol (DHCP) server debugging, use the `debug ip dhcp server` command in privileged EXEC mode. To disable DHCP server debugging, use the `no` form of this command.

```plaintext
debug ip dhcp server {events | packets | linkage | class}
no debug ip dhcp server {events | packets | linkage | class}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>Reports server events, such as address assignments and database updates.</td>
</tr>
<tr>
<td>packets</td>
<td>Decodes DHCP receptions and transmissions.</td>
</tr>
<tr>
<td>linkage</td>
<td>Displays database linkage information, such as parent-child relationships in a radix tree.</td>
</tr>
<tr>
<td>class</td>
<td>Displays DHCP class-based information.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(13)ZH</td>
<td>The <strong>class</strong> keyword was added.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>The <strong>class</strong> keyword was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.3(11)T</td>
<td>The output was enhanced to show the static mappings.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows a combination of DHCP server events and decoded receptions and transmissions:

```plaintext
Router# debug ip dhcp server events
Router# debug ip dhcp server packets
```

DHCPD:DHCPDISCOVER received from client 0b07.1134.a029 through relay 10.1.0.253.
DHCPD:assigned IP address 10.1.0.3 to client 0b07.1134.a029.
DHCPD:Sending DHCPOFFER to client 0b07.1134.a029 (10.1.0.3).
DHCPD:unicasting BOOTREPLY for client 0b07.1134.a029 to relay 10.1.0.253.
DHCPD:DHCPREQUEST received from client 0b07.1134.a029.
DHCPD:Sending DHCPACK to client 0b07.1134.a029 (10.1.0.3).
DHCPD:unicasting BOOTREPLY for client 0b07.1134.a029 to relay 10.1.0.253.
DHCPD:checking for expired leases.

The following example shows database linkage information:

```plaintext
Router# debug ip dhcp server linkage
```
DHCPD: child pool: 10.1.0.0 / 255.255.0.0 (subnet10.1)
DHCPD: parent pool: 10.0.0.0 / 255.0.0.0 (net10)
DHCPD: child pool: 10.0.0.0 / 255.0.0.0 (net10)
DHCPD: pool (net10) has no parent.
DHCPD: child pool: 10.1.0.0 / 255.255.0.0 (subnet10.1)
DHCPD: parent pool: 10.0.0.0 / 255.0.0.0 (net10)
DHCPD: child pool: 10.0.0.0 / 255.0.0.0 (net10)
DHCPD: pool (net10) has no parent.

The following example shows when a DHCP class is removed:

Router# debug ip dhcp server class
DHCPD: deleting class CLASS1

The following example shows the debug output when the configured pattern does not match:

Router# debug ip dhcp server class
DHCPD: searching for a match to 'relay-information 0106000 400020202020800060009e80b8800' in class CLASS1
DHCPD: searching for a match to 'relay-information 0106000400020202020800060009e80b8800' in class CLASS1
DHCPD: searching for a match to 'relay-information 0106000'

The following example shows the debug output when you unconfigure a DHCP pattern in a DHCP class and then configure the pattern in the DHCP class:

Router# debug ip dhcp server class
DHCPD: pattern 'relay-information 123456' removed from class CLASS1
DHCPD: added pattern 'relay-information 0106000400020202020800060009e80b8800' for class CLASS1

The following example shows the debug output when the configured pattern does match:

Router# debug ip dhcp server class
DHCPD: searching for a match to 'relay-information 0106000 400020202020800060009e80b8800' in class CLASS1
DHCPD: input pattern 'relay-information 010600040002020202 0800060009e80b8800' matches class CLASS1
DHCPD: input matches class CLASS1

The following example shows the debug output when static mappings are configured:

Router# debug ip dhcp server
Loading abc/static_pool from 10.19.192.33 (via Ethernet0): !
[OK - 333 bytes]
*May 26 23:14:21.707: DHCPD: parsing text line "IP address Type Hardware address Lease expiration.
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug dhcp</td>
<td>Displays debugging information about the DHCP client and monitors the status of DHCP packets.</td>
</tr>
<tr>
<td>debug ip ddns update</td>
<td>Enables debugging for DDNS updates.</td>
</tr>
<tr>
<td>host (host-list)</td>
<td>Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.</td>
</tr>
<tr>
<td>ip ddns update hostname</td>
<td>Enables a host to be used for DDNS updates of A and PTR RRs.</td>
</tr>
<tr>
<td>ip ddns update method</td>
<td>Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.</td>
</tr>
<tr>
<td>ip dhcp client update dns</td>
<td>Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client on an interface.</td>
</tr>
<tr>
<td>ip dhcp-client update dns</td>
<td>Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.</td>
</tr>
<tr>
<td>ip dhcp update dns</td>
<td>Enables DDNS updates of A and PTR RRs for most address pools.</td>
</tr>
<tr>
<td>ip host-list</td>
<td>Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.</td>
</tr>
<tr>
<td>show ip ddns update</td>
<td>Displays information about the DDNS updates.</td>
</tr>
<tr>
<td>show ip ddns update method</td>
<td>Displays information about the DDNS update method.</td>
</tr>
<tr>
<td>show ip dhcp server pool</td>
<td>Displays DHCP server pool statistics.</td>
</tr>
<tr>
<td>show ip host-list</td>
<td>Displays the assigned hosts in a list.</td>
</tr>
<tr>
<td>update dns</td>
<td>Dynamically updates a DNS with A and PTR RRs for some address pools.</td>
</tr>
</tbody>
</table>
debug ip dhcp server redundancy

To display debugging information about DHCP server and relay agent redundancy events, use the `debug ip dhcp server redundancy` command in privileged EXEC mode. To disable the display of debugging output, use the `no` form of this command.

```
debug ip dhcp server redundancy
no debug ip dhcp server redundancy
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging output is disabled for DHCP server and relay agent redundancy events.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(31)SB2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command with caution. Many bindings being synchronized between the active and standby Route Processor (RP) can trigger a large amount of debugging output.

**Examples**

The following example displays debug messages regarding DHCP server and relay agent redundancy events. The last line (and only that line) is output when the `debug ip dhcp server redundancy` command is enabled. The line indicates that a binding update message has been sent to the standby for the IP address 10.0.0.2 in the pool named “test.”

```
Router# debug ip dhcp server redundancy
*Mar 22 10:32:21: DHCPD: assigned IP address 10.0.0.2 to client 0063.6973.636f.2d30.3030.342e.3465.6130.2e30.3831.632d.4661.312f.302e.31.
*Mar 22 10:32:21: DHCPD: lease time = 3600
*Mar 22 10:32:21: DHCPD: dhcpd_lookup_route: host = 10.0.0.2
*Mar 22 10:32:21: DHCPD: dhcpd_create_and_hash_route: host = 10.0.0.2
*Mar 22 10:32:21: DHCPD: dhcpd_create_and_hash_route index = 0
*Mar 22 10:32:21: DHCPD: dynamic sync completed for 10.0.0.2 in pool test
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug dhcp redundancy</code></td>
<td>Displays debugging information about DHCP proxy client redundancy events.</td>
</tr>
</tbody>
</table>
debug ip dhcp server snmp

To enable DHCP server Simple Network Management Protocol (SNMP) debugging, use the `debug ip dhcp server snmp` command in privileged EXEC mode. To disable DHCP server SNMP debugging, use the `no` form of this command.

```
debug ip dhcp server snmp
```

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRC</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to enable debugging and display DHCP server SNMP debugging events:

```
Router# debug ip dhcp server snmp

00:18:01: DHCDFD SNMP: pool 'pool1' 'high' utilization trap is ignored
00:18:18: DHCDFD SNMP: pool 'pool1' 'low' utilization trap is ignored
00:20:46: DHCDFD SNMP: subnet 4.1.1.0 'high' utilization trap is ignored
00:21:03: DHCDFD SNMP: subnet 4.1.1.0 'low' utilization trap is ignored
00:18:01: DHCDFD SNMP: subnet trap is not enabled
00:37:32: DHCDFD SNMP: pool trap is not enabled
00:37:57: DHCDFD SNMP: interface trap is not enabled
00:27:27: DHCDFD SNMP: duplicate trap is not enabled
```
### debug ip dns name-list

To enable debugging output for Domain Name System (DNS) name list events, use the `debug ip dns name-list` command in privileged EXEC mode. To disable debugging output for DNS name list events, use the `no` form of this command.

```plaintext
debug ip dns name-list
no debug ip dns name-list
```

#### Syntax Description
This command has no arguments or keywords.

#### Command Default
Debugging output is disabled for DNS name lists.

#### Command Modes
Privileged EXEC (#)

#### Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines
This command enables the writing of DNS name list event messages to system message logging (syslog) output. A DNS name list event can be either of the following:

- The addition or removal of a DNS name list entry (a hostname pattern and action to perform on an incoming DNS query for a hostname that matches the pattern). To add or remove a DNS name list entry, use the `ip dns name-list` command.
- The removal of a DNS name list.

**Note**
The addition of a DNS name list is reported as an addition of a name list entry.

To display which debugging options are enabled (DNS name list, DNS view, or DNS view list), use the `show debugging` command. To display the syslog history statistics and buffer contents, use the `show logging` command. To display a particular DNS name list or all configured name lists, use the `show ip dns name-list` command.

#### Examples
The following sample output from the `debug ip dns name-list` command shows the hostname pattern www.example.com being added to DNS name list 1 as a permit clause. Next, the hostname patterns www.example1.com and www.example2.com are added to DNS name list 2 as deny clauses and permit clauses, respectively. Finally, the hostname pattern www.example1.com is removed from DNS name list 2.

```plaintext
Router# debug ip dns name-list
DNS Name-list debugging is on
.
.
```
Router# show debugging

DNS Name-list debugging is on

Router# show logging

*May 16 14:54:44.326: DNS_NAMELIST: adding permit 'WWW.EXAMPLE' to name-list 1
*May 16 14:54:44.910: DNS_NAMELIST: adding deny 'WWW.EXAMPLE1.COM' to name-list 2
*May 16 14:54:45.202: DNS_NAMELIST: adding permit 'WWW.EXAMPLE2.COM' to name-list 2
*May 16 19:32:20.881: DNS_NAMELIST: removing 'WWW.EXAMPLE1.COM' from name-list 2

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dns name-list</td>
<td>Defines a list of pattern-matching rules in which each rule permits or denies the use of a DNS view list member to handle a DNS query based on whether the query hostname matches the specified regular expression.</td>
</tr>
<tr>
<td>show debugging</td>
<td>Displays the state of each debugging option.</td>
</tr>
<tr>
<td>show ip dns name-list</td>
<td>Displays a particular DNS name list or all configured name lists.</td>
</tr>
<tr>
<td>show logging</td>
<td>Displays the contents of logging buffers.</td>
</tr>
</tbody>
</table>
**debug ip dns view**

To enable debugging output for Domain Name System (DNS) view events, use the `debug ip dns view` command in privileged EXEC mode. To disable debugging output for a DNS view, use the `no` form of this command.

```
debug ip dns view
no debug ip dns view
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Debugging output is disabled for DNS views.

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command enables the writing of DNS view event messages to system message logging (syslog) output. A DNS view event can be any of the following:

- The addition or removal of a DNS view definition.
- The addition or removal of a DNS forwarding name server setting for a DNS view.
- The addition or removal of a DNS resolver setting for a DNS view.
- The enabling or disabling of logging of a syslog message each time a DNS view is used.

To display which debugging options are enabled (DNS name list, DNS view, or DNS view list), use the `show debugging` command. To show the syslog history statistics and buffer contents, use the `show logging` command.

**Examples**
The following sample output from the `debug ip dns view` command shows the default DNS view being configured:

```
Router# debug ip dns view

DNS View debugging is on
.
.
Router# show debugging

DNS View debugging is on
.
.
Router# show logging

.
.
```
DNS_VIEW: creating view view1
DNS_VIEW: Clearing logging in view default
DNS_VIEW: Setting domain lookup in view default
DNS_VIEW: Setting domain name to cisco.com in view default
DNS_VIEW: Setting domain list example1.com in view default
DNS_VIEW: Setting domain list example1.com example2.com in view default
DNS_VIEW: Setting domain list example1.com example2.com example3.com in view default
DNS_VIEW: Setting domain multicast to 192.0.2.10 in view default
DNS_VIEW: Setting domain lookup in view default
DNS_VIEW: Setting domain timeout to 7 in view default
DNS_VIEW: Setting domain retry to 7 in view default
DNS_VIEW: Setting domain name-server 192.0.2.204 192.0.2.205 in view default
DNS_VIEW: Setting domain name-server 192.0.2.204 192.0.2.205 192.0.2.206 in view default
DNS_VIEW: Setting domain name-server interface FastEthernet0/1 in view default
DNS_VIEW: Setting domain round-robin to 4 in view default
DNS_VIEW: Setting dns forwarding in view default
DNS_VIEW: Setting dns forwarder 192.0.2.11 in view default
DNS_VIEW: Setting dns forwarder 192.0.2.11 192.0.2.12 in view default
DNS_VIEW: Setting dns forwarder 192.0.2.11 192.0.2.12 192.0.2.13 in view default

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dns view</td>
<td>Enters DNS view configuration mode for the specified DNS view so that the logging setting, forwarding parameters, and resolving parameters can be configured for the view.</td>
</tr>
<tr>
<td>show debugging</td>
<td>Displays the state of each debugging option.</td>
</tr>
<tr>
<td>show logging</td>
<td>Displays the contents of logging buffers.</td>
</tr>
</tbody>
</table>
To enable debugging output for Domain Name System (DNS) view list events, use the **debug ip dns view-list** command in privileged EXEC mode. To disable debugging output for a DNS view list, use the **no** form of this command.

```bash
debug ip dns view-list
no debug ip dns view-list
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging output is disabled for DNS view lists.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command enables the writing of DNS view list event messages to system message logging (syslog) output. A DNS view list event can be any of the following:

- The addition or removal of a DNS view list definition. To add or remove a DNS view list definition, use the **ip dns view-list** command.

- The addition or removal of a DNS view list member (a DNS view and the relative order in which it is to be checked in the view list) to or from a DNS view list. To add or remove a DNS view list member, use the **view** command.

- The setting or clearing of a DNS view list assignment as the default view list (using the **ip dns server view-group** command) or to an interface (using the **ip dns view-group** command).

To show which debugging options are enabled (DNS name list, DNS view, or DNS view list), use the **show debugging** command. To show the syslog history statistics and buffer contents, use the **show logging** command.

**Examples**

The following sample output from the **debug ip dns view-list** command shows the addition of the DNS view list definition named userlist5. Next, five DNS views are added as members of the DNS view list.

```bash
Router# debug ip dns view-list
DNS View-list debugging is on
.
.
Router# show debugging
DNS View-list debugging is on
.
.
```
Router# show logging

*May 16 23:31:17.711: DNS_VIEWLIST: adding member user1 vrf vpn101 order 10 to view-list userlist5
*May 16 23:31:18.583: DNS_VIEWLIST: adding member user2 vrf vpn102 order 20 to view-list userlist5
*May 16 23:31:19.851: DNS_VIEWLIST: adding member user3 vrf vpn103 order 30 to view-list userlist5
*May 16 23:31:21.007: DNS_VIEWLIST: adding member user4 vrf vpn204 order 45 to view-list userlist5
*May 16 23:31:22.199: DNS_VIEWLIST: adding member default order 60 to view-list userlist5

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dns server view-group</td>
<td>Specifies the DNS view list to use to determine which DNS view to use to handle incoming queries that arrive on an interface not configured with a DNS view list.</td>
</tr>
<tr>
<td>ip dns view-group</td>
<td>Specifies the DNS view list to use to determine which DNS view to use to handle incoming DNS queries that arrive on a specific interface.</td>
</tr>
<tr>
<td>ip dns view-list</td>
<td>Enters DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS views.</td>
</tr>
<tr>
<td>show debugging</td>
<td>Displays the state of each debugging option.</td>
</tr>
<tr>
<td>show logging</td>
<td>Displays the contents of logging buffers.</td>
</tr>
<tr>
<td>view</td>
<td>Enters DNS view list member configuration mode so that usage restrictions can be configured for the view list member.</td>
</tr>
</tbody>
</table>
**debug ip domain**

To enable Domain Name System (DNS) debugging and view DNS debugging information, use the `debug ip domain` command in privileged EXEC mode. To disable DNS debugging, use the `no` form of this command.

```
debug ip domain
no debug ip domain
```

**Syntax Description**

This command has no arguments or keywords.

**Note**

Use the `debug ip domain` command form to enable DNS debugging and view basic DNS debugging information. To view more DNS debugging options such as DNS server response debugging and so on, use the question mark (?) online help function.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.13S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.4(3)S</td>
<td>This command was integrated into Cisco IOS Release 15.4(3)S.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip domain` command:

```
Device> enable
Device# debug ip domain

Domain Name System debugging is on
Device#
*Jul 18 09:16:19.546: DNS: Incoming UDP query (id#8168)
*Jul 18 09:16:19.547: DNS: Type 1 DNS query (id#8168) for host 'abc.google.com' from 209.165.200.230(27106)
*Jul 18 09:16:19.547: DNS: Servicing request using view default
*Jul 18 09:16:19.547: search_nametype_index: abc.google.com
*Jul 18 09:16:19.547: search_nametype_index: found abc.google.com for abc.google.com
*Jul 18 09:16:19.547: search_nametype_index: abc.google.com
*Jul 18 09:16:19.547: search_nametype_index: found abc.google.com for abc.google.com
*Jul 18 09:16:19.547: search_nametype_index: google.com
*Jul 18 09:16:19.547: search_nametype_index: com
*Jul 18 09:16:19.547: search_nametype_index: abc.google.com
*Jul 18 09:16:19.547: search_nametype_index: found abc.google.com for abc.google.com
*Jul 18 09:16:19.547: DNS: Reply to client 209.165.200.230/27106 query A
*Jul 18 09:16:19.547: DNS: Finished processing query (id#8168) in 0.001 secs
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>debug ip domain replies</strong></td>
<td>Enables DNS server response debugging and displays debugging information for DNS server responses to clients.</td>
</tr>
<tr>
<td>ip dns server</td>
<td>Enables the DNS server on a device.</td>
</tr>
<tr>
<td>ip dns server view-group</td>
<td>Specifies the default DNS server view list for a device.</td>
</tr>
</tbody>
</table>
debug ip domain replies

To enable debugging for Domain Name System (DNS) server responses to clients and view debugging information for DNS server responses to clients, use the `debug ip domain replies` command in privileged EXEC mode. To disable DNS server response debugging, use the `no` form of this command.

```
detail

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Privileged EXEC (#)</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.13S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.4(3)S</td>
<td>This command was integrated into Cisco IOS Release 15.4(3)S.</td>
</tr>
</tbody>
</table>

Examples

The following is sample output from the `debug ip domain replies` command:

```
Device> enable
Device# debug ip domain replies

Domain Name System Reply debugging is on

*Jul 18 09:17:22.868: DNS: Finished processing query (id#34422) in 0.000 secs
*Jul 18 09:17:23.663: DNS: Finished processing query (id#51171) in 0.000 secs
*Jul 18 09:17:23.665: DNS: Finished processing query (id#46198) in 0.000 secs
```

Examples

Sample Output for Detailed DNS Response Debugging

```
Device> enable
Device# debug ip domain replies detail

Domain Name System Reply debugging is on (detailed)

*Jul 18 09:17:58.635: DNS: Send reply from internal information:
*Jul 18 09:17:58.635: DOM: id=47025, response, opcode=0, aa=0, tc=0, rd=1, ra=1
*Jul 18 09:17:58.635: rcode=0, qdcount=1, ancount=1, nscount=0, arcount=0
*Jul 18 09:17:58.635: query name is abc.google.com, qtype=1, class=1
*Jul 18 09:17:58.635: Answer section:
*Jul 18 09:17:58.635: Name='abc.google.com'
*Jul 18 09:17:58.635: RR type=1, class=1, ttl=10, data length=4
*Jul 18 09:17:58.635: Authority section:
*Jul 18 09:17:58.635: Additional record section:
*Jul 18 09:17:58.635: DNS: Finished processing query (id#47025) in 0.001 secs
```
July 18 09:17:58.637: DNS: Send reply from internal information:
July 18 09:17:58.637: DOM: id=25881, response, opcode=0, aa=0, tc=0, rd=1, ra=1
July 18 09:17:58.637: rcode=0, qdcount=1, ancount=1, nscount=0, arcount=0
July 18 09:17:58.637: query name is abc.google.com, qtype=1, class=1
July 18 09:17:58.637: Answer section:
July 18 09:17:58.637: Name='abc.google.com'
July 18 09:17:58.637: RR type=1, class=1, ttl=10, data length=4
July 18 09:17:58.637: Authority section:
July 18 09:17:58.637: Additional record section:
July 18 09:17:58.637: DNS: Finished processing query (id#25881) in 0.001 secs

July 18 09:17:58.638: DNS: Send reply from internal information:
July 18 09:17:58.638: DOM: id=41387, response, opcode=0, aa=0, tc=0, rd=1, ra=1
July 18 09:17:58.638: rcode=0, qdcount=1, ancount=1, nscount=0, arcount=0
July 18 09:17:58.638: query name is abc.google.com, qtype=1, class=1
July 18 09:17:58.638: Answer section:
July 18 09:17:58.638: Name='abc.google.com'
July 18 09:17:58.638: RR type=1, class=1, ttl=10, data length=4
July 18 09:17:58.638: Authority section:
July 18 09:17:58.638: Additional record section:
July 18 09:17:58.638: DNS: Finished processing query (id#41387) in 0.000 secs

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip domain</td>
<td>Enables DNS debugging and displays DNS debugging information.</td>
</tr>
<tr>
<td>ip dns server</td>
<td>Enables the DNS server on a device.</td>
</tr>
<tr>
<td>ip dns server view-group</td>
<td>Specifies the default DNS server view list for a device.</td>
</tr>
</tbody>
</table>
debug ip drp

To display Director Response Protocol (DRP) information, use the `debug ip drp` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip drp
no debug ip drp
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

The `debug ip drp` command is used to debug the director response agent used by the Distributed Director product. The Distributed Director can be used to dynamically respond to Domain Name System (DNS) queries with the IP address of the “best” host based on various criteria.

**Examples**

The following is sample output from the `debug ip drp` command. This example shows the packet origination, the IP address that information is routed to, and the route metrics that were returned.

```
Router# debug ip drp
DRP: received v1 packet from 172.69.232.8, via Ethernet0
DRP: RTQUERY for 172.69.58.94 returned internal=0, external=0
```

The table below describes the significant fields shown in the display.

**Table 17: debug ip drp Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRP: received v1 packet from 172.69.232.8, via Ethernet0</td>
<td>Router received a version 1 DRP packet from the IP address shown, via the interface shown.</td>
</tr>
<tr>
<td>DRP: RTQUERY for 172.69.58.94</td>
<td>DRP packet contained two Route Query requests. The first request was for the distance to the IP address 171.69.113.50.</td>
</tr>
<tr>
<td>internal</td>
<td>If nonzero, the metric for the internal distance of the route that the router uses to send packets in the direction of the client. The internal distance is the distance within the autonomous system of the router.</td>
</tr>
<tr>
<td>external</td>
<td>If nonzero, the metric for the Border Gateway Protocol (BGP) or external distance used to send packets to the client. The external distance is the distance outside the autonomous system of the router.</td>
</tr>
</tbody>
</table>
The `debug ip dvmrp` command is not available in 12.2(33)SRB, 15.0(1)M, and later 12.2SR, 15.0M, and T releases.

To display information on Distance Vector Multiprotocol Routing Protocol (DVMRP) packets received and sent, use the `debug ip dvmrp` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip dvmrp [detail [access-list] [in | out]]
no debug ip dvmrp [detail [access-list] [in | out]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>detail</code></td>
<td>(Optional) Enables a more detailed level of output and displays packet contents.</td>
</tr>
<tr>
<td><code>access-list</code></td>
<td>(Optional) Causes the <code>debug ip dvmrp</code> command to restrict output to one access list.</td>
</tr>
<tr>
<td><code>in</code></td>
<td>(Optional) Causes the <code>debug ip dvmrp</code> command to output packets received in DVMRP reports.</td>
</tr>
<tr>
<td><code>out</code></td>
<td>(Optional) Causes the <code>debug ip dvmrp</code> command to output packets sent in DVMRP reports.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Usage Guidelines**

Use the `debug ip dvmrp detail` command with care. This command generates a substantial amount of output and can interrupt other activity on the router when it is invoked.

**Examples**

The following is sample output from the `debug ip dvmrp` command:

```
Router# debug ip dvmrp
DVMRP: Received Report on Ethernet0 from 172.19.244.10
DVMRP: Received Report on Ethernet0 from 172.19.244.11
DVMRP: Building Report for Ethernet0 224.0.0.4
DVMRP: Send Report on Ethernet0 to 224.0.0.4
DVMRP: Sending IGMP Reports for known groups on Ethernet0
DVMRP: Received Report on Ethernet0 from 172.19.244.10
DVMRP: Received Report on Tunnel0 from 192.168.199.254
DVMRP: Received Report on Tunnel0 from 192.168.199.254
DVMRP: Received Report on Tunnel0 from 192.168.199.254
DVMRP: Received Report on Tunnel0 from 192.168.199.254
DVMRP: Received Report on Tunnel0 from 192.168.199.254
DVMRP: Received Report on Tunnel0 from 192.168.199.254
DVMRP: Received Report on Tunnel0 from 192.168.199.254
DVMRP: Received Report on Tunnel0 from 192.168.199.254
DVMRP: Received Report on Tunnel0 from 192.168.199.254
DVMRP: Received Report on Tunnel0 from 192.168.199.254
DVMRP: Received Report on Tunnel0 from 192.168.199.254
DVMRP: Building Report for Tunnel0 224.0.0.4
DVMRP: Send Report on Tunnel0 to 192.168.199.254
DVMRP: Send Report on Tunnel0 to 192.168.199.254
DVMRP: Send Report on Tunnel0 to 192.168.199.254
DVMRP: Send Report on Tunnel0 to 192.168.199.254
DVMRP: Send Report on Tunnel0 to 192.168.199.254
DVMRP: Radix tree walk suspension
DVMRP: Send Report on Tunnel0 to 192.168.199.254
```

The following lines show that the router received DVMRP routing information and placed it in the mroute table:
DVMRP: Received Report on Ethernet0 from 172.19.244.10
DVMRP: Received Report on Ethernet0 from 172.19.244.11

The following lines show that the router is creating a report to send to another DVMRP router:

DVMRP: Building Report for Ethernet0 224.0.0.4
DVMRP: Send Report on Ethernet0 to 224.0.0.4

The table below provides a list of internet multicast addresses supported for host IP implementations.

### Table 18: Internet Multicast Addresses

<table>
<thead>
<tr>
<th>Address</th>
<th>Description</th>
<th>RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.0</td>
<td>Base address (reserved)</td>
<td>RFC 1112</td>
</tr>
<tr>
<td>224.0.0.1</td>
<td>All systems on this subnet</td>
<td>RFC 1112</td>
</tr>
<tr>
<td>224.0.0.2</td>
<td>All routers on this subnet</td>
<td></td>
</tr>
<tr>
<td>224.0.0.3</td>
<td>Unassigned</td>
<td></td>
</tr>
<tr>
<td>224.0.0.4</td>
<td>DVMRP routers</td>
<td>RFC 1075</td>
</tr>
<tr>
<td>224.0.0.5</td>
<td>OSPFIGP all routers</td>
<td>RFC 1583</td>
</tr>
</tbody>
</table>

The following lines show that a protocol update report has been sent to all known multicast groups. Hosts use Internet Group Management Protocol (IGMP) reports to communicate with routers and to request to join a multicast group. In this case, the router is sending an IGMP report for every known group to the host, which is running mrouted. The host then responds as though the router were a host on the LAN segment that wants to receive multicast packets for the group.

DVMRP: Sending IGMP Reports for known groups on Ethernet0

The following is sample output from the `debug ip dvmrp detail` command:

```
Router# debug ip dvmrp detail
DVMRP: Sending IGMP Reports for known groups on Ethernet0
DVMRP: Advertise group 224.2.224.2 on Ethernet0
DVMRP: Advertise group 224.2.193.34 on Ethernet0
DVMRP: Advertise group 224.2.231.6 on Ethernet0
DVMRP: Received Report on Tunnel0 from 192.168.199.254
DVMRP: Origin 150.166.195.0/24, metric 13, distance 0
DVMRP: Origin 150.166.54.0/24, metric 13, distance 0
DVMRP: Origin 150.166.55.0/24, metric 13, distance 0
DVMRP: Origin 150.166.56.0/24, metric 13, distance 0
DVMRP: Origin 150.166.92.0/24, metric 12, distance 0
DVMRP: Origin 150.166.100.0/24, metric 12, distance 0
DVMRP: Origin 150.166.101.0/24, metric 12, distance 0
DVMRP: Origin 150.166.142.0/24, metric 8, distance 0
DVMRP: Origin 150.166.200.0/24, metric 12, distance 0
DVMRP: Origin 150.166.237.0/24, metric 12, distance 0
DVMRP: Origin 150.203.5.0/24, metric 8, distance 0
```

The following lines show that this group is available to the DVMRP router. The mrouted process on the host will forward the source and multicast information for this group through the DVMRP cloud to other members.
DVMRP: Advertise group 224.2.224.2 on Ethernet0

The following lines show the DVMRP route information:

DVMRP: Origin 150.166.53.0/24, metric 13, distance 0
DVMRP: Origin 150.166.54.0/24, metric 13, distance 0

The metric is the number of hops the route has covered, and the distance is the administrative distance.
**debug ip eigrp**

To display information on Enhanced Interior Gateway Routing Protocol (EIGRP) protocol packets, use the `debug ip eigrp` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip eigrp [vrf vrf-name]
no debug ip eigrp [vrf vrf-name]
```

**Syntax Description**

| vrf vrf-name | (Optional) Restricts output to a specific VRF. |

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(21)S</td>
<td>This command was modified. The <code>vrf vrf-name</code> keyword and argument were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command helps you analyze the packets that are sent and received on an interface. Because the `debug ip eigrp` command generates a substantial amount of output, only use it when traffic on the network is light.

**Examples**

The following is sample output from the `debug ip eigrp` command:

```
Router# debug ip eigrp
IP-EIGRP: Processing incoming UPDATE packet
IP-EIGRP: Ext 192.168.3.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 - 256000 104960
IP-EIGRP: Ext 192.168.0.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 - 256000 104960
IP-EIGRP: Ext 192.168.3.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 - 256000 104960
IP-EIGRP: 172.69.43.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 172.69.43.0 255.255.255.0 metric 371200 - 256000 115200
IP-EIGRP: 192.135.246.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 192.135.246.0 255.255.255.0 metric 4631656 - 45714176 596480
IP-EIGRP: 192.135.246.0 255.255.255.0 metric 371200 - 256000 115200
IP-EIGRP: 172.69.40.0 255.255.255.0 - do advertise out Ethernet0/1
IP-EIGRP: Ext 172.69.40.0 255.255.255.0 metric 2272256 - 1657856 614400
IP-EIGRP: 192.135.245.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 192.135.245.0 255.255.255.0 metric 40622080 - 40000000 622080
IP-EIGRP: 192.135.244.0 255.255.255.0, - do advertise out Ethernet0/1
```

The table below describes the significant fields shown in the display.

**Table 18: debug ip eigrp Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-EIGRP</td>
<td>Indicates that this is an IP EIGRP message.</td>
</tr>
<tr>
<td>Ext</td>
<td>Indicates that the following address is an external destination rather than an internal destination, which would be labeled as Int.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
--- | ---
M | Displays the computed metric, which includes the value in the SM field and the cost between this router and the neighbor. The first number is the composite metric. The next two numbers are the inverse bandwidth and the delay, respectively.
SM | Displays the metric as reported by the neighbor.

The following example shows how to turn on debugging output for a specific VRF in an EIGRP instance:

```
Router# debug ip eigrp vrf red
EIGRP-IPv4 Route Event debugging is on
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf definition</td>
<td>Defines a virtual routing and forwarding instance.</td>
</tr>
</tbody>
</table>
debug ip eigrp notifications

To display Enhanced Interior Gateway Routing Protocol (EIGRP) events and notifications in the console of the router, use the `debug ip eigrp notifications` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip eigrp notifications
no debug ip eigrp notifications
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output of the `debug ip eigrp notifications` command displays EIGRP events and notifications.

**Examples**

The following example output shows that the NSF-aware router has received the restart notification. The NSF-aware router will now wait for end of transmission (EOT) to be sent from the restarting neighbor (NSF-capable).

```
Router# debug ip eigrp notifications
*Oct 4 11:39:18.092:EIGRP:NSF:AS2. Rec RS update from 135.100.10.1, 00:00:00. Wait for EOT.
*Oct 4 11:39:18.092:%DUAL-5-NBRCHANGE:IP-EIGRP(0) 2:Neighbor 135.100.10.1 (POS3/0) is up:peer NSF restarted
```
debug ip error

To display IP errors, use the `debug ip error` command in privileged EXEC mode. To disable debugging errors, use the `no` form of this command.

```
debug ip error access-list-number [detail] [dump]
no debug ip error
```

**Syntax Description**

| access-list-number | (Optional) The IP access list number that you can specify. If the datagram is not permitted by that access list, the related debugging output (or IP error) is suppressed. Standard, extended, and expanded access lists are supported. The range of standard and extended access lists is from 1 to 199. The range of expanded access lists is from 1300 to 2699. |
| detail | (Optional) Displays detailed IP error debugging information. |
| dump | (Hidden) Displays IP error debugging information along with raw packet data in hexadecimal and ASCII forms. This keyword can be enabled with individual access lists and also with the `detail` keyword. |

**Note**

The `dump` keyword is not fully supported and should be used only in collaboration with Cisco Technical Support. Because of the risk of using significant CPU utilization, the `dump` keyword is hidden from the user and cannot be seen using the “?” prompt. The length of the displayed packet information may exceed the actual packet length and include additional padding bytes that do not belong to the IP packet. Also note that the beginning of a packet may start at different locations in the dump output depending on the specific router, interface type, and packet header processing that may have occurred before the output is displayed.

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

This command is used for IP error debugging. The output displays IP errors which are locally detected by this router.

**Caution**

Enabling this command will generate output only if IP errors occur. However, if the router starts to receive many packets that contain errors, substantial output may be generated and severely affect system performance. This command should be used with caution in production networks. It should only be enabled when traffic on the IP network is low, so other activity on the system is not adversely affected. Enabling the `detail` and `dump` keywords use the highest level of system resources of the available configuration options for this command, so a high level of caution should be applied when enabling either of these keywords.

**Caution**

The `dump` keyword is not fully supported and should be used only in collaboration with Cisco Technical Support.
The following is sample output from the `debug ip error` command:

```
Router# debug ip error
IP packet errors debugging is on
04:04:45:IP:s=10.8.8.1 (Ethernet0/1), d=10.1.1.1, len 28, dispose ip.hopcount
```

The IP error in the above output was caused when the router attempted to forward a packet with a time-to-live (TTL) value of 0. The “ip.hopcount” traffic counter is incremented when a packet is dropped because of an error. This error is also displayed in the output of the `show ip traffic` command by the “bad hop count” traffic counter.

The table below describes the significant fields shown in the display.

**Table 20: debug ip error Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP:s=10.8.8.1 (Ethernet0/1)</td>
<td>The packet source IP address and interface.</td>
</tr>
<tr>
<td>d=10.1.1.1, len 28</td>
<td>The packet destination IP address and prefix length.</td>
</tr>
<tr>
<td>dispose ip.hopcount</td>
<td>This traffic counter increments when an IP packet is dropped because of an error.</td>
</tr>
</tbody>
</table>

The following is sample output from the `debug ip error` command enabled with the `detail` keyword:

```
Router# debug ip error detail
IP packet errors debugging is on (detailed)
1d08h:IP:s=10.0.19.100 (Ethernet0/1), d=10.1.1.1, len 28, dispose udp.noport
1d08h: UDP src=41921, dst=33434
1d08h:IP:s=10.0.19.100 (Ethernet0/1), d=10.2.2.2, len 28, dispose ip.hopcount
1d08h: UDP src=33691, dst=33434
```

The detailed output includes layer 4 information in addition to the standard output. The IP error in the above output was caused when the router received a UDP packet when no application was listening to the UDP port. The “udp.noport” traffic counter is incremented when the router drops a UDP packet because of this error. This error is also displayed in the output of the `show ip traffic` command by the “no port” traffic counter under “UDP statistics.”

The table below describes the significant fields shown in the display.

**Table 21: debug ip error detail Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP:s=10.0.19.100 (Ethernet0/1)</td>
<td>The IP packet source IP address and interface.</td>
</tr>
<tr>
<td>d=10.1.1.1, len 28</td>
<td>The IP packet destination and prefix length.</td>
</tr>
<tr>
<td>dispose udp.noport</td>
<td>The traffic counter that is incremented when a UDP packet is dropped because of this error.</td>
</tr>
</tbody>
</table>
The following is sample output from the `debug ip error` command enabled with the `detail` and `dump` keywords:

```plaintext
Router# debug ip error detail dump
IP packet errors debugging is on (detailed) (dump)
1d08h:IP:s=10.0.19.100 (Ethernet0/1), d=10.1.1.1, len 28, dispose udp.noport
  03D72360: 0001 42AD4242 ..B-BB
  03D72370: 0002FCA5 DC390800 4500001C 30130000 ..|9..E...0...
  03D72380: 011161159 0A001364 0A010101 9430829A ..aY...d.....0..
  03D72390: 0008C0AD ..@
1d08h:IP:s=10.0.19.100 (Ethernet0/1), d=10.2.2.2, len 28, dispose ip.hopcount
  03C01600: 0001 42AD4242 ..B-BB
  03C01610: 0002FCA5 DC390800 4500001C 302A0000 ..|9..E...0*
  03C01620: 01116040 0A001364 0A020202 A188829A ..`@...d....!
  03C01630: 0008B253 ..2S
```

The `dump` keyword is not fully supported and should be used only in collaboration with Cisco Technical Support. See the caution in the usage guidelines section of this command reference page for more specific information.

The output from the `debug ip error` command, when the `dump` keyword is enabled, provides raw packet data in hexadecimal and ASCII forms. This additional output is displayed in addition to the standard output. The dump keyword can be used with all of the available configuration options of this command.

The table below describes the significant fields shown in the display.

### Table 22: `debug ip error detail dump` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP:s=10.0.19.100</td>
<td>The IP packet source IP address and interface.</td>
</tr>
<tr>
<td>d=10.1.1.1, len 28</td>
<td>The IP packet destination and prefix length.</td>
</tr>
<tr>
<td>dispose udp.noport</td>
<td>The traffic counter that is incremented when a UDP packet is dropped because of this error.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip traffic</td>
<td>Displays statistics about IP traffic.</td>
</tr>
</tbody>
</table>
**debug ip flow cache**

To enable debugging output for NetFlow cache, use the `debug ip flow cache` command in user EXEC or privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip flow cache
no debug ip flow cache
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging output for NetFlow data export is disabled.

**Command Modes**

User EXEC
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(1)</td>
<td>Debugging output for NetFlow v9 data export was added.</td>
</tr>
<tr>
<td>12.3(7T)</td>
<td>Debugging output for NetFlow for IPv6 was added.</td>
</tr>
<tr>
<td>12.2(30)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(30)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip flow export` command:

```
Router# debug ip flow cache
IP Flow cache allocation debugging is on
Router# show ipv6 flow
IP packet size distribution (0 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .000  .000  .000  .000  .000  .000  .000  .000  .000  .000  .000  .000  .000  .000
  512  544  576  608  640  672  704  736  768  800  832  864  896  928  960
  .000  .000  .000  .000  .000  .000  .000  .000  .000  .000  .000  .000  .000  .000
IP Flow Switching Cache, 0 bytes
  0 active, 0 inactive, 0 added
  0 age timer polls, 0 flow alloc failures
  Active flows timeout in 15 seconds
  Inactive flows timeout in 15 seconds
SrcAddress   OutIf   Prot SrcPrt DstPrt Packets
000039: 01:56:26: IPFLOW: Sub-Flow numbers are:
```
24 sub-flows per chunk, 0 hashflag len,
1 chunks allocated, 12 max chunks,
24 allocated records, 24 free records, 960 bytes allocated
000040: 01:56:26: IPFLOW: Sub-Flow cache removed

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>export destination</td>
<td>Enables the exporting of information from NetFlow aggregation caches.</td>
</tr>
<tr>
<td>ip flow-aggregation cache</td>
<td>Enables NetFlow aggregation cache schemes.</td>
</tr>
<tr>
<td>ip flow-export</td>
<td>Enables the exporting of information in NetFlow cache entries.</td>
</tr>
<tr>
<td>ipv6 flow-aggregation cache</td>
<td>Enables NetFlow aggregation cache schemes for IPv6 configurations.</td>
</tr>
<tr>
<td>ipv6 flow export</td>
<td>Enables the exporting of information in NetFlow cache entries for IPv6 NetFlow configurations.</td>
</tr>
<tr>
<td>show ip cache flow aggregation</td>
<td>Displays the NetFlow aggregation cache configuration.</td>
</tr>
<tr>
<td>show ip flow export</td>
<td>Display the statistics for NetFlow data export.</td>
</tr>
</tbody>
</table>
debug ip flow export

To enable debugging output for NetFlow data export, use the debug ip flow export command in user EXEC or privileged EXEC mode. To disable debugging output for NetFlow data export, use the no form of this command.

debug ip flow export
no debug ip flow export

Syntax Description
This command has no keywords or arguments.

Command Default
Debugging output for NetFlow data export is disabled.

Command Modes
User EXEC
Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(1)</td>
<td>Debugging output for NetFlow v9 data export was added.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>This command was modified so that NetFlow v9 data is collected for both IPv4 and IPv6.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.2(30)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(30)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(18)SXF</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXF.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Examples

The following is sample output from the debug ip flow export command:

Router# debug ip flow export
IP Flow export mechanism debugging is on
*Mar 6 22:56:21.627:IPFLOW:Sending export pak to 2001::FFFE/64 port 9999

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>export destination</td>
<td>Enables the exporting of information from NetFlow aggregation caches.</td>
</tr>
<tr>
<td>ipv6 flow-aggregation cache</td>
<td>Enables NetFlow aggregation cache schemes for IPv6.</td>
</tr>
<tr>
<td>ipv6 flow-export</td>
<td>Enables the exporting of information in NetFlow cache entries.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show ip cache flow aggregation</code></td>
<td>Displays the NetFlow accounting aggregation cache statistics.</td>
</tr>
<tr>
<td><code>show ip flow export</code></td>
<td>Displays the statistics for NetFlow data export.</td>
</tr>
<tr>
<td><code>show ipv6 flow export</code></td>
<td>Displays the statistics for NetFlow data export for IPv6.</td>
</tr>
</tbody>
</table>
To activate the debugging option to track the transactions submitted during an FTP session, use the **debug ip ftp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip ftp
no debug ip ftp
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

The **debug ip ftp** command is useful for debugging problems associated with FTP.

While configuring the ftp password, only encryption types 0 and 7 are allowed. Other encryption types will invoke an "Invalid encryption type" error.

If encryption type 7 has been chosen, the cli will check if the supplied password is encrypted (encrypted by Cisco proprietary algorithm). If the supplied password is found to be Cisco-encrypted, it will be configured. Otherwise the error "Invalid encrypted password" will be shown. The option 7 expects a Cisco-encrypted password to be supplied in the cli.

While configuring the ftp password, if encryption type 0 has been chosen, the cli will encrypt the password as long as the "service password-encryption" is enabled.

**Examples**

The following is an example of the **debug ip ftp** command:

```
Router# debug ip ftp
FTP transactions debugging is on
```

The following is sample output from the **debug ip ftp** command:

```
FTP: 220 ProFTPD 1.2.0pre8 Server (DFW Nostrum FTP Server) [defiant.dfw.nostrum.com]
Dec 27 22:12:09.133: FTP: ---> USER router
Dec 27 22:12:09.137: FTP: ---> PASS WQHK5JY2
Dec 27 22:12:09.157: FTP: 200 Type set to I.
```

Cisco IOS Debug Command Reference - Commands I through L
debug ip ftp
debug ip http all through debug ip rsvp

- debug ip http all, on page 118
- debug ip http authentication, on page 120
- debug ip http client, on page 122
- debug ip http client cookie, on page 125
- debug ip http ezsetup, on page 126
- debug ip http secure-all, on page 128
- debug ip http secure-session, on page 130
- debug ip http secure-state, on page 132
- debug ip http ssi, on page 133
- debug ip http ssl error, on page 135
- debug ip http token, on page 137
- debug ip http transaction, on page 139
- debug ip http url, on page 141
- debug ip icmp, on page 142
- debug ip igmp, on page 147
- debug ip igmp snooping, on page 149
- debug ip igrp events, on page 150
- debug ip igrp transactions, on page 152
- debug ip inspect, on page 154
- debug ip inspect ha, on page 160
- debug ip inspect L2-transparent, on page 162
- debug ip ips, on page 164
- debug ip mbgp dampening, on page 165
- debug ip mbgp updates, on page 166
- debug ip mcache, on page 168
- debug ip mds ipc, on page 170
- debug ip mds mevent, on page 171
- debug ip mds mpacket, on page 172
- debug ip mds process, on page 173
- debug ip mfib adjacency, on page 174
- debug ip mfib db, on page 175
- debug ip mfib fs, on page 176
- debug ip mfib init, on page 177
debug ip mfib interface, on page 178
debug ip mfib mrrib, on page 179
debug ip mfib nat, on page 180
debug ip mfib pak, on page 181
debug ip mfib platform, on page 182
debug ip mfib ppr, on page 183
debug ip mfib ps, on page 185
debug ip mfib signal, on page 186
debug ip mfib table, on page 187
debug ip mhbeat, on page 188
debug ip mobile, on page 190
debug ip mobile advertise, on page 195
debug ip mobile dyn-pbr, on page 196
debug ip mobile host, on page 199
debug ip mobile mib, on page 200
debug ip mobile redundancy, on page 202
debug ip mobile router, on page 203
debug ip mpacket, on page 205
debug ip mrrib, on page 208
debug ip mrm, on page 209
debug ip mrouting, on page 210
debug ip mrouting limits, on page 213
debug ip msdp, on page 215
debug ip msdp resets, on page 217
debug ip multicast hardware-switching, on page 218
debug ip multicast redundancy, on page 220
debug ip multicast rpf tracked, on page 227
debug ip multicast topology, on page 228
debug ip nat, on page 229
debug ip nat redundancy, on page 237
debug ip nbar trace, on page 238
debug ip nbar clients, on page 240
debug ip nbar config, on page 241
debug ip nbar platform, on page 242
debug ip ospf adj, on page 243
debug ip ospf database-timer rate-limit, on page 244
debug ip ospf events, on page 245
debug ip ospf lsa-maxage, on page 246
debug ip ospf mpls traffic-eng advertisements, on page 247
debug ip ospf nsf, on page 249
debug ip ospf packet, on page 250
debug ip ospf rib, on page 252
debug ip ospf spf statistic, on page 254
debug ip packet, on page 256
debug ip pgm host, on page 262
debug ip pgm router, on page 264
• debug ip pim, on page 266
• debug ip pim atm, on page 270
• debug ip pim auto-rp, on page 271
• debug ip policy, on page 273
• debug ip rbscp, on page 275
• debug ip rbscp ack-split, on page 276
• debug ip rgmp, on page 278
• debug ip rip, on page 279
• debug ip routing, on page 281
• debug ip routing static bfd, on page 283
• debug ip rsvp, on page 284
• debug ip rsvp aggregation, on page 289
• debug ip rsvp authentication, on page 291
• debug ip rsvp detail, on page 293
• debug ip rsvp dump-messages, on page 295
• debug ip rsvp errors, on page 298
• debug ip rsvp hello, on page 300
• debug ip rsvp high-availability, on page 302
• debug ip rsvp p2mp, on page 305
• debug ip rsvp policy, on page 306
• debug ip rsvp rate-limit, on page 309
• debug ip rsvp reliable-msg, on page 311
• debug ip rsvp sbm, on page 313
• debug ip rsvp sso, on page 315
• debug ip rsvp summary-refresh, on page 317
• debug ip rsvp traffic-control, on page 319
• debug ip rsvp wfq, on page 321
**debug ip http all**

To enable debugging output for all HTTP processes on the system, use the `debug ip http all` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip http all
no debug ip http all
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to enable debugging messages for all HTTP processes and activity. Issuing this command is equivalent to issuing the following commands:

- `debug ip http authentication`
- `debug ip http ezsetup`
- `debug ip http ssi`
- `debug ip http token`
- `debug ip http transaction`
- `debug ip http url`

**Examples**

For sample output and field descriptions of this command, see the documentation of the commands listed in the “Usage Guidelines” section.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ip http authentication</code></td>
<td>Enables debugging output for all processes for HTTP server and client access.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>debug ip http ezsetup</td>
<td>Displays the configuration changes that occur during the EZ Setup process.</td>
</tr>
<tr>
<td>debug ip http ssi</td>
<td>Displays SSI translations and SSI ECHO command execution.</td>
</tr>
<tr>
<td>debug ip http token</td>
<td>Displays individual tokens parsed by the HTTP server.</td>
</tr>
<tr>
<td>debug ip http transaction</td>
<td>Displays HTTP server transaction processing.</td>
</tr>
<tr>
<td>debug ip http url</td>
<td>Displays the URLs accessed from the router.</td>
</tr>
</tbody>
</table>
debug ip http authentication

To troubleshoot HTTP authentication problems, use the `debug ip http authentication` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

`debug ip http authentication`  
`no debug ip http authentication`

**Syntax Description**  
This command has no arguments or keywords.

**Command Modes**  
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**  
Use this command to display the authentication method the router attempted and authentication-specific status messages.

**Examples**

The following is sample output from the `debug ip http authentication` command:

```
Router# debug ip http authentication
Authentication for url '/' '/' level 15 privless '/'
Authentication username = 'local15' priv-level = 15 auth-type = local
```

The table below describes the significant fields shown in the display.

**Table 23: debug ip http authentication Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication for url</td>
<td>Provides information about the URL in different forms.</td>
</tr>
<tr>
<td>Authentication username</td>
<td>Identifies the user.</td>
</tr>
<tr>
<td>priv-level</td>
<td>Indicates the user privilege level.</td>
</tr>
<tr>
<td>auth-type</td>
<td>Indicates the authentication method.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ip http all</code></td>
<td>Displays authentication processes for all HTTP server processes on the system.</td>
</tr>
<tr>
<td><code>debug ip http ezsetup</code></td>
<td>Displays the configuration changes that occur during the EZ Setup process.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>debug ip http ssi</td>
<td>Displays SSI translations and SSI ECHO command execution.</td>
</tr>
<tr>
<td>debug ip http token</td>
<td>Displays individual tokens parsed by the HTTP server.</td>
</tr>
<tr>
<td>debug ip http transaction</td>
<td>Displays HTTP server transaction processing.</td>
</tr>
<tr>
<td>debug ip http url</td>
<td>Displays the URLs accessed from the router.</td>
</tr>
</tbody>
</table>
**debug ip http client**

To enable debugging output for the HTTP client, use the `debug ip http client` command in privileged EXEC mode. To disable debugging output for the HTTP client, use the `no` or `undebug` form of this command.

```
debug ip http client {all | api | cache | error | main | msg | socket}
no debug ip http client {all | api | cache | error | main | msg | socket}
undebug ip http client {all | api | cache | error | main | msg | socket}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enables debugging for all HTTP client elements.</td>
</tr>
<tr>
<td>api</td>
<td>Enables debugging output for the HTTP client application interface (API).</td>
</tr>
<tr>
<td>cache</td>
<td>Enables debugging output for the HTTP client cache.</td>
</tr>
<tr>
<td>error</td>
<td>Enables debugging output for HTTP communication errors.</td>
</tr>
<tr>
<td>main</td>
<td>Enables debugging output specific to the Voice XML (VXML) applications interacting with the HTTP client.</td>
</tr>
<tr>
<td>msg</td>
<td>Enables debugging output specific to the HTTP client messages.</td>
</tr>
<tr>
<td>socket</td>
<td>Enables debugging output specific to the HTTP client socket.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to display transactional information for the HTTP client for debugging purposes.

**Examples**

The following example shows sample debugging output for a failed `copy` transfer operation when the host name resolution fails:

```
Router# debug ip http client all
2w4d: Cache ager called
Router# copy http://www.example.com/index.html flash:index.html
```

Destination filename [index.html]?
The following example shows sample debugging output for a failed `copy` transfer operation when the source file is not available:

Router# `copy http://example.com/hi/file.html flash:/file.html`

Destination filename [file.html]? 

% Error opening http://example.com/hi/file.html (No such file or directory)

The table below describes the significant fields shown in the display.

**Table 24: debug ip http client Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2w4d:</td>
<td>In the examples shown, the string “2w4d” is the timestamp configured on the system. Indicates two weeks and four days since the last system reboot.</td>
</tr>
<tr>
<td></td>
<td>• The time-stamp format is configured using the <code>service timestamps debug</code> global configuration mode command.</td>
</tr>
<tr>
<td>HTTPC: or httpsc</td>
<td>Indicates the HTTP client in Cisco IOS software.</td>
</tr>
<tr>
<td>httpc_request:Don't have the credentials</td>
<td>Indicates that this HTTP client request did not supply any authentication information to the server.</td>
</tr>
<tr>
<td></td>
<td>The authentication information consists of a username and password combination.</td>
</tr>
<tr>
<td></td>
<td>The message is applicable to both HTTP and HTTPS.</td>
</tr>
</tbody>
</table>
The “ok” in this line indicates that there were no internal errors relating to processing this HTTP client transaction by the HTTP client. In other words, the HTTP client was able to send the request and receive some response.

Note: The “ok” value in this line does not indicate file availability (“200: OK” message or “404: File Not Found” message).

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy</td>
<td>Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.</td>
</tr>
<tr>
<td>ip http client connection</td>
<td>Configures the HTTP client connection.</td>
</tr>
<tr>
<td>ip http client password</td>
<td>Configures a password for all HTTP client connections.</td>
</tr>
<tr>
<td>ip http client proxy-server</td>
<td>Configures an HTTP proxy server.</td>
</tr>
<tr>
<td>ip http client source-interface</td>
<td>Configures a source interface for the HTTP client.</td>
</tr>
<tr>
<td>ip http client username</td>
<td>Configures a login name for all HTTP client connections.</td>
</tr>
<tr>
<td>service timestamps</td>
<td>Configures the time-stamping format for debugging or system logging messages.</td>
</tr>
<tr>
<td>show ip http client connection</td>
<td>Displays a report about HTTP client active connections.</td>
</tr>
<tr>
<td>show ip http client history</td>
<td>Displays the URLs accessed by the HTTP client.</td>
</tr>
<tr>
<td>show ip http client session-module</td>
<td>Displays a report about sessions that have registered with the HTTP client.</td>
</tr>
</tbody>
</table>
debug ip http client cookie

To debug the HTTP client cookie, use the `debug ip http client cookie` command in privileged EXEC mode. To disable this debugging activity, use the `no` form of this command.

```
debug ip http client cookie
no debug ip http client cookie
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip http client cookie` command:

```
Device# debug ip http client cookie
ClientCookie: Receiving Set-Cookie cookie1=1 domain=172.16.0.2 path=/cwmp-1-0/testacs flags=264 expire=Mon,30-Jun-2008 05:51:27 GMT now=48686D74
ClientCookie2: Receiving Set-Cookie2 cookie1=1 domain=172.16.0.2 path=/cwmp-1-0/ flags=256 expire=60 port=0 now=48686E1A comment= commentURL=  
```
**debug ip http ezsetup**

To display the configuration changes that occur during the EZ Setup process, use the `debug ip http ezsetup` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
default ip http ezsetup
no debug ip http ezsetup
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to verify the EZ Setup actions without changing the configuration of the router. EZ Setup is a form you fill out to perform basic router configuration from most HTML browsers.

**Examples**

The following sample output from the `debug ip http ezsetup` command shows the configuration changes for the router when the EZ Setup form has been submitted:

```
Router# debug ip http ezsetup
service timestamps debug
service timestamps log
service password-encryption
!
hostname router-name
!
enable secret router-pw
line vty 0 4
password router-pw
!
interface ethernet 0
  ip address 172.69.52.9 255.255.255.0
  no shutdown
  ip helper-address 172.31.2.132
  ip name-server 172.31.2.132
  isdn switch-type basic-5ess
  username Remote-name password Remote-chap
interface bri 0
  ip unnumbered ethernet 0
  encapsulation ppp
  no shutdown
  dialer map ip 192.168.254.254 speed 56 name Remote-name Remote-number
  isdn spid1 spid1
  isdn spid2 spid2
  ppp authentication chap callin
  dialer-group 1
!
ip classless
```
access-list 101 deny udp any any eq snmp
access-list 101 deny udp any any eq ntp
access-list 101 permit ip any any
dialer-list 1 list 101
ip route 0.0.0.0 0.0.0.0 192.168.254.254
ip route 192.168.254.254 255.255.255.255 bri 0
logging buffered
snmp-server community public RO
ip http server
ip classless
ip subnet-zero
!
end

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip http all</td>
<td>Displays authentication processes for all HTTP server processes on the system.</td>
</tr>
<tr>
<td>debug ip http authentication</td>
<td>Displays authentication processes for HTTP server and client access.</td>
</tr>
<tr>
<td>debug ip http ssi</td>
<td>Displays SSI translations and SSI ECHO command execution.</td>
</tr>
<tr>
<td>debug ip http token</td>
<td>Displays individual tokens parsed by the HTTP server.</td>
</tr>
<tr>
<td>debug ip http transaction</td>
<td>Displays HTTP server transaction processing.</td>
</tr>
<tr>
<td>debug ip http url</td>
<td>Displays the URLs accessed from the router.</td>
</tr>
</tbody>
</table>
# debug ip http secure-all

To generate the following output, use the `debug ip http secure-all` command in privileged EXEC mode:

- The debugging information generated by the `debug ip http secure-session` command
- The debugging information generated by the `debug ip http secure-state` command
- Debugging information for each call to the SSL driver, for use primarily by Cisco support personnel

To disable this debugging, use the `no` form of this command.

```bash
default ip http secure-all
no debug ip http secure-all
```

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled.

## Command Modes

Privileged EXEC

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(11b)E</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

This command generates the following:

- The debugging information generated by the `debug ip http secure-session` command. See the `debug ip http secure-session` command page for example debugging output.
- The debugging information generated by the `debug ip http secure-state` command. See the `debug ip http secure-state` command page for example debugging output.
- Debugging information for each call to the SSL driver, for use primarily by Cisco support personnel

## Examples

The following example generates the following output:

- The debugging information generated by the `debug ip http secure-session` command
- The debugging information generated by the `debug ip http secure-state` command
- Debugging information for each call to the SSL driver

```bash
Router# debug ip http secure-all
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip http secure-session</td>
<td>Generates debugging information about each new secure HTTPS session when it is created.</td>
</tr>
<tr>
<td>debug ip http secure-state</td>
<td>Generates debugging information each time the secure HTTPS server changes state.</td>
</tr>
</tbody>
</table>
debug ip http secure-session

To generate debugging information about each new secure HTTPS session when it is created, use the `debug ip http secure-session` command in privileged EXEC mode. To disable this debugging, use the `no` form of this command.

```
debug ip http secure-session
no debug ip http secure-session
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(11b)E</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command generates debugging information about each new HTTPS session when it is created. When a new HTTPS session is created, debugging information is generated in the following format:

```
HTTPS SSL Session Established/Handshake done - Peer 10.0.0.1
state = SSL negotiation finished successfully
SessionInfo: Digest=RC4-MD5 SSLVer=SSLv3 KeyEx=RSA Auth=rsa Cipher=RC4(128) Mac=MD5
```

The SessionInfo fields provide the following information about the session:

- **Digest** -- digest mechanism
- **SSLVer** -- SSL or TSL version
- **KeyEx** -- key exchange mechanism
- **Auth** -- authentication mechanism
- **Cipher** -- encryption algorithm
- **Mac** -- Message Authentication Code algorithm

**Examples**

The following example generates debugging information about each new HTTPS session when it is created:

```
debug ip http secure-session
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip http secure-all</td>
<td>Enables all other debugging ip http secure-&lt;x&gt; commands and generates debugging information for each call to the HTTPS server driver.</td>
</tr>
<tr>
<td>debug ip http secure-state</td>
<td>Generates debugging information each time the HTTPS server changes state.</td>
</tr>
</tbody>
</table>
debug ip http secure-state

To generate debugging output each time the Secure HTTP (HTTPS) feature changes state, use the `debug ip http secure-state` command in privileged EXEC mode. To disable this debugging, use the `no` form of this command.

```
dbg ip http secure-state
no dbg ip http secure-state
```

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
Disabled.

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(11b)E</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command generates debugging information each time the Secure HTTP (HTTPS) feature changes state. When the Secure HTTP (HTTPS) feature changes state, debugging information is generated in the following format:

```
HTTPS SSL State Change - Peer 10.0.0.1
Old State = SSLv3 read finished A, New State = SSL negotiation finished successfully
```

**Examples**
The following example generates debugging information each time the Secure HTTP (HTTPS) feature changes state:

```
dbg ip http secure-state
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ip http secure-all</code></td>
<td>Enables all other debugging <code>ip http secure-x</code> commands and generates debugging information for each call to the HTTPS server driver.</td>
</tr>
<tr>
<td><code>debug ip http secure-state</code></td>
<td>Generates debugging information each time the HTTPS server changes state.</td>
</tr>
</tbody>
</table>
debug ip http ssi

To display information about the HTML SSI EXEC command or HTML SSI ECHO command, use the `debug ip http ssi` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

`debug ip http ssi`  
`no debug ip http ssi`

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip http ssi` command:

```
Router# debug ip http ssi
HTML: filtered command 'exec cmd="show users"'
HTML: SSI command 'exec'
HTML: SSI tag 'cmd' = "show users"
HTML: Executing CLI 'show users' in mode 'exec' done
```

The following line shows the contents of the SSI EXEC command:

```
HTML: filtered command 'exec cmd="show users"'
```

The following line indicates the type of SSI command that was requested:

```
HTML: SSI command 'exec'
```

The following line shows the `show users` argument assigned to the `tag command`:

```
HTML: SSI tag 'cmd' = "show users"
```

The following line indicates that the `show users` command is being executed in EXEC mode:

```
HTML: Executing CLI 'show users' in mode 'exec' done
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ip http all</code></td>
<td>Displays authentication processes for all HTTP server processes on the system.</td>
</tr>
<tr>
<td><code>debug ip http authentication</code></td>
<td>Displays authentication processes for HTTP server and client access.</td>
</tr>
<tr>
<td><code>debug ip http ezsetup</code></td>
<td>Displays the configuration changes that occur during the EZ Setup process.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>debug ip http token</td>
<td>Displays individual tokens parsed by the HTTP server.</td>
</tr>
<tr>
<td>debug ip http transaction</td>
<td>Displays HTTP server transaction processing.</td>
</tr>
<tr>
<td>debug ip http url</td>
<td>Displays the URLs accessed from the router.</td>
</tr>
</tbody>
</table>
debug ip http ssl error

To enable debugging messages for the secure HTTP (HTTPS) web server and client, use the `debug ip http ssl error` command in privileged EXEC mode. To disable debugging messages for the HTTPS web server and client, use the `no debug ip http ssl error` command.

**debug ip http ssl error**

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging message output is disabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays output for debugging purposes related to the HTTPS server and HTTPS client. HTTPS services use the Secure Socket Layer (SSL) protocol, version 3.0, for encryption.

**Examples**

The following is sample debugging output from the `debug ip http ssl error` command:

```
Router# 000030:00:08:01:%HTTPS:Key pair generation failed
Router# 000030:00:08:10:%HTTPS:Failed to generate self-signed cert
Router# 000030:00:08:15:%HTTPS:SSL handshake fail
Router# 000030:00:08:21:%HTTPS:SSL read fail, uninitialized hndshk ctxt
Router# 000030:00:08:25:%HTTPS:SSL write fail, uninitialized hndshk ctxt
```

The table below describes the debug messages shown above.

**Table 25: debug ip http ssl error Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%HTTPS:Key pair generation failed</td>
<td>The RSA key pair generation failed.</td>
</tr>
<tr>
<td>%HTTPS:Failed to generate self-signed cert</td>
<td>The HTTPS server or client failed to generate a self-signed certificate.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL connection handshake failed.</td>
</tr>
<tr>
<td>A read operation failed for SSL with an uninitialized handshake context</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip http secure-server</strong></td>
<td>Enables the secure HTTP (HTTPS) server.</td>
</tr>
</tbody>
</table>
debug ip http token

To display individual tokens parsed by the HTTP server, use the `debug ip http token` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
 debug ip http token
 no debug ip http token
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ip http token` command to display low-level HTTP server parsings. To display high-level HTTP server parsings, use the `debug ip http transaction` command.

**Examples**

The following is part of sample output from the `debug ip http token` command. In this example, the browser accessed the router’s home page `http://router-name/`. The output gives the token parsed by the HTTP server and its length.

```
Router# debug ip http token
HTTP: token len 3: 'GET'
HTTP: token len 1: ':'
HTTP: token len 1: '/'
HTTP: token len 1: '
HTTP: token len 4: 'HTTP'
HTTP: token len 1: '/'
HTTP: token len 1: '1'
HTTP: token len 1: '
HTTP: token len 1: '0'
HTTP: token len 2: '\15\12'
HTTP: token len 7: 'Referer'
HTTP: token len 1: ':'
HTTP: token len 1: '
HTTP: token len 4: 'http'
HTTP: token len 1: ':'
HTTP: token len 1: '/'
HTTP: token len 1: '
HTTP: token len 1: 'www'
HTTP: token len 3: 'thesite'
HTTP: token len 1: '
HTTP: token len 3: 'com'
HTTP: token len 1: '/'
HTTP: token len 2: '\15\12'
HTTP: token len 10: 'Connection'
HTTP: token len 1: ':'
HTTP: token len 1: '
```

`debug ip http token` is the command introduced in Release 12.3(2)T. It allows you to display individual tokens parsed by the HTTP server in privileged EXEC mode. To disable debugging output, use the `no` form of this command.
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip http all</td>
<td>Displays authentication processes for all HTTP server processes on the system.</td>
</tr>
<tr>
<td>debug ip http authentication</td>
<td>Displays authentication processes for HTTP server and client access.</td>
</tr>
<tr>
<td>debug ip http ezsetup</td>
<td>Displays the configuration changes that occur during the EZ Setup process.</td>
</tr>
<tr>
<td>debug ip http ssi</td>
<td>Displays SSI translations and SSI ECHO command execution.</td>
</tr>
<tr>
<td>debug ip http transaction</td>
<td>Displays HTTP server transaction processing.</td>
</tr>
<tr>
<td>debug ip http url</td>
<td>Displays the URLs accessed from the router.</td>
</tr>
</tbody>
</table>
debug ip http transaction

To display HTTP server transaction processing, use the debug ip http transaction command in privileged EXEC mode. To disable debugging output, use the no form of this command.

deploy ip http transaction
no debug ip http transaction

Syntax Description
This command has no arguments or keywords.

Command Modes
Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td>
</tr>
</tbody>
</table>

Usage Guidelines
Use the debug ip http transaction command to display what the HTTP server is parsing at a high level. To display what the HTTP server is parsing at a low level, use the debug ip http token command.

Examples
The following is sample output from the debug ip http transaction command. In this example, the browser accessed the router’s home page http://router-name/.

```
Router# debug ip http transaction
HTTP: parsed uri '/'
HTTP: client version 1.1
HTTP: parsed extension Referer
HTTP: parsed line http://www.company.com/
HTTP: parsed extension Connection
HTTP: parsed line Keep-Alive
HTTP: parsed extension User-Agent
HTTP: parsed line Mozilla/2.01 (X11; I; FreeBSD 2.1.0-RELEASE i386)
HTTP: parsed extension Host
HTTP: parsed line router-name
HTTP: parsed extension Accept
HTTP: parsed line image/gif, image/x-xbitmap, image/jpeg, image/
HTTP: parsed extension Authorization
HTTP: parsed authorization type Basic
HTTP: received GET ''
```

The table below describes the significant fields shown in the display.

Table 26: debug ip http transaction Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP: parsed uri '/'</td>
<td>Uniform resource identifier that is requested.</td>
</tr>
<tr>
<td>HTTP: client version 1.1</td>
<td>Client HTTP version.</td>
</tr>
<tr>
<td>HTTP: parsed extension Referer</td>
<td>HTTP extension.</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
HTTP: received GET " | HTTP request method.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip http all</td>
<td>Displays authentication processes for all HTTP server processes on the system.</td>
</tr>
<tr>
<td>debug ip http authentication</td>
<td>Displays authentication processes for HTTP server and client access.</td>
</tr>
<tr>
<td>debug ip http ezsetup</td>
<td>Displays the configuration changes that occur during the EZ Setup process.</td>
</tr>
<tr>
<td>debug ip http token</td>
<td>Displays individual tokens parsed by the HTTP server.</td>
</tr>
<tr>
<td>debug ip http ssi</td>
<td>Displays SSI translations and SSI ECHO command execution.</td>
</tr>
<tr>
<td>debug ip http url</td>
<td>Displays the URLs accessed from the router.</td>
</tr>
</tbody>
</table>
**debug ip http url**

To show the URLs accessed from the router, use the `debug ip http url` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip http url
no debug ip http url
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ip http url` command to keep track of the URLs that are accessed and to determine from which hosts the URLs are accessed.

**Examples**

The following is sample output from the `debug ip http url` command. In this example, the HTTP server accessed the URLs and /exec. The output shows the URL being requested and the IP address of the host requesting the URL.

```
Router# debug ip http url
HTTP: processing URL '/' from host 172.31.2.141
HTTP: processing URL '/exec' from host 172.31.2.141
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ip http all</code></td>
<td>Displays authentication processes for all HTTP server processes on the system.</td>
</tr>
<tr>
<td><code>debug ip http authentication</code></td>
<td>Displays authentication processes for HTTP server and client access.</td>
</tr>
<tr>
<td><code>debug ip http ezsetup</code></td>
<td>Displays the configuration changes that occur during the EZ Setup process.</td>
</tr>
<tr>
<td><code>debug ip http ssi</code></td>
<td>Displays SSI translations and SSI ECHO command execution.</td>
</tr>
<tr>
<td><code>debug ip http token</code></td>
<td>Displays individual tokens parsed by the HTTP server.</td>
</tr>
<tr>
<td><code>debug ip http transaction</code></td>
<td>Displays HTTP server transaction processing.</td>
</tr>
</tbody>
</table>
**debug ip icmp**

To display information on Internal Control Message Protocol (ICMP) transactions, use the `debug ip icmp` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip icmp
no debug ip icmp
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

This command helps you determine whether the router is sending or receiving ICMP messages. Use it, for example, when you are troubleshooting an end-to-end connection problem.

**Note**


**Examples**

The following is sample output from the `debug ip icmp` command:

```
Router# debug ip icmp
ICMP: rcvd type 3, code 1, from 10.95.192.4
ICMP: src 10.56.0.202, dst 172.69.16.1, echo reply
ICMP: dst (10.120.1.0) port unreachable rcv from 10.120.1.15
ICMP: src 172.69.12.35, dst 172.69.20.7, echo reply
ICMP: dst (255.255.255.255) protocol unreachable rcv from 10.31.7.21
ICMP: dst (10.120.1.0) port unreachable rcv from 10.120.1.15
ICMP: dst (255.255.255.255) protocol unreachable rcv from 10.31.7.21
ICMP: dst (10.120.1.0) port unreachable rcv from 10.120.1.15
ICMP: src 10.56.0.202, dst 172.69.16.1, echo reply
ICMP: dst (10.120.1.0) port unreachable rcv from 10.120.1.15
ICMP: dst (255.255.255.255) protocol unreachable rcv from 10.31.7.21
ICMP: dst (10.120.1.0) port unreachable rcv from 10.120.1.15
ICMP: dst (255.255.255.255) protocol unreachable rcv from 10.31.7.21
ICMP: dst (10.120.1.0) port unreachable rcv from 10.120.1.15
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP:</td>
<td>Indication that this message describes an ICMP packet.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| rcvd type 3 | The type field can be one of the following:  
  • 0--Echo Reply  
  • 3--Destination Unreachable  
  • 4--Source Quench  
  • 5--Redirect  
  • 8--Echo  
  • 9--Router Discovery Protocol Advertisement  
  • 10--Router Discovery Protocol Solicitations  
  • 11--Time Exceeded  
  • 12--Parameter Problem  
  • 13--Timestamp  
  • 14--Timestamp Reply  
  • 15--Information Request  
  • 16--Information Reply  
  • 17--Mask Request  
  • 18--Mask Reply |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| code 1 | This field is a code. The meaning of the code depends upon the type field value, as follows:  
   - Echo and Echo Reply--The code field is always zero.  
   - Destination Unreachable--The code field can have the following values:  
     0--Network unreachable  
     1--Host unreachable  
     2--Protocol unreachable  
     3--Port unreachable  
     4--Fragmentation needed and DF bit set  
     5--Source route failed  
     - Source Quench--The code field is always 0.  
     - Redirect--The code field can have the following values:  
     0--Redirect datagrams for the network  
     1--Redirect datagrams for the host  
     2--Redirect datagrams for the command mode of service and network  
     3--Redirect datagrams for the command mode of service and host  
     - Router Discovery Protocol Advertisements and Solicitations--The code field is always zero.  
   - Time Exceeded--The code field can have the following values:  
     0--Time to live exceeded in transit  
     1--Fragment reassembly time exceeded  
   - Parameter Problem--The code field can have the following values:  
     0--General problem  
     1--Option is missing  
     2--Option missing, no room to add  
     - Timestamp and Timestamp Reply--The code field is always zero.  
     - Information Request and Information Reply--The code field is always zero.  
     - Mask Request and Mask Reply--The code field is always zero. |
| from 10.95.192.4 | Source address of the ICMP packet. |

The table below describes the significant fields shown in the second line of the display.
Table 28: debug ip icmp Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP:</td>
<td>Indicates that this message describes an ICMP packet.</td>
</tr>
<tr>
<td>src 10.56.10.202</td>
<td>Address of the sender of the echo.</td>
</tr>
<tr>
<td>dst 172.69.16.1</td>
<td>Address of the receiving router.</td>
</tr>
<tr>
<td>echo reply</td>
<td>Indicates that the router received an echo reply.</td>
</tr>
</tbody>
</table>

Other messages that the `debug ip icmp` command can generate follow.

When an IP router or host sends out an ICMP mask request, the following message is generated when the router sends a mask reply:

```
ICMP: sending mask reply (255.255.255.0) to 172.69.80.23 via Ethernet0
```

The following two lines are examples of the two forms of this message. The first form is generated when a mask reply comes in after the router sends out a mask request. The second form occurs when the router receives a mask reply with a nonmatching sequence and ID. Refer to Appendix I of RFC 950, Internet Standard Subnetting Procedures, for details.

```
ICMP: mask reply 255.255.255.0 from 172.69.80.31
ICMP: unexpected mask reply 255.255.255.0 from 172.69.80.32
```

The following output indicates that the router sent a redirect packet to the host at address 172.69.80.31, instructing that host to use the gateway at address 172.69.80.23 in order to reach the host at destination address 172.69.1.111:

```
ICMP: redirect sent to 172.69.80.31 for dest 172.69.1.111 use gw 172.69.80.23
```

The following message indicates that the router received a redirect packet from the host at address 172.69.80.23, instructing the router to use the gateway at address 172.69.80.28 in order to reach the host at destination address 172.69.81.34:

```
ICMP: redirect rcvd from 172.69.80.23 -- for 172.69.81.34 use gw 172.69.80.28
```

The following message is displayed when the router sends an ICMP packet to the source address (172.69.94.31 in this case), indicating that the destination address (172.69.13.33 in this case) is unreachable:

```
ICMP: dst (172.69.13.33) host unreachable sent to 172.69.94.31
```

The following message is displayed when the router receives an ICMP packet from an intermediate address (172.69.98.32 in this case), indicating that the destination address (172.69.13.33 in this case) is unreachable:

```
ICMP: dst (172.69.13.33) host unreachable rcv from 172.69.98.32
```

Depending on the code received (as the first table above describes), any of the unreachable messages can have any of the following “strings” instead of the “host” string in the message:

```
et
```
The following message is displayed when the TTL in the IP header reaches zero and a time exceed ICMP message is sent. The fields are self-explanatory.

ICMP: time exceeded (time to live) send to 10.95.1.4 (dest was 172.69.1.111)

The following message is generated when parameters in the IP header are corrupted in some way and the parameter problem ICMP message is sent. The fields are self-explanatory.

ICMP: parameter problem sent to 128.121.1.50 (dest was 172.69.1.111)

Based on the preceding information, the remaining output can be easily understood:

ICMP: parameter problem rcvd 172.69.80.32
ICMP: source quench rcvd 172.69.80.32
ICMP: source quench sent to 128.121.1.50 (dest was 172.69.1.111)
ICMP: sending time stamp reply to 172.69.80.45
ICMP: sending info reply to 172.69.80.12
ICMP: rdp advert rcvd type 9, code 0, from 172.69.80.23
ICMP: rdp solicit rcvd type 10, code 0, from 172.69.80.43
**debug ip igmp**

To display Internet Group Management Protocol (IGMP) packets received and sent, and IGMP-host related events, use the `debug ip igmp` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
depbug ip igmp [vrf vrf-name] [group-address]
no debug ip igmp [vrf vrf-name] [group-address]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf</code></td>
<td>(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td><code>vrf-name</code></td>
<td>(Optional) Name assigned to the VRF.</td>
</tr>
<tr>
<td><code>group-address</code></td>
<td>(Optional) Address of a particular group about which to display IGMP information.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(3)T</td>
<td>Fields were added to the output of this command to support the Source Specific Multicast (SSM) feature.</td>
</tr>
<tr>
<td>12.0(23)S</td>
<td>The <code>vrf</code> keyword and <code>vrf-name</code> argument were added.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>The <code>vrf</code> keyword and <code>vrf-name</code> argument were added.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.3(2)T</td>
<td>Fields were added to the output of this command to support the SSM Mapping feature. The <code>group-address</code> attribute was added.</td>
</tr>
<tr>
<td>12.2(18)SXD3</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXD3.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command helps discover whether the IGMP processes are functioning. In general, if IGMP is not working, the router process never discovers that another host is on the network that is configured to receive multicast packets. In dense mode, this situation will result in packets being delivered intermittently (a few every 3 minutes). In sparse mode, packets will never be delivered.

Use this command in conjunction with the `debug ip pim` and `debug ip mroute` commands to observe additional multicast activity and to learn the status of the multicast routing process, or why packets are forwarded out of particular interfaces.

When SSM mapping is enabled, a debug message is displayed to indicate that the router is converting an IGMP version 2 report from the group (G) into an IGMP version 3 join. After SSM mapping has generated
the appropriate IGMP version 3 report, any debug output that follows is seen as if the router had received the same IGMP version 3 report directly.

**Examples**

The following is sample output from the `debug ip igmp` command:

```
Router# debug ip igmp
IGMP: Received Host-Query from 172.16.37.33 (Ethernet1)
IGMP: Received Host-Report from 172.16.37.192 (Ethernet1) for 224.0.255.1
IGMP: Received Host-Report from 172.16.37.57 (Ethernet1) for 224.2.127.255
IGMP: Received Host-Report from 172.16.37.33 (Ethernet1) for 225.2.2.2
```

The messages displayed by the `debug ip igmp` command show query and report activity received from other routers and multicast group addresses.

The following is sample output from the `debug ip igmp` command when SSM is enabled. Because IGMP version 3 lite (IGMPv3lite) requires the host to send IGMP version 2 (IGMPv2) packets, IGMPv2 host reports also will be displayed in response to the router IGMPv2 queries. If SSM is disabled, the word “ignored” will be displayed in the `debug ip igmp` command output.

```
IGMP: Received v3-lite Report from 10.0.119.142 (Ethernet3/3), group count 1
IGMP: Received v3 Group Record from 10.0.119.142 (Ethernet3/3) for 232.10.10.10
IGMP: Update source 224.1.1.1
IGMP: Send v2 Query on Ethernet3/3 to 224.0.0.1
IGMP: Received v2 Report from 10.0.119.142 (Ethernet3/3) for 232.10.10.10
IGMP: Update source 224.1.1.1
```

The following is sample output from the `debug ip igmp` command when SSM static mapping is enabled. The following output indicates that the router is converting an IGMP version 2 join for group (G) into an IGMP version 3 join:

```
IGMP(0): Convert IGMPv2 report (*.232.1.2.3) to IGMPv3 with 2 source(s) using STATIC.
```

The following is sample output from the `debug ip igmp` command when SSM DNS-based mapping is enabled. The following output indicates that a DNS lookup has succeeded:

```
IGMP(0): Convert IGMPv2 report (*.232.1.2.3) to IGMPv3 with 2 source(s) using DNS.
```

The following is sample output from the `debug ip igmp` command when SSM DNS-based mapping is enabled and a DNS lookup has failed:

```
IGMP(0): DNS source lookup failed for (*. 232.1.2.3), IGMPv2 report failed
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ip mrm</code></td>
<td>Displays MRM control packet activity.</td>
</tr>
<tr>
<td><code>debug ip mrouter</code></td>
<td>Displays changes to the mroute table.</td>
</tr>
<tr>
<td><code>debug ip pim</code></td>
<td>Displays PIM packets received and sent and PIM-related events.</td>
</tr>
</tbody>
</table>
**debug ip igmp snooping**

To display debugging messages about Internet Group Management Protocol (IGMP) snooping services, use the `debug ip igmp snooping` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip igmp snooping {group | management | router | timer}
no debug ip igmp snooping {group | management | router | timer}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group</code></td>
<td>Displays debugging messages related to multicast groups.</td>
</tr>
<tr>
<td><code>management</code></td>
<td>Displays debugging messages related to IGMP management services.</td>
</tr>
<tr>
<td><code>router</code></td>
<td>Displays debugging messages related to the local router.</td>
</tr>
<tr>
<td><code>timer</code></td>
<td>Displays debugging messages related to the IGMP timer.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(6)EA2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)ZJ</td>
<td>This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows debugging messages for the IGMP snooping services being displayed:

```
Router# debug ip igmp snooping
IGMP snooping enabled
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip igmp snooping</code></td>
<td>Displays the IGMP snooping configuration.</td>
</tr>
</tbody>
</table>
debug ip igrp events

to display summary information on Interior Gateway Routing Protocol (IGRP) routing messages that indicate
the source and destination of each update, and the number of routes in each update, use the debug ip igrp
events command in privileged EXEC mode. To disable debugging output, use the no form of this command.

d debug ip igrp events [ip-address]
no debug ip igrp events [ip-address]

Syntax Description

<table>
<thead>
<tr>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

Usage Guidelines

If the IP address of an IGRP neighbor is specified, the resulting debug ip igrp events output includes messages
describing updates from that neighbor and updates that the router broadcasts toward that neighbor. Messages
are not generated for each route.

This command is particularly useful when there are many networks in your routing table. In this case, using
d debug ip igrp transactions could flood the console and make the router unusable. Use debug ip igrp events
instead to display summary routing information.

Examples

The following is sample output from the debug ip igrp events command:

```
router# debug ip igrp events

Updates sent
to these two
destination
direction

Updates received
from these source
direction

IGRP: sending update to 255.255.255.255 via Ethernet1 (160.89.33.8)
IGRP: Update contains 26 interior, 40 system, and 3 exterior routes.
IGRP: Total routes in update: 69

IGRP: sending update to 255.255.255.255 via Ethernet0 (160.85.32.8)
IGRP: Update contains 1 interior, 0 system, and 0 exterior routes.
IGRP: Total routes in update: 1

IGRP: received update from 160.89.32.24 on Ethernet0
IGRP: Update contains 17 interior, 1 system, and 0 exterior routes.
IGRP: Total routes in update: 18

IGRP: received update from 160.89.32.7 on Ethernet0
IGRP: Update contains 5 interior, 1 system, and 0 exterior routes.
IGRP: Total routes in update: 6
```

This shows that the router has sent two updates to the broadcast address 255.255.255.255. The router
also received two updates. Three lines of output describe each of these updates.

The first line indicates whether the router sent or received the update packet, the source or destination
address, and the interface through which the update was sent or received. If the update was sent, the
IP address assigned to this interface is shown (in parentheses).

```
IGRP: sending update to 255.255.255.255 via Ethernet1 (160.89.33.8)
```

The second line summarizes the number and types of routes described in the update:

```
IGRP: Update contains 26 interior, 40 system, and 3 exterior routes.
```

The third line indicates the total number of routes described in the update:
IGRP: Total routes in update: 69
debug ip igrp transactions

To display transaction information on Interior Gateway Routing Protocol (IGRP) routing transactions, use the `debug ip igrp transactions` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip igrp transactions [ip-address]
no debug ip igrp transactions [ip-address]
```

**Syntax Description**

- `ip-address` (Optional) The IP address of an IGRP neighbor.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

If the IP address of an IGRP neighbor is specified, the resulting `debug ip igrp transactions` output includes messages describing updates from that neighbor and updates that the router broadcasts toward that neighbor.

When many networks are in your routing table, the `debug ip igrp transactions` command can flood the console and make the router unusable. In this case, use the `debug ip igrp events` command instead to display summary routing information.

**Examples**

The following is sample output from the `debug ip igrp transactions` command:

```
Router# debug ip igrp transactions

Updates received from these two source addresses
IGRP: received update from 160.89.80.240 on Ethernet
  subnet 160.89.66.0, metric 1300 (neighbor 1230)
  subnet 160.89.56.0, metric 8676 (neighbor 9576)
  subnet 160.89.48.0, metric 1200 (neighbor 1130)
  subnet 160.89.50.0, metric 1300 (neighbor 1230)
  subnet 160.89.40.0, metric 8676 (neighbor 9576)
  network 192.68.151.0, metric 1185511 (neighbor 1185411)
  network 150.136.0.0, metric 16777215 (inaccessible)
  exterior network 128.140.0.0, metric 6676 (neighbor 9576)
  exterior network 140.222.0.0, metric 6676 (neighbor 9576)
IGRP: received update from 160.89.80.28 on Ethernet
  subnet 160.89.95.0, metric 180671 (neighbor 180571)
  subnet 160.89.61.0, metric 1200 (neighbor 1130)
  subnet 160.89.15.0, metric 16777215 (inaccessible)
 Updates sent to these two destination addresses
IGRP: sending update to 255.255.255.255 via Ethernet0 (160.89.64.31)
  subnet 160.89.94.0, metric=647
IGRP: sending update to 255.255.255.255 via Serial0 (160.88.90.31)
  subnet 160.89.80.0, metric=16777215
  subnet 160.89.64.0, metric=1130
```

The output shows that the router being debugged has received updates from two other routers on the network. The router at source address 160.89.80.240 sent information about ten destinations in the update; the router at source address 160.89.80.28 sent information about three destinations in its update. The router being debugged also sent updates—in both cases to the broadcast address 255.255.255.255 as the destination address.
On the second line the first field refers to the type of destination information: “subnet” (interior), “network” (system), or “exterior” (exterior). The second field is the Internet address of the destination network. The third field is the metric stored in the routing table and the metric advertised by the neighbor sending the information. “Metric inaccessible” usually means that the neighbor router has put the destination in a hold down state.

The entries show that the router is sending updates that are similar, except that the numbers in parentheses are the source addresses used in the IP header. A metric of 16777215 is inaccessible.

Other examples of output that the `debug ip igrp transactions` command can produce follow.

The following entry indicates that the routing table was updated and shows the new edition number (97 in this case) to be used in the next IGRP update:

```
IGRP: edition is now 97
```

Entries such as the following occur on startup or when some event occurs such as an interface making a transition or a user manually clearing the routing table:

```
IGRP: broadcasting request on Ethernet0
IGRP: broadcasting request on Ethernet1
```

The following type of entry can result when routing updates become corrupted between sending and receiving routers:

```
IGRP: bad checksum from 172.69.64.43
```

An entry such as the following should never appear. If it does, the receiving router has a bug in the software or a problem with the hardware. In either case, contact your technical support representative.

```
IGRP: system 45 from 172.69.64.234, should be system 109
```
debug ip inspect

Effective with Cisco IOS Release 12.4(20)T, the `debug ip inspect` command is replaced by the `debug policy-firewall` command. See the `debug policy-firewall` command for more information.

To display messages about Cisco IOS Firewall events, use the `debug ip inspect` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
default ip inspect {function-trace | object-creation | object-deletion | events | timers | protocol | detailed | update}
```

Firewall MIB Statistics Syntax
```
default ip inspect mib {object-creation | object-deletion | events | retrieval | update}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>mib</td>
<td>(Optional) Displays messages about MIB functionality.</td>
</tr>
<tr>
<td>function-trace</td>
<td>Displays messages about software functions called by the Cisco IOS Firewall.</td>
</tr>
<tr>
<td>object-creation</td>
<td>Displays messages about software objects being created by the Cisco IOS Firewall. Object creation corresponds to the beginning of Cisco IOS Firewall-inspected sessions.</td>
</tr>
<tr>
<td>object-deletion</td>
<td>Displays messages about software objects being deleted by the Cisco IOS Firewall. Object deletion corresponds to the closing of Cisco IOS Firewall-inspected sessions.</td>
</tr>
<tr>
<td>events</td>
<td>Displays messages about Cisco IOS Firewall software events, including information about Cisco IOS Firewall packet processing or MIB special events.</td>
</tr>
<tr>
<td>timers</td>
<td>Displays messages about Cisco IOS Firewall timer events such as when the Cisco IOS Firewall idle timeout is reached.</td>
</tr>
<tr>
<td>protocol</td>
<td>Displays messages about Cisco IOS Firewall-inspected protocol events, including details about the packets of the protocol. The table below provides a list of <code>protocol</code> keywords.</td>
</tr>
<tr>
<td>detailed</td>
<td>Displays detailed information to be displayed for all the other enabled Cisco IOS Firewall debugging. Use this form of the command in conjunction with other Cisco IOS Firewall debug commands.</td>
</tr>
<tr>
<td>retrieval</td>
<td>Displays messages of statistics requested via Simple Network Management Protocol (SNMP) or command-line interface (CLI).</td>
</tr>
<tr>
<td>update</td>
<td>Displays messages about Cisco IOS Firewall software updates or updates to MIB counters.</td>
</tr>
</tbody>
</table>

Table 29: Protocol Keywords for the debug ip inspect Command

<table>
<thead>
<tr>
<th>Application Protocol</th>
<th>Protocol Keyword</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport-layer protocols</td>
<td></td>
</tr>
<tr>
<td>Application Protocol</td>
<td>Protocol Keyword</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>ICMP</td>
<td>icmp</td>
</tr>
<tr>
<td>TCP</td>
<td>tcp</td>
</tr>
<tr>
<td>User Datagram Protocol (UDP)</td>
<td>udp</td>
</tr>
<tr>
<td>Application-layer protocols</td>
<td></td>
</tr>
<tr>
<td>CU-SeeMe</td>
<td>cuseeme</td>
</tr>
<tr>
<td>FTP commands and responses</td>
<td>ftp-cmd</td>
</tr>
<tr>
<td>FTP tokens (enables tracing of the FTP tokens parsed)</td>
<td>ftp-tokens</td>
</tr>
<tr>
<td>H.323 (version 1 and version 2)</td>
<td>h323</td>
</tr>
<tr>
<td>HTTP</td>
<td>http</td>
</tr>
<tr>
<td>IMAP</td>
<td>imap</td>
</tr>
<tr>
<td>Microsoft NetShow</td>
<td>netshow</td>
</tr>
<tr>
<td>POP3</td>
<td>pop3</td>
</tr>
<tr>
<td>RealAudio</td>
<td>realaudio</td>
</tr>
<tr>
<td>Remote procedure call (RPC)</td>
<td>rpc</td>
</tr>
<tr>
<td>Real Time Streaming Protocol (RTSP)</td>
<td>rtsp</td>
</tr>
<tr>
<td>Session Initiation Protocol (SIP)</td>
<td>sip</td>
</tr>
<tr>
<td>Simple Mail Transfer Protocol (SMTP)</td>
<td>smtp</td>
</tr>
<tr>
<td>Skinny Client Control Protocol (SCCP)</td>
<td>skinny</td>
</tr>
<tr>
<td>Structured Query Language<em>Net (SQL</em>Net)</td>
<td>sqlnet</td>
</tr>
<tr>
<td>StreamWorks</td>
<td>streamworks</td>
</tr>
<tr>
<td>TFTP</td>
<td>tftp</td>
</tr>
<tr>
<td>UNIX r-commands (rlogin, rexec, rsh)</td>
<td>rcmd</td>
</tr>
<tr>
<td>VDOLive</td>
<td>vdlive</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 P</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>12.0(5)T</td>
<td>NetShow support was added.</td>
</tr>
<tr>
<td>12.0(7)T</td>
<td>H.323 V2 and RTSP protocol support were added.</td>
</tr>
<tr>
<td>12.2(11)YU</td>
<td>Support for the ICMP and SIP protocols was added.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.3(1)</td>
<td>Support for the skinny protocol was added.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>Support for the IMAP and POP3 protocols was added.</td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>The MIB syntax was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was replaced by the <code>debug policy-firewall</code> command.</td>
</tr>
</tbody>
</table>

The following is sample output from the `debug ip inspect function-trace` command:

```
Router# debug ip inspect function-trace
*Mar 2 01:16:16: CBAC FUNC: insp_inspection
*Mar 2 01:16:16: CBAC FUNC: insp_pre_process_sync
*Mar 2 01:16:16: CBAC FUNC: insp_find_tcp_host_entry addr 40.0.0.1 bucket 41
*Mar 2 01:16:16: CBAC FUNC: insp_find_pregen_session
*Mar 2 01:16:16: CBAC FUNC: insp_get_idb
*Mar 2 01:16:16: CBAC FUNC: insp_get_idb
*Mar 2 01:16:16: CBAC FUNC: insp_get_idb
*Mar 2 01:16:16: CBAC FUNC: insp_create_sis
*Mar 2 01:16:16: CBAC FUNC: insp_inc_halfopen_sis
*Mar 2 01:16:16: CBAC FUNC: insp_link_session_to_hash_table
*Mar 2 01:16:16: CBAC FUNC: insp_inspect_pak
*Mar 2 01:16:16: CBAC FUNC: insp_l4_inspection
*Mar 2 01:16:16: CBAC FUNC: insp_process_tcp_seg
*Mar 2 01:16:16: CBAC FUNC: insp_listen_state
*Mar 2 01:16:16: CBAC FUNC: insp_ensure_return_traffic
*Mar 2 01:16:16: CBAC FUNC: insp_add_acl_item
*Mar 2 01:16:16: CBAC FUNC: insp_ensure_return_traffic
*Mar 2 01:16:16: CBAC FUNC: insp_add_acl_item
*Mar 2 01:16:16: CBAC FUNC: insp_process_syn_packet
*Mar 2 01:16:16: CBAC FUNC: insp_find.tcp_host_entry addr 40.0.0.1 bucket 41
*Mar 2 01:16:16: CBAC FUNC: insp_create tcp_host_entry
*Mar 2 01:16:16: CBAC FUNC: insp_fast inspection
*Mar 2 01:16:16: CBAC FUNC: insp_inspect_pak
*Mar 2 01:16:16: CBAC FUNC: insp_l4_inspection
*Mar 2 01:16:16: CBAC FUNC: insp_process tcp_seg
*Mar 2 01:16:16: CBAC FUNC: insp_synrcvd_state
*Mar 2 01:16:16: CBAC FUNC: insp_fast inspection
*Mar 2 01:16:16: CBAC FUNC: insp_inspect_pak
*Mar 2 01:16:16: CBAC FUNC: insp_l4_inspection
*Mar 2 01:16:16: CBAC FUNC: insp_process tcp_seg
*Mar 2 01:16:16: CBAC FUNC: insp_synrcvd_state
*Mar 2 01:16:16: CBAC FUNC: insp_dec_halfopen_sis
*Mar 2 01:16:16: CBAC FUNC: insp_remove_sis_from_host_entry
*Mar 2 01:16:16: CBAC FUNC: insp_find.tcp_host_entry addr 40.0.0.1 bucket 41
```
This output shows the functions called by the Cisco IOS Firewall as a session is inspected. Entries with an asterisk (*) after the word “CBAC” are entries when the fast path is used; otherwise, the process path is used.

The following is sample output from the `debug ip inspect object-creation` and `debug ip inspect object-deletion` commands:

```
Router# debug ip inspect object-creation
Router# debug ip inspect object-deletion
*Mar 2 01:18:30: CBAC OBJ_CREATE: create pre-gen sis 25A3574
*Mar 2 01:18:30: CBAC OBJ_CREATE: create acl wrapper 25A36FC -- acl item 25A3634
*Mar 2 01:18:30: CBAC OBJ_CREATE: create sis 25C1CC4
*Mar 2 01:18:30: CBAC OBJ_DELETE: delete pre-gen sis 25A3574
*Mar 2 01:18:30: CBAC OBJ_CREATE: create host entry 25A3574 addr 10.0.0.1 bucket 31
*Mar 2 01:18:30: CBAC OBJ_DELETE: delete sis 25C1CC4
*Mar 2 01:18:30: CBAC OBJ_DELETE: delete create acl wrapper 25A36FC -- acl item 25A3634
*Mar 2 01:18:31: CBAC OBJ_DELETE: delete host entry 25A3574 addr 10.0.0.1
```

The following is sample output from the `debug ip inspect object-creation`, `debug ip inspect object-deletion`, and `debug ip inspect events` commands:

```
Router# debug ip inspect object-creation
Router# debug ip inspect object-deletion
Router# debug ip inspect events
*Mar 2 01:18:51: CBAC OBJ_CREATE: create pre-gen sis 25A3574
*Mar 2 01:18:51: CBAC OBJ_CREATE: create acl wrapper 25A36FC -- acl item 25A3634
*Mar 2 01:18:51: CBAC Src 10.1.0.1 Port [1:65535]
*Mar 2 01:18:51: CBAC Dst 10.0.0.1 Port [46406:46406]
*Mar 2 01:18:51: CBAC OBJ_CREATE: create sis 25C1CC4
*Mar 2 01:18:51: CBAC OBJ_CREATE: create sis 25C1CC4 initiator_addr (10.1.0.1:20) responder_addr (30.0.0.1:46406) initiator_alt_addr (40.0.0.1:20) responder_alt_addr (10.0.0.1:46406)
*Mar 2 01:18:51: CBAC OBJ_DELETE: delete pre-gen sis 25A3574
*Mar 2 01:18:51: CBAC OBJ_CREATE: create sis 25C1CC4
*Mar 2 01:18:51: CBAC OBJ_DELETE: delete host entry 25A3574 addr 10.0.0.1 bucket 31
*Mar 2 01:18:51: CBAC OBJ_DELETE: delete sis 25C1CC4
*Mar 2 01:18:51: CBAC OBJ_DELETE: delete create acl wrapper 25A36FC -- acl item 25A3634
*Mar 2 01:18:51: CBAC OBJ_DELETE: delete host entry 25A3574 addr 10.0.0.1
```

The following is sample output from the `debug ip inspect timers` command:

```
Router# debug ip inspect timers
*Mar 2 01:19:15: CBAC Timer Init Leaf: Pre-gen sis 25A3574
*Mar 2 01:19:15: CBAC Timer Init Leaf: sis 25C1CC4
*Mar 2 01:19:15: CBAC Timer Start: sis 25C1CC4 Timer: 25C1D5C Time: 3600000 milisecs
*Mar 2 01:19:15: CBAC Timer Stop: sis 25C1CC4 Timer: 25C1D5C
```

The following is sample output from the `debug ip inspect tcp` command:

```
Router# debug ip inspect tcp
*Mar 2 01:20:43: CBAC* sis 25A3604 pak 2541C58 TCP P ack 4223720032 seq 4200176225(22) (10.0.0.1:46409) => (10.1.0.1:21)
*Mar 2 01:20:43: CBAC sis 25A3604 pak 2541C58 TCP P ack 4223720032 seq 4200176225(22) (10.0.0.1:46409) => (10.1.0.1:21)
*Mar 2 01:20:43: CBAC* sis 25A3604 pak 2544374 TCP P ack 4200176247 seq 4223720032(30) (10.0.0. 1:46409) <= (10.1.0.1:21)
```
This sample shows TCP packets being processed and lists the corresponding acknowledge (ACK) packet numbers and sequence (SEQ) numbers. The number of data bytes in the TCP packet is shown in parentheses—for example, (22). For each packet shown, the addresses and port numbers are shown separated by a colon. For example, (10.1.0.1:21) indicates an IP address of 10.1.0.1 and a TCP port number of 21.

Entries with an asterisk (*) after the word “CBAC” are entries when the fast path is used; otherwise, the process path is used.

The following is sample output from the `debug ip inspect tcp` and `debug ip inspect detailed` commands:

```
Router# debug ip inspect tcp
Router# debug ip inspect detailed
```

```
*Mar 2 01:20:58: CBAC* Pak 2541E38 Find session for (30.0.0.1:46409) (40.0.0.1:21) tcp
*Mar 2 01:20:58: Pak 4223720160 seq 4200176262(22) (30.0.0.1:46409) => (40.0.0.1:21)
*Mar 2 01:20:58: CBAC* Pak 2541E38 Addr:port pairs to match: (30.0.0.1:46409) (40.0.0.1:21)
*Mar 2 01:20:58: CBAC* sis 25A3604 SIS_OPEN
*Mar 2 01:20:58: CBAC* Pak 2541E38 IP: s=30.0.0.1 (Ethernet0), d=40.0.0.1 (Ethernet1), len 76, proto=6
*Mar 2 01:20:58: CBAC sis 25A3604 Saving State: SIS_OPEN/ESTAB iisn 4200176160 i_rcvnxt 4223719771 i_sndnxt 4200176262 i_rcvwnd 8760 r_sndnxt 4223719771 r_rcvwnd 8760
*Mar 2 01:20:58: CBAC* pak 2541E38 TCP S seq 4200176262(22) Flags: ACK 4223720160 PSH
*Mar 2 01:20:58: CBAC* sis 25A3604 pak 2541E38 TCP S ack 4223720160 seq 4200176262(22)
*Mar 2 01:20:58: CBAC* sis 25A3604 L4 inspect result: PASS packet 2541E38 (30.0.0.1:46409) (40.0.0.1:21) bytes 22 ftp
```

The following is sample output from the `debug ip inspect icmp` and `debug ip inspect detailed` commands:

```
Router# debug ip inspect icmp
Router# debug ip inspect detailed
```

```
*Mar 2 01:20:58: CBAC* sis 81073F0C SIS_CLOSED
```

This sample shows TCP packets being processed and lists the corresponding acknowledge (ACK) packet numbers and sequence (SEQ) numbers. The number of data bytes in the TCP packet is shown in parentheses—for example, (22). For each packet shown, the addresses and port numbers are shown separated by a colon. For example, (10.1.0.1:21) indicates an IP address of 10.1.0.1 and a TCP port number of 21.

Entries with an asterisk (*) after the word “CBAC” are entries when the fast path is used; otherwise, the process path is used.

The following is sample output from the `debug ip inspect tcp` and `debug ip inspect detailed` commands:

```
Router# debug ip inspect tcp
Router# debug ip inspect detailed
```

```
*Mar 2 01:20:58: CBAC* Pak 2541E38 Find session for (30.0.0.1:46409) (40.0.0.1:21) tcp
*Mar 2 01:20:58: Pak 4223720160 seq 4200176262(22) (30.0.0.1:46409) => (40.0.0.1:21)
*Mar 2 01:20:58: CBAC* Pak 2541E38 Addr:port pairs to match: (30.0.0.1:46409) (40.0.0.1:21)
*Mar 2 01:20:58: CBAC* sis 25A3604 SIS_OPEN
*Mar 2 01:20:58: CBAC* Pak 2541E38 IP: s=30.0.0.1 (Ethernet0), d=40.0.0.1 (Ethernet1), len 76, proto=6
*Mar 2 01:20:58: CBAC sis 25A3604 Saving State: SIS_OPEN/ESTAB iisn 4200176160 i_rcvnxt 4223719771 i_sndnxt 4200176262 i_rcvwnd 8760 r_sndnxt 4223719771 r_rcvwnd 8760
*Mar 2 01:20:58: CBAC* pak 2541E38 TCP S seq 4200176262(22) Flags: ACK 4223720160 PSH
*Mar 2 01:20:58: CBAC* sis 25A3604 pak 2541E38 TCP S ack 4223720160 seq 4200176262(22)
*Mar 2 01:20:58: CBAC* sis 25A3604 L4 inspect result: PASS packet 2541E38 (30.0.0.1:46409) (40.0.0.1:21) bytes 22 ftp
*Mar 2 01:20:58: CBAC* sis 25A3604 Restoring State: SIS_OPEN/ESTAB iisn 4200176160 i_rcvnxt 4223720160 i_sndnxt 4200176262 i_rcvwnd 8760 r_sndnxt 4223719771 r_rcvwnd 8760
*Mar 2 01:20:58: CBAC* Bump up: inspection requires the packet in the process path(30.0.0.1) (40.0.0.1) (40.0.0.1) (40.0.0.1)
```

The following is sample output from the `debug ip inspect icmp` and `debug ip inspect detailed` commands:

```
Router# debug ip inspect icmp
Router# debug ip inspect detailed
```

```
*Mar 2 01:20:58: CBAC* sis 81073F0C SIS_CLOSED
```
l1w6d:CBAC Pak 80D2E9EC IP:s=192.168.133.3 (Ethernet1), d=0.0.0.0 (Ethernet0), len 98, proto=1
l1w6d:CBAC ICMP:sis 81073F0C pak 80D2E9EC SIS_CLOSED ICMP packet (192.168.133.3:0) =>
(0.0.0.0:0) datalen 56
l1w6d:CBAC ICMP:start session from 192.168.133.3
l1w6d:CBAC sis 81073F0C --> SIS_OPENING (192.168.133.3:0) (0.0.0.0:0)
l1w6d:CBAC sis 81073F0C L4 inspect result:PASS packet 80D2E9EC (192.168.133.3:0) (0.0.0.0:0)
bytes 56 icmp
l1w6d:CBAC sis 81073F0C SIS_OPENING
l1w6d:CBAC Pak 80E72BFC IP:s=0.0.0.0 (Ethernet0), d=192.168.133.3 (Ethernet1), len 98, proto=1
l1w6d:CBAC ICMP:sis 81073F0C pak 80E72BFC SIS_OPENING ICMP packet (192.168.133.3:0) <=
(0.0.0.0:0) datalen 56
l1w6d:CBAC sis 81073F0C --> SIS_OPEN (192.168.133.3:0) (0.0.0.0:0)
l1w6d:CBAC sis 81073F0C L4 inspect result:PASS packet 80E72BFC (0.0.0.0:0) (192.168.133.3:0)
bytes 56 icmp
l1w6d:CBAC* sis 81073F0C SIS_OPEN
l1w6d:CBAC* Pak 80D2F2C8 IP:s=192.168.133.3 (Ethernet1), d=0.0.0.0 (Ethernet0), len 98,
proto=1
l1w6d:CBAC* ICMP:sis 81073F0C pak 80D2F2C8 SIS_OPEN ICMP packet (192.168.133.3:0) =>
(0.0.0.0:0) datalen 56
l1w6d:CBAC* sis 81073F0C --> SIS_OPEN (192.168.133.3:0) (0.0.0.0:0)
l1w6d:CBAC* sis 81073F0C L4 inspect result:PASS packet 80D2F2C8 (192.168.133.3:0) (0.0.0.0:0)
bytes 56 icmp
l1w6d:CBAC* sis 81073F0C SIS_OPEN
l1w6d:CBAC* Pak 80E737CC IP:s=0.0.0.0 (Ethernet0), d=192.168.133.3 (Ethernet1), len 98,
proto=1
l1w6d:CBAC* ICMP:sis 81073F0C pak 80E737CC SIS_OPEN ICMP packet (192.168.133.3:0) <=
(0.0.0.0:0) datalen 56
l1w6d:CBAC* sis 81073F0C --> SIS_OPEN (192.168.133.3:0) (0.0.0.0:0)
l1w6d:CBAC* sis 81073F0C L4 inspect result:PASS packet 80E737CC (0.0.0.0:0) (192.168.133.3:0)
bytes 56 icmp
l1w6d:CBAC* sis 81073F0C SIS_OPEN
l1w6d:CBAC* Pak 80F554F0 IP:s=192.168.133.3 (Ethernet1), d=0.0.0.0 (Ethernet0), len 98,
proto=1
l1w6d:CBAC* ICMP:sis 81073F0C pak 80F554F0 SIS_OPEN ICMP packet (192.168.133.3:0) =>
(0.0.0.0:0) datalen 56
l1w6d:CBAC* sis 81073F0C --> SIS_OPEN (192.168.133.3:0) (0.0.0.0:0)
l1w6d:CBAC* sis 81073F0C L4 inspect result:PASS packet 80F554F0 (192.168.133.3:0) (0.0.0.0:0)
bytes 56 icmp
l1w6d:CBAC* sis 81073F0C SIS_OPEN
l1w6d:CBAC* Pak 80E73AC0 IP:s=0.0.0.0 (Ethernet0), d=192.168.133.3 (Ethernet1), len 98,
proto=1
l1w6d:CBAC* ICMP:sis 81073F0C pak 80E73AC0 SIS_OPEN ICMP packet (192.168.133.3:0) <=
(0.0.0.0:0) datalen 56
l1w6d:CBAC* sis 81073F0C --> SIS_OPEN (192.168.133.3:0) (0.0.0.0:0)
l1w6d:CBAC* sis 81073F0C L4 inspect result:PASS packet 80E73AC0 (0.0.0.0:0) (192.168.133.3:0)
bytes 56 icmp
l1w6d:CBAC* sis 81073F0C SIS_OPEN
l1w6d:CBAC* Pak 80E73AC0 IP:s=0.0.0.0 (Ethernet0), d=192.168.133.3 (Ethernet1), len 98,
proto=1
l1w6d:CBAC* ICMP:sis 81073F0C pak 80E73AC0 SIS_OPEN ICMP packet (192.168.133.3:0) <=
(0.0.0.0:0) datalen 56
l1w6d:CBAC* sis 81073F0C --> SIS_OPEN (192.168.133.3:0) (0.0.0.0:0)
l1w6d:CBAC* sis 81073F0C L4 inspect result:PASS packet 80E73AC0 (0.0.0.0:0) (192.168.133.3:0)
bytes 56 icmp
debug ip inspect ha

To display messages about Cisco IOS stateful failover high availability (HA) events, use the `debug ip inspect ha` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip inspect ha [manager | packet | update]
no debug ip inspect ha [manager | packet | update]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>manager</td>
<td>(Optional) Displays detailed messages for interaction of firewall HA manager with the box-to-box high availability infrastructure.</td>
</tr>
<tr>
<td>packet</td>
<td>(Optional) Used to debug the processing of the first packet post-failover on the new active device.</td>
</tr>
<tr>
<td>update</td>
<td>(Optional) Used to debug the periodic update messages between the active and standby. The Firewall HA sends periodical messages to update the standby of the firewall sessions state on the active.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip inspect ha` command. This example shows an add session message and a delete session message received by the the active and standby devices:

```
Router# debug ip inspect ha
Active debugs -
*Apr 13 17:15:20.795: FW-HA:Send add session msg for session 2C6B820
*Apr 13 17:15:36.919: FW-HA:Send delete session msg for session 2C6B820
Standby debugs -
*Apr 13 17:19:00.471: FW-HA:Received add session message
(10.0.0.10:56733:0)=>(11.0.0.10:23:0)
*Apr 13 17:19:12.051: FW-HA:Received delete session message
(10.0.0.10:56733:0)=>(11.0.0.10:23:0)
```

The following is sample output from the `debug ip inspect ha manager` command. Using the `manager` keyword provides a more detailed debug analysis:

```
Router# debug ip inspect ha manager
*Apr 13 17:23:28.995: HA Message 0:flags=0x01 len=727 FW_HA_MSG_INSERT_SESSION (1)
*Apr 13 17:23:28.995: ID: grp1
*Apr 13 17:23:28.995: attr FW_HA_ATT_INITIATOR_ADDR (1) len 4
*Apr 13 17:23:28.995: 0A 00 00 0A
*Apr 13 17:23:28.995: attr FW_HA_ATT_RESPONDER_ADDR (2) len 4
```
# debug ip inspect L2-transparent

To enable debugging messages for transparent firewall events, use the `debug ip inspect L2-transparent` command in privileged EXEC mode. To disable debugging messages, use the `no` form of this command.

```bash
debug ip inspect L2-transparent {packet | dhcp-passthrough}
no debug ip inspect L2-transparent {packet | dhcp-passthrough}
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>packet</code></td>
<td>Displays messages for all debug packets that are inspected by the transparent firewall.</td>
</tr>
<tr>
<td><code>Note</code></td>
<td>Only IP packets (TCP, User Datagram Protocol [UDP], and Internet Control Management Protocol [ICMP]) are subjected to inspection by the transparent firewall.</td>
</tr>
<tr>
<td><code>dhcp-passthrough</code></td>
<td>Displays debug messages only for DHCP pass-through traffic that the transparent firewall forwards across the bridge.</td>
</tr>
<tr>
<td><code>To allow a transparent firewall to forward DHCP pass-through traffic, use the ip inspect L2-transparent dhcp-passthrough command.</code></td>
<td></td>
</tr>
</tbody>
</table>

## Command Modes

Privileged EXEC

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

The `debug ip inspect L2-transparent` command can be used to help verify and troubleshoot transparent firewall-related configurations, such as a Telnet connection from the client to the server with inspection configured.

## Examples

The following example shows how the transparent firewall debug command works in a basic transparent firewall configuration. (Note that each debug message is preceded by an asterisk (*).)

```bash
! Enable debug commands.
Router# debug ip inspect L2-transparent packet
INSPECT L2 firewall debugging is on
Router# debug ip inspect object-creation
INSPECT Object Creations debugging is on
Router# debug ip inspect object-deletion
INSPECT Object Deletions debugging is on
! Start the transparent firewall configuration process
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
! Configure bridging
Router(config)# bridge 1 protocol ieee
Router(config)# bridge 1nb
Router(config)# bridge 1 route ip
Router(config)# interface bvi1
*Mar  1 00:06:42.511:LIB-3-UPDOWN:Interface BV1, changed state to down.
Router(config-if)# ip address 209.165.200.225 255.255.255.254
```
! Configure inspection
Router(config)# ip inspect name test tcp
! Following debugs show the memory allocated for CBAC rules.
*Mar 1 00:07:21.127:CBAC OBJ_CREATE:create irc 817F04F0 (test)
*Mar 1 00:07:21.127:CBAC OBJ_CREATE:create irt 818AED20 Protocol:tcp Inactivity time:0
Router(config)# ip inspect name test icmp
Router(config)#
*Mar 1 00:07:39.211:CBAC OBJ_CREATE:create irt 818AEDCC Protocol:icmp Inactivity time:0
! Configure Bridging on ethernet0 interface
Router(config)# interface ethernet0
Router(config-if)# bridge-group 1
*Mar 1 00:07:49.071:%LINK-3-UPDOWN:Interface BVI1, changed state to up
*Mar 1 00:07:50.071:%LINEPROTO-5-UPDOWN:Line protocol on Interface BVI1, changed state to up
! Configure inspection on ethernet0 interface
Router(config-if)# ip inspect test in
Router(config-if)#
*Mar 1 00:07:57.543:CBAC OBJ_CREATE:create idbsb 8189CBFC (Ethernet0)
! Incremented the number of bridging interfaces configured for inspection */
*Mar 1 00:07:57.543:L2FW:Incrementing L2FW i/f count
Router(config-if)# interface ethernet1
! Configure bridging and ACL on interface ethernet1
Router(config-if)# bridge-group 1
Router(config-if)# ip access-group 101 in
*Mar 1 00:08:26.711:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet1, changed state to up
Router(config-if)# end

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip inspect L2-transparent dhcp-passthrough</strong></td>
<td>Allows a transparent firewall to forward DHCP pass-through traffic.</td>
</tr>
</tbody>
</table>
**debug ip ips**

To enable debugging messages for Cisco IOS Intrusion Prevention System (IPS), use the `debug ip ips` command in privileged EXEC mode. To disable debugging messages, use the `no` form of this command.

```
debug ip ips [engine] [detailed] [service-msrpc] [service-sm]
o no debug ip ips [engine] [detailed]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>engine</td>
<td>(Optional) Displays debugging messages only for a specific signature engine.</td>
</tr>
<tr>
<td>detailed</td>
<td>(Optional) Displays detailed debugging messages for the specified signature engine or for all IPS actions.</td>
</tr>
<tr>
<td>service-msrpc</td>
<td>(Optional) Displays debugging messages for Microsoft RPC (Remote Procedure Call) (MSRPC) actions.</td>
</tr>
<tr>
<td>service-sm</td>
<td>(Optional) Displays debugging messages for Microsoft SMB (Server Message Block) actions.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(15)T</td>
<td>The <code>service-msrpc</code> and the <code>service-sm</code> keywords were added to support Microsoft communication protocols MSRPC and SMB.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable debugging messages for the Cisco IOS IPS:

```
Router# debug ip ips
```
debug ip mbgp dampening

To log route flap dampening activity related to multiprotocol Border Gateway Protocol (BGP), use the `debug ip mbgp dampening` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
depug ip mbgp dampening [access-list-number]
no debug ip mbgp dampening [access-list-number]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list-number</code></td>
<td>(Optional) The number of an access list in the range from 1 to 99. If an access list number is specified, debugging occurs only for the routes permitted by the access list.</td>
</tr>
</tbody>
</table>

| Command Default | Logging for route flap dampening activity is not enabled. |
| Command Modes | Privileged EXEC |
| Command History | |
| **Release** | **Modification** |
| 11.1(20)CC | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

<table>
<thead>
<tr>
<th>Examples</th>
<th>The following is sample output from the <code>debug ip mbgp dampening</code> command:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router#</td>
<td><code>debug ip mbgp dampening</code></td>
</tr>
<tr>
<td>BGP: charge penalty for 173.19.0.0/16 path 49 with halflife-time 15 reuse/suppress 750/2000</td>
<td></td>
</tr>
<tr>
<td>BGP: flapped 1 times since 00:00:00. New penalty is 1000</td>
<td></td>
</tr>
<tr>
<td>BGP: charge penalty for 173.19.0.0/16 path 19 49 with halflife-time 15 reuse/suppress 750/2000</td>
<td></td>
</tr>
<tr>
<td>BGP: flapped 1 times since 00:00:00. New penalty is 1000</td>
<td></td>
</tr>
</tbody>
</table>
debug ip mbgp updates

To log multiprotocol Border Gateway Protocol (BGP)-related information passed in BGP update messages, use the **debug ip mbgp updates** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ip mbgp updates**
**no debug ip mbgp updates**

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Logging for multiprotocol BGP-related information in BGP update messages is not enabled.

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1(20)CC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**
The following is sample output from the **debug ip mbgp updates** command:

```
Router# debug ip mbgp updates
BGP: NEXT_HOP part 1 net 200.10.200.0/24, neigh 171.69.233.49, next 171.69.233.34
BGP: 171.69.233.49 send UPDATE 200.10.200.0/24, next 171.69.233.34, metric 0, path 33 34
    19 49 109 65000 297 1239 1800 3597
BGP: NEXT_HOP part 1 net 200.10.202.0/24, neigh 171.69.233.49, next 171.69.233.34
BGP: 171.69.233.49 send UPDATE 200.10.202.0/24, next 171.69.233.34, metric 0, path 33 34
    19 49 109 65000 297 1239 1800 3597
BGP: NEXT_HOP part 1 net 200.10.228.0/22, neigh 171.69.233.49, next 171.69.233.34
BGP: 171.69.233.49 rcv UPDATE about 222.2.2.0/24, next hop 171.69.233.49, path 49 109 metric 0
BGP: 171.69.233.49 rcv UPDATE about 131.103.0.0/16, next hop 171.69.233.49, path 49 109 metric 0
BGP: 171.69.233.49 rcv UPDATE about 206.205.242.0/24, next hop 171.69.233.49, path 49 109 metric 0
BGP: 171.69.233.49 rcv UPDATE about 1.0.0.0/8, next hop 171.69.233.49, path 49 19 metric 0
BGP: 171.69.233.49 rcv UPDATE about 198.1.2.0/24, next hop 171.69.233.49, path 49 19 metric 0
BGP: 171.69.233.49 rcv UPDATE about 171.69.0.0/16, next hop 171.69.233.49, path 49 metric 0
BGP: 171.69.233.49 rcv UPDATE about 172.19.0.0/16, next hop 171.69.233.49, path 49 metric 0
BGP: nettable_walker 172.19.0.0/255.255.0.0 calling revise_route
BGP: revise route installing 172.19.0.0/255.255.0.0 -> 171.69.233.49
BGP: 171.69.233.19 computing updates, neighbor version 267099, table version 267100, starting at 0.0.0.0
BGP: NEXT_HOP part 1 net 172.19.0.0/16, neigh 171.69.233.19, next 171.69.233.49
BGP: 171.69.233.19 send UPDATE 172.19.0.0/16, next 171.69.233.49, metric 0, path 33 49
BGP: 1 updates (average = 46, maximum = 46)
BGP: 171.69.233.19 updates replicated for neighbors: 171.69.233.34, 171.69.233.49, 171.69.233.56
BGP: 171.69.233.19 1 updates enqueued (average=46, maximum=46)
```
BGP: 171.69.233.19 update run completed, ran for 0ms, neighbor version 267099, start version 267100, throttled to 267100, check point net 0.0.0.0
debug ip mcache

**Note**
Effective with Cisco IOS Release 15.0(1)M and Cisco IOS Release 12.2(33)SRE, the `debug ip mcache` command is not available in Cisco IOS software.

To display IP multicast fast-switching events, use the `debug ip mcache` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip mcache [vrf vrf-name] [{hostnamegroup-address}]
no debug ip mcache [vrf vrf-name] [{hostnamegroup-address}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vrf</th>
<th>(Optional) Supports the Multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vrf-name</td>
<td>(Optional) Name assigned to the VRF.</td>
</tr>
<tr>
<td></td>
<td>hostname</td>
<td>(Optional) The host name.</td>
</tr>
<tr>
<td></td>
<td>group-address</td>
<td>(Optional) The group address.</td>
</tr>
</tbody>
</table>

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(23)S</td>
<td>The <code>vrf</code> keyword and <code>vrf-name</code> argument were added.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was removed.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was removed.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use this command when multicast fast switching appears not to be functioning.

**Examples**
The following is sample output from the `debug ip mcache` command when an IP multicast route is cleared:

```
Router# debug ip mcache
```
IP multicast fast-switching debugging is on

Router# clear ip mroute *
MRC: Build MAC header for (172.31.60.185/32, 224.2.231.173), Ethernet0
MRC: Fast-switch flag for (172.31.60.185/32, 224.2.231.173), off -> on, caller
ip_mroute_replicate-1
MRC: Build MAC header for (172.31.191.10/32, 224.2.127.255), Ethernet0
MRC: Build MAC header for (172.31.60.152/32, 224.2.231.173), Ethernet0

The table below describes the significant fields shown in the display.

Table 30: debug ip mcache Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRC</td>
<td>Multicast route cache.</td>
</tr>
<tr>
<td>Fast-switch flag</td>
<td>Route is fast switched.</td>
</tr>
<tr>
<td>(172.31.60.185/32)</td>
<td>Host route with 32 bits of mask.</td>
</tr>
<tr>
<td>off -&gt; on</td>
<td>State has changed.</td>
</tr>
<tr>
<td>caller ...</td>
<td>The code function that activated the state change.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip dvmrp</td>
<td>Displays information on DVMRP packets received and sent.</td>
</tr>
<tr>
<td>debug ip igmp</td>
<td>Displays IGMP packets received and sent, and IGMP-host related events.</td>
</tr>
<tr>
<td>debug ip igrp transactions</td>
<td>Displays transaction information on IGRP routing transactions.</td>
</tr>
<tr>
<td>debug ip mrm</td>
<td>Displays MRM control packet activity.</td>
</tr>
<tr>
<td>debug ip sd</td>
<td>Displays all SD announcements received.</td>
</tr>
</tbody>
</table>
debug ip mds ipc

To debug multicast distributed switching (MDS) interprocessor communication, that is, synchronization between the Multicast Forwarding Information Base (MFIB) on the line card and the multicast routing table in the Route Processor (RP), use the `debug ip mds ipc` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip mds ipc {event | packet}
no debug ip mds ipc {event | packet}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>event</td>
<td>Displays MDS events when there is a problem.</td>
</tr>
<tr>
<td>packet</td>
<td>Displays MDS packets.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Usage Guidelines**

Use this command on the line card or RP.

**Examples**

The following is sample output from the `debug ip mds ipc packet` command:

```
Router# debug ip mds ipc packet
MDFS: ipc packet debugging is on
Router#
MDFS: LC sending statistics message to RP with code 0 of size 36
MDFS: LC sending statistics message to RP with code 1 of size 680
MDFS: LC sending statistics message to RP with code 2 of size 200
MDFS: LC sending statistics message to RP with code 3 of size 152
MDFS: LC sending window message to RP with code 36261 of size 8
MDFS: LC received IPC packet of size 60 sequence 36212
```

The following is sample output from the `debug ip mds ipc event` command:

```
Router# debug ip mds ipc event
MDFS: LC received invalid sequence 21 while expecting 20
```
debug ip mds mevent

To debug Multicast Forwarding Information Base (MFIB) route creation, route updates, and so on, use the debug ip mds mevent command in privileged EXEC mode. To disable debugging output, use the no form of this command.

**debug ip mds mevent**

**no debug ip mds mevent**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

Use this command on the line card.

**Examples**

The following is sample output from the debug ip mds mevent command:

```
Router# debug ip mds mevent
MDFS mroute event debugging is on
Router#clear ip mdfs for *
Router# MDFS: Create (*, 239.255.255.255)
MDFS: Create (192.168.1.1/32, 239.255.255.255), RPF POS2/0/0
MDFS: Add OIF for mroute (192.168.1.1/239.255.255.255) on Fddi0/0/0
MDFS: Create (*, 224.2.127.254)
MDFS: Create (192.168.1.1/32, 224.2.127.254), RPF POS2/0/0
MDFS: Add OIF for mroute (192.168.1.1/224.2.127.254) on Fddi0/0/0
MDFS: Create (128.9.160.67/32, 224.2.127.254), RPF POS2/0/0
```
To debug multicast distributed switching (MDS) events such as packet drops, interface drops, and switching failures, use the `debug ip mds mpacket` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
deploy ip mds mpacket
no debug ip mds mpacket
```

**Syntax Description**
This command has no arguments or keywords.

**Command Modes**
Privileged EXEC

**Usage Guidelines**
Use this command on the line card.
**debug ip mds process**

To debug line card process level events, use the `debug ip mds process` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip mds process
no debug ip mds process
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

Use this command on the line card or Route Processor (RP).

**Examples**

The following is sample output from the `debug ip mds process` command:

```
Router# debug ip mds process
MDFS process debugging is on
Mar 19 16:15:47.448: MDFS: RP queueing mdb message for (210.115.194.5, 224.2.127.254) to all linecards
Mar 19 16:15:47.448: MDFS: RP queueing midb message for (210.115.194.5, 224.2.127.254) to all linecards
Mar 19 16:15:47.628: MDFS: RP servicing low queue for LC in slot 0
Mar 19 16:15:47.628: MDFS: RP servicing low queue for LC in slot 2
Mar 19 16:15:48.229: MDFS: RP queueing mdb message for (171.68.224.10, 224.2.127.254) to all linecards
Mar 19 16:15:48.229: MDFS: RP queueing mdb message for (171.69.67.106, 224.2.127.254) to all linecards
Mar 19 16:15:48.229: MDFS: RP queueing mdb message for (210.115.194.5, 224.2.127.254) to all linecards
```
debug ip mfib adjacency

To enable debugging output for IPv4 Multicast Forwarding Information Base (MFIB) adjacency management activity, use the `debug ip mfib adjacency` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip mfib adjacency
no debug ip mfib adjacency
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable debugging output for IPv4 MFIB adjacency management activity:

```
Router# debug ip mfib adjacency
```
debug ip mfib db

To enable debugging output for IPv4 Multicast Forwarding Information Base (MFIB) route database management activity, use the **debug ip mfib db** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip mfib [vrf {vrf-name | *}] db [{source-address} [group-address] | group-address [source-address]]
no debug ip mfib [vrf {vrf-name | *}] db [{source-address} [group-address] | group-address [source-address]]
```

**Syntax Description**

- **vrf {vrf-name | *}** (Optional) Enables debugging output for IPv4 MFIB route database management activity associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances.

  After specifying the optional `vrf` keyword, you must specify either:
  
  - *vrf-name* -- Name of an MVRF. Enables debugging output for IPv4 MFIB route database management activity associated with the MVRF specified for the `vrf-name` argument.
  
  - *--* -- Enables debugging output for route database management activity associated with all tables (all MVRF tables and the global table).

- **source-address** (Optional) Multicast source address.

- **group-address** (Optional) Multicast group address.

**Command Modes**

- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable debugging output for IPv4 MFIB route database management activity:

```
Router# debug ip mfib db
```
**debug ip mfib fs**

To enable debugging output for IPv4 Multicast Forwarding Information Base (MFIB) fast switching activity, use the `debug ip mfib fs` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip mfib [vrf {vrf-name | *}] fs [{source-address [group-address] | group-address [source-address]}
```

**Syntax Description**

- `vrf {vrf-name | *}`: (Optional) Enables debugging output for IPv4 MFIB fast switching activity associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances. After specifying the optional `vrf` keyword, you must specify either:
  - `vrf-name` -- Name of an MVRF. Enables debugging output for IPv4 MFIB fast switching activity associated with the MVRF specified for the `vrf-name` argument.
  - `*` -- Enables debugging output for IPv4 MFIB fast switching activity associated with all tables (all MVRF tables and the global table).

- `source-address` (Optional) Multicast source address.
- `group-address` (Optional) Multicast group address.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable debugging output for IPv4 MFIB fast switching activity:

```
Router# debug ip mfib fs
```
debug ip mfib init

To enable debugging output for events related to IPv4 Multicast Forwarding Information Base (MFIB) system initialization, use the `debug ip mfib init` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
direct ip mfib init
no debug ip mfib init
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable debugging output for events related to IPv4 MFIB system initialization:

```
Router# debug ip mfib init
```
# debug ip mfib interface

To enable debugging output for IPv4 Multicast Forwarding Information Base (MFIB) interfaces, use the `debug ip mfib interface` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip mfib interface
no debug ip mfib interface
```

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

## Examples

The following example shows how to enable debugging output for IPv4 MFIB interfaces:

```
Router# debug ip mfib interface
```
### debug ip mfib mrib

To enable debugging output for IPv4 Multicast Forwarding Information Base (MFIB) communication with the IPv4 Multicast Routing Information Base (MRIB), use the `debug ip mfib mrib` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```plaintext
debug ip mfib [vrf {vrf-name | *}] mrib [{source-address [group-address] | group-address [source-address]}] [detail]
no debug ip mfib [vrf {vrf-name | *}] mrib [{source-address [group-address] | group-address [source-address]}] [detail]
```

#### Syntax Description

- **vrf {vrf-name | *}** *(Optional) Enables debugging output for IPv4 MFIB communication with the IPv4 MRIB associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances.*

  After specifying the optional `vrf` keyword, you must specify either:
  - `vrf-name` -- Name of an MVRF. Enables debugging output for IPv4 MFIB communication with the IPv4 MRIB associated with the MVRF specified for the `vrf-name` argument.
  - `*` -- Enables debugging output for IPv4 MFIB communication with the IPv4 MRIB associated with all tables (all MVRF tables and the global table).

- **source-address** *(Optional) Multicast source address.*

- **group-address** *(Optional) Multicast group address.*

- **detail** *(Optional) Displays detailed debugging output for IPv4 MFIB communication with the IPv4 MRIB.*

#### Command Modes

Privileged EXEC (#)

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was modified. The <code>detail</code> keyword was added.</td>
</tr>
<tr>
<td>15.1(1)T</td>
<td>This command was modified. The <code>detail</code> keyword was added.</td>
</tr>
</tbody>
</table>

#### Examples

The following example shows how to enable debugging output for IPv4 MFIB communication with the IPv4 MRIB:

```plaintext
Router# debug ip mfib mrib
```
**debug ip mfib nat**

To enable debugging output for IPv4 Multicast Forwarding Information Base (MFIB) Network Address Translation (NAT) events associated with all tables, use the `debug ip mfib nat` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip mfib nat [{source-address [group-address] | group-address [source-address]}]
no debug ip mfib nat [{source-address [group-address] | group-address [source-address]}]
```

**Syntax Description**

- `source-address` (Optional) Multicast source address.
- `group-address` (Optional) Multicast group address.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable debugging output for IPv4 MFIB NAT events associated with all tables:

```
Router# debug ip mfib nat
```
debug ip mfib pak

To enable debugging output for IPv4 Multicast Forwarding Information Base (MFIB) packet forwarding activity, use the `debug ip mfib pak` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip mfib [vrf {vrf-name | *}] pak [{source-address [group-address] | group-address [source-address]}]
no debug ip mfib [vrf {vrf-name | *}] pak [{source-address [group-address] | group-address [source-address]}]
```

**Syntax Description**

- `vrf {vrf-name | *} [source-address [group-address] | group-address [source-address]]`
  - `(Optional) Enables debugging output for IPv4 MFIB packet forwarding activity associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances.
  - After specifying the optional `vrf` keyword, you must specify either:
    - `*` -- Enables debugging output for IPv4 MFIB packet forwarding activity associated with all tables (all MVRF tables and the global table).
    - `vrf-name` -- Name of an MVRF. Enables debugging output for IPv4 MFIB packet forwarding activity associated with the MVRF specified for the `vrf-name` argument.
  - `source-address` (Optional) Multicast source address.
  - `group-address` (Optional) Multicast group address.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable debugging output for IPv4 MFIB packet forwarding activity:

```
Router# debug ip mfib pak
```
debug ip mfib platform

To enable debugging output related to the hardware platform use of IPv4 Multicast Forwarding Information Base (MFIB) application program interfaces (APIs), use the `debug ip mfib platform` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip mfib [vrf {vrf-name | *}] platform {api | callbacks | errors | notify | trnx}
no debug ip mfib [vrf {vrf-name | *}] platform {api | callbacks | errors | notify | trnx}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`vrf {vrf-name</td>
<td>*}`</td>
</tr>
<tr>
<td>• <code>vrf-name</code></td>
<td>--Name of an MVRF. Enables debugging output related to the hardware platform use of IPv4 MFIB APIs associated with the MVRF specified for the <code>vrf-name</code> argument.</td>
</tr>
<tr>
<td>• <code>*</code></td>
<td>--Enables debugging output related to the hardware platform use of IPv4 MFIB APIs associated with all tables (all MVRF tables and the global table).</td>
</tr>
<tr>
<td><code>api</code></td>
<td>Enables debugging output related to the hardware platform use of IPv4 MFIB API calls.</td>
</tr>
<tr>
<td><code>callbacks</code></td>
<td>Enables debugging output related to the hardware platform use of IPv4 MFIB API callbacks.</td>
</tr>
<tr>
<td><code>errors</code></td>
<td>Enables debugging output related to the hardware platform use of IPv4 MFIB API errors.</td>
</tr>
<tr>
<td><code>notify</code></td>
<td>Enables debugging output related to the hardware platform use of IPv4 MFIB notifications.</td>
</tr>
<tr>
<td><code>trnx</code></td>
<td>Enables debugging output related to the hardware platform use of IPv4 MFIB database transactions.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable debugging output related to the hardware platform use of IPv4 MFIB API errors:

```
Router# debug ip mfib platform errors
```
debug ip mfib ppr

To enable debugging output for IPv4 Multicast Forwarding Information Base (MFIB) packet preservation events, use the `debug ip mfib ppr` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip mfib [vrf {vrf-name | *}] ppr [{errors | limit | preserve | release | trnx}] [{source-address [group-address] | group-address [source-address]]]
```

**Syntax Description**

- `vrf {vrf-name | *}` (Optional) Enables debugging output for IPv4 MFIB packet preservation events associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances.
  
  After specifying the optional `vrf` keyword, you must specify either:
  
  - `vrf-name` -- Name of an MVRF. Enables debugging output for IPv4 MFIB packet preservation events associated with the MVRF specified for the `vrf-name` argument.
  
  - `*` -- Enables debugging output for IPv4 MFIB packet preservation events associated with all tables (all MVRF tables and the global table).

- `errors` (Optional) Enables debugging output for IPv4 MFIB packet preservation errors.

- `limit` (Optional) Enables debugging output for IPv4 MFIB packet preservation limits.

- `preserve` (Optional) Enables debugging output for IPv4 MFIB packet preservation events.

- `release` (Optional) Enables debugging output for IPv4 MFIB packet preservation release events.

- `trnx` (Optional) Enables debugging output for IPv4 MFIB packet preservation database transaction events.

- `source-address` (Optional) Multicast source address.

- `group-address` (Optional) Multicast group address.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>
The following example shows how to enable debugging output for IPv4 MFIB packet preservation errors:

Router# debug ip mfib ppr errors
debug ip mfib ps

To enable debugging output for IPv4 Multicast Forwarding Information Base (MFIB) process switching activity, use the `debug ip mfib ps` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip mfib [vrf {vrf-name | *}] ps [{source-address [group-address] | group-address [source-address]}]
no debug ip mfib [vrf {vrf-name | *}] ps [{source-address [group-address] | group-address [source-address]}]
```

**Syntax Description**

- `vrf {vrf-name | *}`: (Optional) Enables debugging output for IPv4 MFIB process switching activity associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances. After specifying the optional `vrf` keyword, you must specify either:
  - `vrf-name` -- Name of an MVRF. Enables debugging output for IPv4 MFIB process switching activity associated with the MVRF specified for the `vrf-name` argument.
  - `*` -- Enables debugging output for IPv4 MFIB process switching activity associated with all tables (all MVRF tables and the global table).

- `source-address`: (Optional) Multicast source address.
- `group-address`: (Optional) Multicast group address.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable debugging output for IPv4 MFIB process switching activity:

```
Router# debug ip mfib ps
```
# debug ip mfib signal

To enable debugging output for IPv4 Multicast Forwarding Information Base (MFIB) signal activity, use the `debug ip mfib signal` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```plaintext
debug ip mfib [vrf {vrf-name | *}] signal [{source-address} [group-address] | group-address [source-address]]

no debug ip mfib [vrf {vrf-name | *}] signal [{source-address} [group-address] | group-address [source-address]]
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| `vrf {vrf-name | *}` | (Optional) Enables debugging output for IPv4 MFIB signal activity associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances. After specifying the optional `vrf` keyword, you must specify either:  
  - `vrf-name` -- Name of an MVRF. Enables debugging output for IPv4 MFIB signal activity associated with the MVRF specified for the `vrf-name` argument.  
  - `*` -- Enables debugging output for IPv4 MFIB fast signal activity associated with all tables (all MVRF tables and the global table). |
| `source-address`     | (Optional) Multicast source address. |
| `group-address`      | (Optional) Multicast group address. |

## Command Modes

Privileged EXEC (#)

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

## Examples

The following example shows how to enable debugging output for IPv4 MFIB signal activity for the default IPv4 table:

```plaintext
Router# debug ip mfib signal
```

The following example shows how to enable debugging output for IPv4 MFIB signal activity for the group 224.0.1.40, the source 10.1.1.1, and for the VRF Mgmt-intf:

```plaintext
Router# debug ip mfib vrf Mgmt-intf signal 10.1.1.1 224.0.1.40
```
debug ip mfib table

To enable debugging output for IPv4 Multicast Forwarding Information Base (MFIB) table activity, use the `debug ip mfib table` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip mfib [vrf {vrf-name | *}] table {db | mrib}
no debug ip mfib [vrf {vrf-name | *}] table {db | mrib}
```

### Syntax Description

| vrf {vrf-name | *} | (Optional) Enables debugging output for IPv4 MFIB signal activity associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances. After specifying the optional `vrf` keyword, you must specify either:
| vrf-name --Name of an MVRF. Enables debugging output for IPv4 MFIB signal activity associated with the MVRF specified for the `vrf-name` argument.
| * --Enables debugging output for IPv4 MFIB fast signal activity associated with all tables (all MVRF tables and the global table).
| db | Enables debugging output for IPv4 MFIB database table events and operations.
| mrib | Enables debugging output for IPv4 MFIB Multicast Routing Information Base (MRIB) API table events and operations.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to enable debugging output for IPv4 MFIB database table events and operations:

```
Router# debug ip mfib table db
```

The following example shows how to enable debugging output for IPv4 MFIB MRIB API table events and operations:

```
Router# debug ip mfib table mrib
```
debug ip mhbeat

To monitor the action of the heartbeat trap, use the `debug ip mhbeat` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
ddebug ip mhbeat
no debug ip mhbeat
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Debugging is not enabled.

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(2)XH</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**
The following is sample output from the `debug ip mhbeat` command.

```
Router# debug ip mhbeat
IP multicast heartbeat debugging is on
Router debug snmp packets

SNMP packet debugging is on

Router(config)# ip multicast heartbeat intervals-of 10
Dec 23 13:34:21.132: MHBEAT: ip multicast-heartbeat group 224.0.1.53 port 0
source 0.0.0.0 0.0.0.0 at-least 3 in 5 intervals-of 10 seconds
d
Router# Dec 23 13:34:23: %SYS-5-CONFIG_I: Configured from console by console
Dec 23 13:34:31.136: MHBEAT: timer ticked, t=1,i=1,c=0
Dec 23 13:34:41.136: MHBEAT: timer ticked, t=2,i=2,c=0
Dec 23 13:34:51.136: MHBEAT: timer ticked, t=3,i=3,c=0
Dec 23 13:35:01.136: MHBEAT: timer ticked, t=4,i=4,c=0
Dec 23 13:35:11.136: MHBEAT: timer ticked, t=5,i=0,c=0
Dec 23 13:35:21.135: Send SNMP Trap for missing heartbeat
Dec 23 13:35:21.135: SNMP: V1 Trap, ent ciscoExperiment.2.3.1, addr 4.4.4.4, gentrap 6, spectrap 1
ciscoIpMRoutHeartBeat.1.0 = 224.0.1.53
ciscoIpMRoutHeartBeat.2.0 = 0.0.0.0
ciscoIpMRoutHeartBeat.3.0 = 10
ciscoIpMRoutHeartBeat.4.0 = 5
ciscoIpMRoutHeartBeat.5.0 = 0
ciscoIpMRoutHeartBeat.6.0 = 3
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip multicast heartbeat</code></td>
<td>Monitors the health of multicast delivery, and alerts when the delivery fails to meet certain parameters.</td>
</tr>
</tbody>
</table>
**debug ip mobile**

To display IP mobility activities, use the `debug ip mobile` command in privileged EXEC mode.

```
depend ip mobile [{advertise | host [access-list-number] | local-area | redundancy | udp-tunneling}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>advertise</td>
<td>(Optional) Advertisement information.</td>
</tr>
<tr>
<td>host</td>
<td>(Optional) The mobile node host.</td>
</tr>
<tr>
<td>access-list-number</td>
<td>(Optional) The number of an IP access list.</td>
</tr>
<tr>
<td>local-area</td>
<td>(Optional) The local area.</td>
</tr>
<tr>
<td>redundancy</td>
<td>(Optional) Redundancy activities.</td>
</tr>
<tr>
<td>udp-tunneling</td>
<td>(Optional) User Datagram Protocol (UDP) tunneling activities.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(2)T</td>
<td>The standby keyword was added.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td>The standby keyword was replaced by the redundancy keyword.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was enhanced to display information about foreign agent reverse tunnels and the mobile networks attached to the mobile router.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>The udp-tunneling keyword was added and the command was enhanced to display information about NAT traversal using UDP tunneling.</td>
</tr>
<tr>
<td>12.3(7)XJ</td>
<td>This command was enhanced to include the Resource Management capability.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ip mobile redundancy` command to troubleshoot redundancy problems.

No per-user debugging output is shown for mobile nodes using the network access identifier (NAI) for the `debug ip mobile host` command. Debugging of specific mobile nodes using an IP address is possible through the access list.
Examples

The following is sample output from the `debug ip mobile` command when foreign agent reverse tunneling is enabled:

MobileIP: MN 14.0.0.30 deleted from ReverseTunnelTable of Ethernet2/1 (Entries 0)

The following is sample output from the `debug ip mobile advertise` command:

Router# debug ip mobile advertise
MobileIP: Agent advertisement sent out Ethernet1/2: type=16, len=10, seq=1, lifetime=36000,
flags=0x1400{rbhFmGv-rsv-},
Care-of address: 68.0.0.31
Prefix Length ext: len=1 (8)
FA Challenge value: 769C808D

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>Type of advertisement.</td>
</tr>
<tr>
<td>len</td>
<td>Length of extension (in bytes).</td>
</tr>
<tr>
<td>seq</td>
<td>Sequence number of this advertisement.</td>
</tr>
<tr>
<td>lifetime</td>
<td>Lifetime (in seconds).</td>
</tr>
<tr>
<td>flags</td>
<td>Capital letters represent bits that are set; lowercase letters represent unset bits.</td>
</tr>
<tr>
<td>Care-of address</td>
<td>IP address.</td>
</tr>
<tr>
<td>Prefix Length ext</td>
<td>Number of prefix lengths advertised. This is the bits in the mask of the interface sending this advertisement. Used for roaming detection.</td>
</tr>
<tr>
<td>FA Challenge value</td>
<td>Foreign Agent challenge value (randomly generated by the foreign agent.)</td>
</tr>
</tbody>
</table>

The following is sample output from the `debug ip mobile host` command:

Router# debug ip mobile host
MobileIP: HA received registration for MN 20.0.0.6 on interface Ethernet1 using COA 68.0.0.31 HA 66.0.0.5 lifetime 30000 options abdmgvT
MobileIP: Authenticated FA 68.0.0.31 using SPI 110 (MN 20.0.0.6)
MobileIP: Authenticated MN 20.0.0.6 using SPI 300
MobileIP: HA accepts registration from MN 20.0.0.6
MobileIP: Mobility binding for MN 20.0.0.6 updated
MobileIP: Roam timer started for MN 20.0.0.6, lifetime 30000
MobileIP: MN auth ext added (SPI 300) in reply to MN 20.0.0.6
MobileIP: HF auth ext added (SPI 220) in reply to MN 20.0.0.6
MobileIP: HA sent reply to MN 20.0.0.6

The following is sample output from the `debug ip mobile redundancy` command. In this example, the active home agent receives a registration request from mobile node 20.0.0.2 and sends a binding update to peer home agent 1.0.0.2:

MobileIP: MN 20.0.0.2 - sent BindUpd to HA 1.0.0.2 HAA 20.0.0.1
MobileIP:HA standby maint started - cnt 1
MobileIP:MN 20.0.0.2 - sent BindUpd id 3780410816 cnt 0 elapsed 0
  adjust -0 to HA 1.0.0.2 in grp 1.0.0.10 HAA 20.0.0.1

In this example, the standby home agent receives a binding update for mobile node 20.0.0.2 sent by
the active home agent:

MobileIP:MN 20.0.0.2 - HA rcv BindUpd from 1.0.0.3 HAA 20.0.0.1

The following is sample output from the `debug ip mobile udp-tunneling` command and displays
the registration, authentication, and establishment of UDP tunneling of a mobile node (MN) with a
foreign agent (FA):

Dec 31 12:34:25.707: UDP: rcvd src=10.10.10.10(434), dst=10.30.30.1(434), length=54
Dec 31 12:34:25.707: MobileIP: ParseRegExt skipping 10 to next
Dec 31 12:34:25.707: MobileIP: FA rcv registration for MN 10.10.10.10 on Ethernet2/2 using
  COA 10.30.30.1 HA 10.10.10.100 lifetime 65535 options sbdmg-T-identification
Dec 31 12:34:25.707: MobileIP: Ethernet2/2 glean 10.10.10.10 accepted
Dec 31 12:34:25.707: MobileIP: Registration request byte count = 74
Dec 31 12:34:25.707: MobileIP: FA queued MN 10.10.10.10 in register table
Dec 31 12:34:25.707: MobileIP: Visitor registration timer started for MN 10.10.10.10,
  lifetime 120
Dec 31 12:34:25.707: MobileIP: Adding UDP Tunnel req extension
Dec 31 12:34:25.707: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:25.707: MobileIP: MN 10.10.10.10 FHAE added to HA 10.10.10.100 using SPI 1000
Dec 31 12:34:25.707: MobileIP: FA forwarded registration for MN 10.10.10.10 to HA
  10.10.10.100
Dec 31 12:34:25.715: UDP: rcvd src=10.10.10.100(434), dst=10.30.30.1(434), length=94
Dec 31 12:34:25.715: MobileIP: ParseRegExt type NVSE(134) addr 20010B28 end 20010B6A
Dec 31 12:34:25.715: MobileIP: ParseRegExt type MN-config NVSE(14) subtype 1 (MN prefix
  length) prefix length (24)
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 12 to next
Dec 31 12:34:25.715: MobileIP: ParseRegExt type UDPTUNREPE(44) addr 20010B4C end 20010B6A
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 6 to next
Dec 31 12:34:25.715: MobileIP: ParseRegExt type FHAE(34) addr 20010B54 end 20010B6A
Dec 31 12:34:25.715: MobileIP: FA rcv accept (0) reply for MN 10.10.10.10 on Ethernet2/3
  using HA 10.10.10.100 lifetime 65535
Dec 31 12:34:25.719: MobileIP: Authenticating HA 10.10.10.100 using SPI 1000
Dec 31 12:34:25.719: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:25.719: MobileIP: Authenticated HA 10.10.10.100 using SPI 1000 and 16 byte
  key
Dec 31 12:34:25.719: MobileIP: HA accepts UDP Tunneling
Dec 31 12:34:25.719: MobileIP: Update visitor table for MN 10.10.10.10
Dec 31 12:34:25.719: MobileIP: Tunnel0 (MIPUDP/IP) created with src 10.30.30.1 dst
  10.10.10.100
Dec 31 12:34:25.719: MobileIP: Setting up UDP Keep-Alive Timer for tunnel 10.30.30.1:0 -
  10.10.10.100:0 with keep-alive 30
Dec 31 12:34:25.719: MobileIP: Starting the tunnel keep-alive timer
Dec 31 12:34:25.719: MobileIP: ARP entry for MN 10.10.10.10 using 10.10.10.10 inserted on
  Ethernet2/2
Dec 31 12:34:25.719: MobileIP: FA route add 10.10.10.10 successful. Code = 0
Dec 31 12:34:25.719: MobileIP: MN 10.10.10.10 added to ReverseTunnelTable of Ethernet2/2
  (Entries 1)
Dec 31 12:34:25.719: MobileIP: FA dequeued MN 10.10.10.10 from register table
Dec 31 12:34:25.719: MobileIP: MN 10.10.10.10 using 10.10.10.10 visiting on Ethernet2/2 Dec
The following is sample output from the `debug ip mobile udp-tunneling` command and displays the registration, authentication, and establishment of UDP tunneling of a MN with a home agent (HA):

Dec 31 12:34:26.167: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:26.167: MobileIP: ParseRegExt skipping 6 to next
Dec 31 12:34:26.167: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:26.167: MobileIP: HA 167 rcv registration for MN 10.10.10.10 on Ethernet2/1 using HomeAddr 10.10.10.10 COA 10.30.30.1 HA 10.10.10.100 lifetime 65535 options
Dec 31 12:34:26.167: MobileIP: NAT detected SRC:10.10.10.50 COA: 10.30.30.1
Dec 31 12:34:26.167: MobileIP: UDP Tunnel Request accepted 10.10.10.50:434
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authenticated FA 10.10.10.50 using SPI 1000
Dec 31 12:34:26.167: MobileIP: MN 10.10.10.10 MHAE added to MN 10.10.10.10 using SPI 1000
Dec 31 12:34:26.167: MobileIP: MHAE added to MN 10.10.10.10 using SPI 1000
Dec 31 12:34:26.167: MobileIP: MN 10.10.10.10 FHAE added to FA 10.10.10.50 using SPI 1000
Dec 31 12:34:26.167: MobileIP: MN 10.10.10.10 HHAE added to HA 10.10.10.3 using SPI 1000
Dec 31 12:34:26.167: MobileIP: Tunnel0 (MIFUDP/IP) created with src 10.10.10.100 dst 10.10.10.50
Dec 31 12:34:26.167: MobileIP: Tunnel0 (MIFUDP/IP) created with src 10.10.10.100 dst 10.10.10.50
Dec 31 12:34:26.167: MobileIP: Setting up UDP Keep-Alive Timer for tunnel 10.10.10.100:0 - 10.10.10.50:0 with keep-alive 30
Dec 31 12:34:26.167: MobileIP: Starting the tunnel keep-alive timer
Dec 31 12:34:26.167: MobileIP: MN 10.10.10.10 Insert route for 10.10.10.10/255.255.255.255 via gateway 10.10.10.50 on Tunnel0
Dec 31 12:34:26.167: MobileIP: MN 10.10.10.10 is now roaming
Dec 31 12:34:26.171: MobileIP: Gratuitous ARPs sent for MN 10.10.10.10 MAC 0002.fca5.bc39
Dec 31 12:34:26.171: MobileIP: Mask for address is 24
Dec 31 12:34:26.171: MobileIP: HA accepts registration from MN 10.10.10.10
Dec 31 12:34:26.171: MobileIP: Dynamic and Static Network Extension Length 0 - 0
Dec 31 12:34:26.171: MobileIP: Composed mobile network extension length:0
Dec 31 12:34:26.171: MobileIP: Added prefix length vse in reply
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and truncated key
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: Authenticated MN 10.10.10.10 using SPI 1000
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and truncated key
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 MHAE added to MN 10.10.10.10 using SPI 1000
Dec 31 12:34:26.171: MobileIP: MHAE added to MN 10.10.10.10 using SPI 1000
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 FHAE added to FA 10.10.10.50 using SPI 1000
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 HHAE added to HA 10.10.10.3 using SPI 1000
Dec 31 12:34:26.175: MobileIP: ParseRegExt type CVSE(38) addr 2000128C end 200012AE
Dec 31 12:34:26.175: MobileIP: ParseRegExt type HA red. version CVSE(6)
Dec 31 12:34:26.175: MobileIP: ParseRegExt skipping 8 to next
Dec 31 12:34:26.175: MobileIP: ParseRegExt type HHAE(35) addr 20001298 end 200012AE
Dec 31 12:34:26.175: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:26.175: MobileIP: Authenticating HA 10.10.10.3 using SPI 1000
Dec 31 12:34:26.175: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.175: MobileIP: Authentication algorithm MD5 and truncated key
Dec 31 12:34:26.175: MobileIP: Authenticated HA 10.10.10.3 using SPI 1000 and 16 byte key
Dec 31 12:34:27.167: MobileIP: swif coming up Tunnel0d0
**debug ip mobile advertise**

The `debug ip mobile advertise` command was consolidated with the `debug ip mobile` command. See the description of the `debug ip mobile` command in the “Debug Commands” chapter for more information.

To display advertisement information, use the `debug ip mobile advertise` EXEC command.

```plaintext
debug ip mobile advertise
no debug ip mobile advertise
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

No default values.

### Command Modes

EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `debug ip mobile advertise` command. The table below describes significant fields shown in the display.

```
Router# debug ip mobile advertise
MobileIP: Agent advertisement sent out Ethernet1/2: type=16, len=10, seq=1,
lifetime=36000, flags=0x1400(vehFmGv-rsv-),
Care-of address: 14.0.0.31
Prefix Length ext: len=1 (8 )
```

**Table 32: Debug IP Mobile Advertise Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>Type of advertisement.</td>
</tr>
<tr>
<td>len</td>
<td>Length of extension in bytes.</td>
</tr>
<tr>
<td>seq</td>
<td>Sequence number of this advertisement.</td>
</tr>
<tr>
<td>lifetime</td>
<td>Lifetime in seconds.</td>
</tr>
<tr>
<td>flags</td>
<td>Capital letters represent bits that are set, lower case letters represent unset bits.</td>
</tr>
<tr>
<td>Care-of address</td>
<td>IP address.</td>
</tr>
<tr>
<td>Prefix Length ext</td>
<td>Number of prefix lengths advertised. This is the bits in the mask of the interface sending this advertisement. Used for roaming detection.</td>
</tr>
</tbody>
</table>

---

**debug ip http all through debug ip rsvp**
debug ip mobile dyn-pbr

To display debugging messages for the mobile IP (MIP) dynamic policy based routing (PBR) mobile router, use the `debug ip mobile dyn-pbr` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip mobile dyn-pbr
no debug ip mobile dyn-pbr
```

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following sample output from the `debug ip mobile dyn-pbr` command:

```
Router# debug ip mobile dyn-pbr
```
*Jan 12 19:50:16.271: MIP-PBR: After api bind, ACL VIDEO-to-192.0.2.0/24, user_count 3
*Jan 12 19:50:16.271: MIP-PBR: current_map_entry->dyn_rmaps = 0
*Jan 12 19:50:16.271: MIP-PBR: found rmap_info = VIDEO-to-192.0.2.0/24
*Jan 12 19:50:16.271: MIP-PBR: added route-map entry for VIDEO-to-192.0.2.0/24 via Tunnel2
*Jan 12 19:50:16.271: MIP-PBR: After api bind, ACL VIDEO-to-192.0.2.32/20, user_count 3
*Jan 12 19:50:16.271: MIP-PBR: found rmap_info = VIDEO-to-192.0.2.32/20
*Jan 12 19:50:16.271: MIP-PBR: Dyn route-map entry added for home address 192.0.2.32 on HA
*Jan 12 19:50:16.271: MIP-PBR: ACL handle VOICE-to-192.0.2.0/24 created
*Jan 12 19:50:16.271: MIP-PBR: Using existing dyn acl hdl VOICE-to-192.0.2.0/24
*Jan 12 19:50:16.271: MIP-PBR: After api bind, ACL VOICE-to-192.0.2.0/24, user_count 3
*Jan 12 19:50:16.271: MIP-PBR: current_map_entry->dyn_rmaps = 0
*Jan 12 19:50:16.271: MIP-PBR: found rmap_info = VOICE-to-192.0.2.0/24
*Jan 12 19:50:16.271: MIP-PBR: added route-map entry for VOICE-to-192.0.2.0/24 via Tunnel4
*Jan 12 19:50:16.271: MIP-PBR: Dyn route-map entry added for home address 192.0.2.32 on HA
*Jan 12 19:50:16.271: MIP-PBR: Using existing dyn acl hdl VOICE-to-192.0.2.0/24
*Jan 12 19:50:16.271: MIP-PBR: After api bind, ACL VOICE-to-192.0.2.0/24, user_count 3
*Jan 12 19:50:16.271: MIP-PBR: found rmap_info = VOICE-to-192.0.2.0/24
*Jan 12 19:50:16.271: MIP-PBR: added route-map entry for VOICE-to-192.0.2.0/24 via Tunnel4
*Jan 12 19:50:16.271: MIP-PBR: Dyn route-map entry added for home address 192.0.2.32 on HA
*Jan 12 19:50:16.291: Looking at reg_info: Tunnel2 MPATH_1 10
*Jan 12 19:50:16.291: Looking at reg_info: Tunnel2 MPATH_1 10
debug ip mobile host

The `debug ip mobile host` command was consolidated with the `debug ip mobile` command. See the description of the `debug ip mobile` command in the “Debug Commands” chapter for more information.

Use the `debug ip mobile host` EXEC command to display IP mobility events.

```
debug ip mobile host [access-list-number] [nai {NAI username | username@realm}]
no debug ip mobile host [access-list-number] [nai {NAI username | username@realm}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>access-list-number</th>
<th>(Optional) The mobile node host.</th>
</tr>
</thead>
<tbody>
<tr>
<td>nai</td>
<td>(Optional) Mobile host identified by NAI.</td>
</tr>
</tbody>
</table>

**Command Default**

No default values.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip mobile host` command:

```
Router# debug ip mobile host
MobileIP: HA received registration for MN 10.0.0.6 on interface Ethernet1 using COA 14.0.0.31 HA 15.0.0.5 lifetime 30000 options sbdmgVT
MobileIP: Authenticated FA 15.0.0.31 using SPI 110 {MN 20.0.0.6}
MobileIP: Authenticated MN 11.0.0.6 using SPI 300

MobileIP: HA accepts registration from MN 11.0.0.6
MobileIP: Mobility binding for MN 11.0.0.6 updated
MobileIP: Roam timer started for MN 11.0.0.6, lifetime 30000
MobileIP: MH auth ext added (SPI 300) in reply to MN 11.0.0.6
MobileIP: HF auth ext added (SPI 220) in reply to MN 11.0.0.6

MobileIP: HA sent reply to MN 11.0.0.6
```
**debug ip mobile mib**

To display debugging messages for mobile networks, use the `debug ip mobile mib` command in privileged EXEC mode. To disable, use the `no` form of this command.

```
debug ip mobile mib
no debug ip mobile mib
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is useful for customers deploying mobile networks functionality that need to monitor and debug mobile router information via the Simple Network Management Protocol (SNMP).

Set operations (performed from a Network Management System) are supported for mobile network services. While setting the values for MIBs, a set operation may fail. The `debug ip mobile mib` command allows error messages explaining the failure to be displayed on the console of the home agent.

**Examples**

The following mobile networks deployment MIB debug messages are displayed only on certain conditions or when a certain condition fails.

```
Router# debug ip mobile mib
! Mobile router is not enabled
MIPMIB: Mobile Router is not enabled
! Care-of-interface can be set as transmit-only only if its a Serial interface
MIPMIB: Serial interfaces can only be set as transmit-only
! The Care of address can be configured only if foreign agent is running
MIPMIB: FA cannot be started
! Check if home agent is active
MIPMIB: HA is not enabled
! For mobile router configuration, host configuration must have been done already
MIPMIB: MN <address> is not configured
! Mobile Network does not match the existing mobile network
MIPMIB: Conflict with existing mobile networks <name>
! Mobile router present
MIPMIB: MR <address> is not configured

! Static mobile networks can be configured only for single member mobilenetgroups
MIPMIB: MR is part of group <name>, network cannot be configured
! If a binding exists for this mobile router, then delete the route for this unconfigured mobile network
MIPMIB: Delete static mobile net for MR
! Check if its a dynamically registered mobile network
nMIPMIB: Mobile network <address mask> is dynamically registered, cannot be removed
! Check if the mobile network has already been configured for another group
nMIPMIB: Mobile network already configured for MR
```
! Check if the network has been dynamically registered
nMIPMIB: Deleted dynamic mobnet <address mask> for MR <name>
! Check if the redundancy group exists
MIPMIB: Redundancy group <name> does not exist
! CCoA configuration, use primary interface address as the CCoA
MIPMIB: No IP address on this interface
! CCoA configuration, CCoA address shouldn’t be the same as the Home Address

nMIPMIB: Collocated CoA is the same as the Home Address, registrations will fail
debug ip mobile redundancy

The debug ip mobile redundancy command was consolidated with the debug ip mobile command. See the description of the debug ip mobile command in the “Debug Commands” chapter for more information.

Use the debug ip mobile redundancy EXEC command to display IP mobility events.

d debug ip mobile redundancy
no debug ip mobile redundancy

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default values.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the debug ip mobile redundancy command:

Router# debug ip mobile redundancy
00:19:21: MobileIP: Adding MN service flags to bindupdate
00:19:21: MobileIP: Adding MN service flags 0 init registration flags 1
00:19:21: MobileIP: Adding a hared version cvse - bindupdate
00:19:21: MobileIP: HARelayBindUpdate version number 2MobileIP: MN 14.0.0.20 - sent BindUpd
to HA 11.0.0.3 HAA 11.0.0.4
00:19:21: MobileIP: HA standby maint started - cnt 1
00:19:21: MobileIP: MN 14.0.0.20 - HA rcv BindUpdAck accept from 11.0.0.3 HAA 11.0.0.4
00:19:22: MobileIP: HA standby maint started - cnt 1
debug ip mobile router

To display debugging messages for the mobile router, use the `debug ip mobile router` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
details (Optional) Displays detailed mobile router debug messages.
```

Syntax Description

```
no debug ip mobile router [detail]
```

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was enhanced to display information about the addition and deletion of mobile networks.</td>
</tr>
<tr>
<td>15.4(3)T</td>
<td>This command was enhanced to display information about Multi-VRF for Network Mobility.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The mobile router operations can be debugged. The following conditions trigger debugging messages:

- Agent discovery
- Registration
- Mobile router state change
- Routes and tunnels created or deleted
- Roaming information

Debugging messages are prefixed with “MobRtr” and detail messages are prefixed with “MobRtrX”.

Examples

The following is sample output from the `debug ip mobile router` command:

```
Device# debug ip mobile router
MobileRouter: New FA 27.0.0.12 coa 27.0.0.12 int Ethernet0/1 MAC 0050.50c1.c855
2w2d: MobileRouter: Register reason: isolated
2w2d: MobileRouter: Snd reg request agent 27.0.0.12 coa 27.0.0.12 home 9.0.0.1 ha 29.0.0.4
  lifetime 36000 int Ethernet0/1 flag sbdmgvt cnt 0 id B496B69C.55E77974
2w2d: MobileRouter: Status Isolated -> Pending
```

The following is sample output from the `debug ip mobile router detail` command:

```
Device# debug ip mobile router detail
1d09h: MobRtr: New agent 20.0.0.2 coa 30.0.0.2 int Ethernet3/1 MAC 00b0.8e35.a055
1d09h: MobRtr: Register reason: left home
```
The following is sample output from the `debug ip mobile router detail` command when Multi-VRF for Network Mobility feature is configured:

```
Device# debug ip mobile router detail
1d09h: MobRtr: New agent 10.0.0.2 coa 10.1.0.2 int Ethernet3/1 MAC 00b0.8e35.a055
1d09h: MobRtr: Register reason: left home
1d09h: MobRtr: Extsize 18 add 1 delete 0
1d09h: MobRtrX: Add network 10.0.0.0/8
1d09h: MobRtr: Register to fa 10.1.0.20 coa 30.0.0.2 home 10.0.10.11 ha 10.1.1.3 life 120
int Ethernet3/1 flag sbdmgvt cnt 0 id BE804340.447F50A4
1d09h: MobRtr: Status Isolated -> Pending
1d09h: MobRtr: MN rcv accept (0) reply on Ethernet3/1 from 10.0.0.2 lifetime 120
MobileIP: MN 10.0.0.3 - authenticating HA 10.0.0.3 using SPI 100
MobileIP: MN 10.0.0.3 - authenticated HA 10.0.0.3 using SPI 100
1d09h: MobRtr: Status Pending -> Registered
1d09h: MobRtr: Add default gateway 10.0.0.2 (Ethernet3/1)
1d09h: MobRtr: Add default route via 10.0.0.2 (Ethernet3/1)
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip mobile</td>
<td>Displays Mobile IP information.</td>
</tr>
</tbody>
</table>
debug ip mpacket

Note
Effective with Cisco IOS Release 15.0(1)M and Cisco IOS Release 12.2(33)SRE, the `debug ip mpacket` command is replaced by the `debug ip mfib ps` command and the `debug ip mcache` command with the `fastswitch` keyword is replaced by the `debug ip mfib pak` command. See the `debug ip mfib ps` and `debug ip mfib pak` commands for more information.

To display IP multicast packets received and sent, use the `debug ip mpacket` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
ddebug ip mpacket [vrf vrf-name] [{detail | fastswitch}] [access-list] [group]
no debug ip mpacket [vrf vrf-name] [{detail | fastswitch}] [access-list] [group]
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf (Optional) Supports the Multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td>vrf-name (Optional) Name assigned to the VRF.</td>
</tr>
<tr>
<td>detail (Optional) Displays IP header information and MAC address information.</td>
</tr>
<tr>
<td>fastswitch (Optional) Displays IP packet information in the fast path.</td>
</tr>
<tr>
<td>access-list (Optional) The access list number.</td>
</tr>
<tr>
<td>group (Optional) The group name or address.</td>
</tr>
</tbody>
</table>

Command Default
The `debug ip mpacket` command displays all IP multicast packets switched at the process level.

Command Modes
Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(2)T</td>
<td>This command was modified. The <code>fastswitch</code> keyword was added.</td>
</tr>
<tr>
<td>12.0(23)S</td>
<td>This command was modified. The <code>vrf</code> keyword and <code>vrf-name</code> argument were added.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was replaced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

This command displays information for multicast IP packets that are forwarded from this router. Use the `access-list` or `group` argument to limit the display to multicast packets from sources described by the access list or a specific multicast group.

Use this command with the `debug ip packet` command to display additional packet information.

Note

The `debug ip mpacket` command generates many messages. Use this command with care so that performance on the network is not affected by the debug message traffic.

Examples

The following is sample output from the `debug ip mpacket` command:

```
Router# debug ip mpacket 224.2.0.1
IP: s=10.188.34.54 (Ethernet1), d=224.2.0.1 (Tunnel0), len 88, mforward
IP: s=10.188.34.54 (Ethernet1), d=224.2.0.1 (Tunnel0), len 88, mforward
IP: s=10.188.34.54 (Ethernet1), d=224.2.0.1 (Tunnel0), len 88, mforward
IP: s=10.162.3.27 (Ethernet1), d=224.2.0.1 (Tunnel0), len 68, mforward
```

The table below describes the significant fields shown in the display.

*Table 33: debug ip mpacket Field Descriptions*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>IP packet.</td>
</tr>
<tr>
<td>s=10.188.34.54</td>
<td>Source address of the packet.</td>
</tr>
<tr>
<td>(Ethernet1)</td>
<td>Name of the interface that received the packet.</td>
</tr>
<tr>
<td>d=224.2.0.1</td>
<td>Multicast group address that is the destination for this packet.</td>
</tr>
<tr>
<td>(Tunnel0)</td>
<td>Outgoing interface for the packet.</td>
</tr>
<tr>
<td>len 88</td>
<td>Number of bytes in the packet. This value will vary depending on the application and the media.</td>
</tr>
<tr>
<td>mforward</td>
<td>Packet has been forwarded.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip dvmrp</td>
<td>Displays information on DVMRP packets received and sent.</td>
</tr>
<tr>
<td>debug ip igmp</td>
<td>Displays IGMP packets received and sent, and IGMP host-related events.</td>
</tr>
<tr>
<td>debug ip mrm</td>
<td>Displays MRM control packet activity.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>debug ip packet</td>
<td>Displays general IP debugging information and IPSO security transactions.</td>
</tr>
<tr>
<td>debug ip sd</td>
<td>Displays all SD announcements received.</td>
</tr>
</tbody>
</table>
debug ip mrib

To enable debugging output for IPv4 Multicast Routing Information Base (MRIB) activity, use the `debug ip mrib` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip mrib [vrf vrf-name] [client | io | issu | proxy | route | table | trans]
no debug ip mrib [vrf vrf-name] [client | io | issu | proxy | route | table | trans]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Enables debugging output for IPv4 MRIB activity associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the <code>vrf-name</code> argument.</td>
</tr>
<tr>
<td>client</td>
<td>Enables debugging output for IPv4 MRIB client management activity.</td>
</tr>
<tr>
<td>io</td>
<td>Enables debugging output for IPv4 MRIB input/output (I/O) events.</td>
</tr>
<tr>
<td>issu</td>
<td>Enables debugging output for IPv4 MRIB events associated with In-Service Software Upgrades (ISSUs).</td>
</tr>
<tr>
<td>proxy</td>
<td>Enables debugging output related to IPv4 MRIB proxy activity between the Route Processor (RP) and line cards.</td>
</tr>
<tr>
<td>route</td>
<td>Enables debugging output for IPv4 MRIB activity pertaining to routing entries.</td>
</tr>
<tr>
<td>table</td>
<td>Enables debugging output for IPv4 MRIB table management activity.</td>
</tr>
<tr>
<td>trans</td>
<td>Enables debugging output for activity related to IPv4 Protocol Independent Multicast (PIM) to MRIB translation.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable debugging output for IPv4 MRIB client management activity:

```
Router# debug ip mrib client
```
debug ip mrm

To display Multicast Routing Monitor (MRM) control packet activity, use the `debug ip mrm` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
description
debug ip mrm [{events | packets}]
no debug ip mrm [{events | packets}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>(Optional) Displays MRM events.</td>
</tr>
<tr>
<td>packets</td>
<td>(Optional) Displays MRM test packets.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip mrm` command on different devices:

**On Manager**

*Feb 28 16:25:44.009: MRM: Send Beacon for group 239.1.1.1, holdtime 86100 seconds
*Feb 28 16:26:01.095: MRM: Receive Status Report from 10.1.4.2 on Ethernet0
*Feb 28 16:26:01.099: MRM: Send Status Report Ack to 10.1.4.2 for group 239.1.1.1

**On Test-Sender**

MRM: Receive Test-Sender Request/Local trigger from 1.1.1.1 on Ethernet0
MRM: Send TS request Ack to 1.1.1.1 for group 239.1.2.3
MRM: Send test packet src:2.2.2.2 dst:239.1.2.3 manager:1.1.1.1

**On Test-Receiver**

MRM: Receive Test-Receiver Request/Monitor from 1.1.1.1 on Ethernet0
MRM: Send TR request Ack to 1.1.1.1 for group 239.1.2.3
MRM: Receive Beacon from 1.1.1.1 on Ethernet0
MRM: Send Status Report to 1.1.1.1 for group 239.1.2.3
MRM: Receive Status Report Ack from 1.1.1.1 on Ethernet0
debug ip mrouteing

To display information about activity in the multicast route (mroute) table, use the `debug ip mrouteing` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
depbug ip mrouteing [vrf vrf-name] [[rpf-events | timers] [group-address]]
no debug ip mrouteing [vrf vrf-name] [[rpf-events | timers] [group-address]]
```

**Command Syntax in Cisco IOS 12.2(33)SXH and Subsequent 12.2SX Releases**
```
depbug ip mrouteing [vrf vrf-name] [[high-availability | rpf-events [group-address] | timers group-address]]
no debug ip mrouteing [vrf vrf-name] [[high-availability | rpf-events [group-address] | timers group-address]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Displays debugging information related to mroute activity associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the <code>vrf-name</code> argument.</td>
</tr>
<tr>
<td><code>high-availability</code></td>
<td>(Optional) Displays high availability (HA) events associated with supervisor engine switchovers on Catalyst 6500 series switches, in Cisco IOS Release 12.2(33)SXH and subsequent 12.2SX releases.</td>
</tr>
<tr>
<td><code>rpf-events</code></td>
<td>(Optional) Displays Reverse Path Forwarding (RPF) events associated with mroutes in the mroute table.</td>
</tr>
<tr>
<td><code>timers</code></td>
<td>(Optional) Displays timer-related events associated with mroutes in the mroute table.</td>
</tr>
<tr>
<td><code>group-address</code></td>
<td>(Optional) IP address or Domain Name System (DNS) name of a multicast group. Entering a multicast group address restricts the output to only display mroute activity associated with the multicast group address specified for the optional <code>group-address</code> argument.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>The <code>rpf-events</code> keyword was added.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>The <code>timers</code> keyword, <code>vrf</code> keyword, and <code>vrf-name</code> argument were added.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>The <code>timers</code> keyword, <code>vrf</code> keyword, and <code>vrf-name</code> argument were added.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH. The <code>high-availability</code> keyword was added in support of the PIM Triggered Joins feature.</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

This command indicates when the router has made changes to the mroute table. Use the `debug ip pim` and `debug ip mrouting` commands consecutively to obtain additional multicast routing information. In addition, use the `debug ip igmp` command to learn why an mroute message is being displayed.

This command generates a substantial amount of output. Use the optional `group-address` argument to limit the output to a single multicast group.

In Cisco IOS 12.2(33)SXH and subsequent 12.2SX releases, the `high-availability` keyword was added in support of the PIM Triggered Joins feature to monitor HA events in the event of a supervisor engine switchover on a Catalyst 6500 series switch. The PIM Triggered Joins feature is an HA multicast enhancement that improves the reconvergence of mroutes after a supervisor engine switchover on a Catalyst 6500 series switch. After a service engine switchover, all instances of PIM running on the newly active supervisor engine will modify the value of the Generation ID (GenID) that is included in PIM hello messages sent to adjacent PIM neighbors. When an adjacent PIM neighbor receives a PIM hello message on an interface with a new GenID, the PIM neighbor will interpret the modified GenID as an indication that all mroutes states on that interface have been lost. A modified GenID, thus, is utilized as a mechanism to alert all adjacent PIM neighbors that PIM forwarding on that interface has been lost, which then triggers adjacent PIM neighbors to send PIM joins for all (*, G) and (S, G) mroute states that use that interface as an RPF interface.

**Examples**

The following is sample output from the `debug ip mrouting` command:

```
Router# debug ip mrouting 224.2.0.1
MRT: Delete {10.0.0.0/8, 224.2.0.1}
MRT: Delete {10.4.0.0/16, 224.2.0.1}
MRT: Delete {10.6.0.0/16, 224.2.0.1}
MRT: Delete {10.9.0.0/16, 224.2.0.1}
MRT: Delete {10.16.0.0/16, 224.2.0.1}
MRT: Create (*, 224.2.0.1), if_input NULL
MRT: Create {224.69.15.0/24, 225.2.2.4}, if_input Ethernet0, RPF nbr 224.69.61.15
MRT: Create {224.69.39.0/24, 225.2.2.4}, if_input Ethernet1, RPF nbr 0.0.0.0
MRT: Create {10.0.0.0/8, 224.2.0.1}, if_input Ethernet1, RPF nbr 224.0.0.0
MRT: Create {10.4.0.0/16, 224.2.0.1}, if_input Ethernet1, RPF nbr 224.0.0.0
MRT: Create {10.6.0.0/16, 224.2.0.1}, if_input Ethernet1, RPF nbr 224.0.0.0
MRT: Create {10.9.0.0/16, 224.2.0.1}, if_input Ethernet1, RPF nbr 224.0.0.0
MRT: Create {10.16.0.0/16, 224.2.0.1}, if_input Ethernet1, RPF nbr 224.0.0.0
```

The following lines show that multicast IP routes were deleted from the routing table:

```
MRT: Delete {10.0.0.0/8, 224.2.0.1}
MRT: Delete {10.4.0.0/16, 224.2.0.1}
MRT: Delete {10.6.0.0/16, 224.2.0.1}
```

The (*, G) entries are generally created by receipt of an Internet Group Management Protocol (IGMP) host report from a group member on the directly connected LAN or by a Protocol Independent Multicast (PIM) join message (in sparse mode) that this router receives from a router that is sending joins toward the Route Processor (RP). This router will in turn send a join toward the RP that creates the shared tree (or RP tree).

```
MRT: Create (*, 224.2.0.1), if_input NULL
```

The following lines are an example of creating an (S, G) entry that shows that an IP multicast packet (mpacket) was received on Ethernet interface 0. The second line shows a route being created for a source that is on a directly connected LAN. The RPF means “Reverse Path Forwarding,” whereby the router looks up the source address of the multicast packet in the unicast routing table and determines which interface will be used to send a packet to that source.
The following lines show that multicast IP routes were added to the routing table. Note the 224.0.0.0 as the RPF, which means the route was created by a source that is directly connected to this router.

If the source is not directly connected, the neighbor address shown in these lines will be the address of the router that forwarded the packet to this router.

The shortest path tree state maintained in routers consists of source (S), multicast address (G), outgoing interface (OIF), and incoming interface (IIF). The forwarding information is referred to as the multicast forwarding entry for (S, G).

An entry for a shared tree can match packets from any source for its associated group if the packets come through the proper incoming interface as determined by the RPF lookup. Such an entry is denoted as (*, G). A (*, G) entry keeps the same information a (S, G) entry keeps, except that it saves the rendezvous point address in place of the source address in sparse mode or as 240.0.0.0 in dense mode.

The table below describes the significant fields shown in the display.

### Table 34: debug ip mrouting Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRT</td>
<td>Multicast route table.</td>
</tr>
<tr>
<td>RPF</td>
<td>Reverse Path Forwarding.</td>
</tr>
<tr>
<td>nbr</td>
<td>Neighbor.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip dvmrp</td>
<td>Displays information on DVMRP packets received and sent.</td>
</tr>
<tr>
<td>debug ip igmp</td>
<td>Displays IGMP packets received and sent, and IGMP host-related events.</td>
</tr>
<tr>
<td>debug ip packet</td>
<td>Displays general IP debugging information and IPSO security transactions.</td>
</tr>
<tr>
<td>debug ip pim</td>
<td>Displays all PIM announcements received.</td>
</tr>
<tr>
<td>debug ip sd</td>
<td>Displays all SD announcements received.</td>
</tr>
</tbody>
</table>
debug ip mroute limits

To display debugging information about configured per interface mroute state limiters and bandwidth-based multicast Call Admission Control (CAC) policies, use the debug ip mroute limits command in privileged EXEC mode. To disable debugging output, use the no form of this command.

**debug ip mroute [vrf vrf-name] limits [group-address]**

**no debug ip mroute [vrf vrf-name] limits [group-address]**

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Logs per interface mroute state limiter and bandwidth-based multicast CAC policy events related to multicast groups associated with the Multicast Virtual Private Network (VPN) routing and forwarding (MVRF) instance specified for the vrf-name argument.</td>
</tr>
<tr>
<td>group-address</td>
<td>(Optional) Multicast group address or group name for which to log per interface mroute state limiter and bandwidth-based multicast CAC policy events.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRB.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command may generate a substantial amount of output. Use the optional group-address argument to restrict the output to display only per interface mroute state limiter and bandwidth-based multicast CAC policy events related to a particular multicast group.

**Examples**

The following output is from the **debug ip mroute limits** command. The output displays the following events:

- An mroute state being created and the corresponding per interface mroute state limiter counter being increased by the default cost of 1 on incoming Ethernet interface 1/0.

- An mroute olist member being removed from the olist and the corresponding per interface mroute limiter being decreased by the default cost of 1 on outgoing Ethernet interface 1/0.

- An mroute being denied by the per interface mroute state limiter because the maximum number of mroute states has been reached.

- An mroute state being created and the corresponding per interface mroute state limiter counter being increased by the cost of 2 on incoming Ethernet interface 1/0.

- An mroute olist member being removed from the olist and the corresponding per interface mroute limiter being decreased by a cost of 2 on outgoing Ethernet interface 1/0.
Router# debug ip mrouting limits

MRL(0): incr-ed acl 'rpf-list' to (13 < max 32), (n:0,p:0), (main) GigabitEthernet0/0, (10.41.0.41, 225.30.200.60)
MRL(0): decr-ed acl 'out-list' to (10 < max 32), (n:0,p:0), (main) GigabitEthernet0/0, (*, 225.40.202.60)
MRL(0): Add mroute (10.43.0.43, 225.30.200.60) denied for GigabitEthernet0/2, acl std-list, (16 = max 16)
MRL(0): incr-ed limit-acl 'rpf-list' to (12 < max 32), cost-acl 'cost-list' cost 2, (n:0,p:0), (main) GigabitEthernet0/0, (10.41.0.41, 225.30.200.60)
MRL(0): decr-ed limit-acl 'out-list' to (8 < max 32), cost-acl 'cost-list'' cost 2, (n:0,p:0), (main) GigabitEthernet0/0, (*, 225.40.202.60)

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip multicast limit</td>
<td>Resets the exceeded counter for per interface mroute state limiters.</td>
</tr>
<tr>
<td>ip multicast limit</td>
<td>Configures per interface mroute state limiters.</td>
</tr>
<tr>
<td>ip multicast limit cost</td>
<td>Applies costs to per interface mroutes state limiters.</td>
</tr>
<tr>
<td>show ip multicast limit</td>
<td>Displays statistics about configured per interface mroute state limiters.</td>
</tr>
</tbody>
</table>
debug ip msdp

To debug Multicast Source Discovery Protocol (MSDP) activity, use the `debug ip msdp` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

### Syntax Description

- **vrf**: (Optional) Supports the Multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
- **vrf-name**: (Optional) Name assigned to the VRF.
- **peer-address | name**: (Optional) The peer for which debug events are logged.
- **detail**: (Optional) Provides more detailed debugging information.
- **routes**: (Optional) Displays the contents of Source-Active messages.

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(23)S</td>
<td>The <code>vrf</code> keyword and <code>vrf-name</code> argument were added.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `debug ip msdp` command:

```
Router# debug ip msdp
MSDP debugging is on
Router#
MSDP: 224.150.44.254: Received 1388-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.254: Received 1028-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1028, ec: 85, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1028-byte SA to peer
MSDP: 224.150.44.254: Received 1388-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
```
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.250: Received 56-byte message from peer
MSDP: 224.150.44.250: SA TLV, len: 56, ec: 4, RP: 205.167.76.241
MSDP: 224.150.44.250: Peer RPF check passed for 205.167.76.241, used EMBGP peer
MSDP: 224.150.44.254: Forward 56-byte SA to peer
MSDP: 224.150.44.254: Received 116-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 116, ec: 9, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
MSDP: 224.150.44.254: Forward 116-byte SA to peer
MSDP: 224.150.44.254: Received 32-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 32, ec: 2, RP: 172.31.3.78
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.78, used EMBGP peer
MSDP: 224.150.44.254: Forward 32-byte SA to peer

The table below describes the significant fields shown in the display.

**Table 35: debug ip msdp Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSDP</td>
<td>Protocol being debugged.</td>
</tr>
<tr>
<td>224.150.44.254:</td>
<td>IP address of the MSDP peer.</td>
</tr>
<tr>
<td>Received 1388-byte</td>
<td>MSDP event.</td>
</tr>
<tr>
<td>message from peer</td>
<td></td>
</tr>
</tbody>
</table>
debug ip msdp resets

To debug Multicast Source Discovery Protocol (MSDP) peer reset reasons, use the `debug ip msdp resets` command in privileged EXEC mode.

```
dump ip msdp [vrf vrf-name] resets
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf</code></td>
<td>(Optional) Supports the Multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td><code>vrf-name</code></td>
<td>(Optional) Name assigned to the VRF.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(23)S</td>
<td>The <code>vrf</code> keyword and <code>vrf-name</code> argument were added.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
debug ip multicast hardware-switching

To display information about multicast hardware switching, use the `debug ip multicast hardware-switching` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip multicast hardware-switching {control group-name | error A.B.C.D | event A.B.C.D | ha-error A.B.C.D | ha-event A.B.C.D}
no debug ip multicast hardware-switching {control group-name | error A.B.C.D | event A.B.C.D | ha-error A.B.C.D | ha-event A.B.C.D}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>control</td>
<td>Displays all multicast hardware switching debugging information, including errors, events, and packets for the specified group.</td>
</tr>
<tr>
<td>group-name</td>
<td>Specifies the selected group.</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Specifies the source or group I.D. address.</td>
</tr>
<tr>
<td>error</td>
<td>Displays error messages related to multicast hardware switching.</td>
</tr>
<tr>
<td>event</td>
<td>Displays the run-time sequence of events for multicast hardware switching.</td>
</tr>
<tr>
<td>ha-error</td>
<td>Displays the run-time sequence of ha-errors for multicast hardware switching.</td>
</tr>
<tr>
<td>ha-event</td>
<td>Displays the run-time sequence of ha-events for multicast hardware switching.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging is not enabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRE</td>
<td>This command was introduced on Cisco 7600 series routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Only one of the keywords is required.

**Examples**

The following example shows output from the `debug ip multicast hardware-switching` command using the `error` keyword:

```
Router# debug ip multicast hardware-switching error 232.0.1.4
PE1-7600#debug ip multicast hardware-switching error 232.0.1.4
CMFIB-RP IPv4 error debugging enabled for group 232.0.1.4
PE1-7600#
```

The following example shows output from the `debug ip multicast hardware-switching` command using the `event` keyword:

```
Router# debug ip multicast hardware-switching event 232.0.1.4
```
The following example shows output from the `debug ip multicast hardware-switching` command using the `ha-event` keyword:

```
Router# debug ip multicast hardware-switching ha-event 232.0.1.4
CMFIB-RP IPv4 ha event debugging enabled for group 232.0.1.4
PE1-7600#
Router#
```

The following example shows output from the `debug ip multicast hardware-switching` command using the `ha-error` keyword:

```
Router# debug ip multicast hardware-switching ha-error 232.0.1.4
CMFIB-RP IPv4 ha error debugging enabled for group 232.0.1.4
Router#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 multicast hardware-switching connected</code></td>
<td>Downloads the interface and mask entry for IPv6 multicast packet.</td>
</tr>
</tbody>
</table>
debug ip multicast redundancy

To display information about IP multicast redundancy events, use the `debug ip multicast redundancy` command in privileged EXEC mode. To disable debugging output for IP multicast redundancy events, use the `no` form of this command.

```
debug ip multicast [{default-vrf | vrf vrf-name}] [group group-address] redundancy [verbose]
no debug ip multicast [{default-vrf | vrf vrf-name}] [group group-address] redundancy [verbose]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-vrf</td>
<td>(Optional) Restricts the logging of IP multicast events associated with Multicast Virtual Private Network routing and forwarding (MVRF) instances to events associated with the default MVRF.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Restricts the logging of IP multicast events associated with MVRFs to events associated with the MVRF specified for the <code>vrf-name</code> argument.</td>
</tr>
<tr>
<td>group group-address</td>
<td>(Optional) Restricts the output for multicast groups to events associated with the multicast group specified for the <code>group-address</code> argument.</td>
</tr>
<tr>
<td>verbose</td>
<td>(Optional) Logs events that may occur frequently during normal operation, but that may be useful for tracking in short intervals.</td>
</tr>
</tbody>
</table>

### Command Default

IP multicast events related to all multicast groups and all MVRFs are displayed. Logging events enabled with the `verbose` keyword are not displayed.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXI</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.6</td>
<td>This command was integrated into Cisco IOS XE Release 2.6.</td>
</tr>
<tr>
<td>15.0(1)S</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)S.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to display IP multicast redundancy events.

This command logs events that are important in verifying nonstop forwarding (NSF) with stateful switchover (SSO) for IP multicast. The classes of events logged by the `debug ip multicast redundancy` command include stateful switchover events during a Route Processor (RP) switchover and dynamic synchronization events that occur during steady state operation.

Use the optional `verbose` keyword to log events that may occur frequently during normal operation, but that may be useful for tracking in short intervals.

### Examples

The following sample output from the `debug ip multicast redundancy` command shows the initial logging messages that display when the system detects an RP switchover:
The following is sample output from the `debug ip multicast redundancy` command. As interfaces come up on the new active RP, unicast convergence occurs in parallel with a multicast route refresh from Protocol Independent Multicast (PIM) neighbors. Unicast convergence is followed by Reverse Path Forwarding (RPF) adjustments to the refreshed mroute information.

*Aug 7 02:31:28.107: MCAST-HA: Triggering unicast convergence notification process handling for all MVRFs
*Aug 7 02:31:28.111: MCAST-HA: Unicast convergence notification has been received for the only unconverged VRF.
Stopping the unicast routing convergence failsafe timer.
*Aug 7 02:31:28.111: MCAST-HA: Unicast convergence notification received for the wildcard tableid (all VRFs).
Triggering RPF updates for all MVRFs and stopping the unicast IGP convergence failsafe timer.
The following is sample output from the `debug ip multicast redundancy` command. After the processing of unicast and multicast route convergence, time is allowed for Internet Group Management Protocol (IGMP) reporting. Following IGMP reporting, the control plane then sends out requests for the Multicast Forwarding Information Base (MFIB) replay of data driven events (DDEs) to retrigger multicast route information that cannot be obtained from PIM neighbors or directly connected hosts. After this processing completes, the control plane waits for the NSF hold-off time period to terminate. The refreshed multicast control plane information is then downloaded to the forwarding plane; once the download is completed, the stale multicast forwarding plane information is subsequently flushed.

*Aug 7 02:31:43.651: MCAST-HA: Sending DDE replay request for MVRF red.
*Aug 7 02:31:43.651: MCAST-HA: MFIB DDE replay completed for mvrf red
*Aug 7 02:31:43.651: MCAST-HA: No NSF Holdoff extension requested for mvrf red at completion of DDE replay.
*Aug 7 02:31:43.651: MCAST-HA: Terminating multicast NSF holdoff for MVRF red
*Aug 7 02:31:43.651: MCAST-HA: Still awaiting MFIB DDE replay for mvrf green DDE replay: NOT COMPLETED, MRIB update: NOT PENDING
*Aug 7 02:31:43.651: MCAST-HA: Sending DDE replay request for MVRF green.
*Aug 7 02:31:43.651: MCAST-HA: MFIB DDE replay completed for mvrf green
*Aug 7 02:31:43.651: MCAST-HA: No NSF Holdoff extension requested for mvrf green at completion of DDE replay.
*Aug 7 02:31:43.651: MCAST-HA: Terminating multicast NSF holdoff for MVRF green
*Aug 7 02:31:43.651: MCAST-HA: Still awaiting MFIB DDE replay for mvrf blue DDE replay: NOT COMPLETED, MRIB update: NOT PENDING
*Aug 7 02:31:43.651: MCAST-HA: Sending DDE replay request for MVRF blue.
*Aug 7 02:31:43.651: MCAST-HA: MFIB DDE replay completed for mvrf blue
*Aug 7 02:31:43.651: MCAST-HA: No NSF Holdoff extension requested for mvrf blue at completion of DDE replay.
The following is sample output from the `debug ip multicast redundancy` command. This output shows the events related to the reloading of the standby RP, in particular, ISSU negotiation between the active and standby RP and synchronization of dynamic multicast forwarding information from the active RP to the standby RP. Synchronization events are also logged in steady state for events that occur that affect dynamic group-to-RP mapping information or dynamic tunnel state.

00:11:50: %HA-6-MODE: Operating RP redundancy mode is SSO
Aug 7 02:32:50.955: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.955: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.955: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.959: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.959: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.959: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.959: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.959: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.963: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.963: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.963: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.963: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.967: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.967: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.967: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.967: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.967: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.967: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.967: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.967: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.967: MCAST-ISSU Negotiation message sent from primary, rc = 0
Aug 7 02:32:50.971: MCAST-ISSU Negotiation completed for PIM Checkpoint Facility client, negotiation rc = 4, negotiation result = COMPATIBLE
Aug 7 02:32:59.927: MCAST-HA-RF: Progression event: RF_Event=RF_PROG_STANDBY_FILESYS
RFState=ACTIVE
Aug 7 02:32:59.963: MCAST-HA-RF: Progression event: RF_Event=RF_PROG_STANDBY_BULK
RFState=ACTIVE
Aug 7 02:32:59.963: MCAST-HA: Successfully created the bulk sync process
Aug 7 02:32:59.963: MCAST-HA: Starting Bulk sync
Aug 7 02:32:59.963: MCAST HA Executing BSR cache bulk sync.
Aug 7 02:32:59.963: MCAST-HA BSR cache sync request received for mvrf IPv4 default
Aug 7 02:32:59.963: MCAST-HA: Allocating Bootstrap cache sync request sync request
search for mvrf IPv4 default result is 0 mvrf at 0x4A21680
Aug 7 02:32:59.971: MCAST-HA BSR cache sync request received for mvrf blue
Aug 7 02:32:59.971: MCAST-HA: Allocating Bootstrap cache sync request sync request
search for mvrf blue result is 0 mvrf at 0x50EE660
Aug 7 02:32:59.983: MCAST-HA BSR cache sync request received for mvrf green
Aug 7 02:32:59.991: MCAST-HA: Allocating Bootstrap cache sync request sync request
search for mvrf green result is 0 mvrf at 0x5103300
Aug 7 02:33:00.003: MCAST HA Executing AutoRP discovery IDB bulk sync.
Aug 7 02:33:00.003: MCAST-HA AutoRP discovery IDB sync request received for mvrf IPv4 default
Aug 7 02:33:00.003: MCAST-HA: Creating Autorp discovery IDB sync request chunk size=112 max=585 align=8
Aug 7 02:33:00.011: MCAST-HA AutoRP discovery IDB sync request received for mvrf blue
Aug 7 02:33:00.011: MCAST-HA: Allocating Autorp discovery IDB sync request sync request
search for mvrf IPv4 default result is 0 mvrf at 0x4A21680
Aug 7 02:33:00.023: MCAST-HA AutoRP discovery IDB sync request received for mvrf green
Aug 7 02:33:00.023: MCAST-HA: Allocating AutoRP discovery IDB sync request sync request
search for mvrf green result is 0 mvrf at 0x5103300
Aug 7 02:33:00.023: MCAST-HA Formatting AutoRP discovery IDB sync message:
sync request received for mvrf red
Aug 7 02:33:00.031: MCAST-HA: Allocating AutoRP discovery IDB sync request sync request
search for mvrf red result is 0 mvrf at 0x5135FE0
Aug 7 02:33:00.031: MCAST-HA AutoRP discovery IDB sync request received for mvrf red
Aug 7 02:33:00.031: MCAST-HA Formatting AutoRP discovery IDB sync message:
sync request received for mvrf red
Aug 7 02:33:00.043: MCAST-HA Executing dummy bulk sync function.
Aug 7 02:33:00.043: MCAST-HA Executing dummy bulk sync function.
Aug 7 02:33:00.043: MCAST-HA Executing MDT tunnel bulk sync.
Aug 7 02:33:00.043: MCAST-HA MDT tunnel sync request received for mvrf blue
Aug 7 02:33:00.043: MCAST-HA: Creating MDT tunnel sync request chunk size=112 max=585
align=8
Aug 7 02:33:00.043: MCAST-HA: Allocating MDT tunnel sync request sync request
search for mvrf blue result is 0 mvrf at 0x50EE660
Aug 7 02:33:00.043: MCAST-HA MDT tunnel sync request received for mvrf green
Aug 7 02:33:00.043: MCAST-HA: Allocating MDT tunnel sync request sync request
search for mvrf green result is 0 mvrf at 0x5103300
Aug 7 02:33:00.043: MCAST-HA MDT tunnel sync request received for mvrf red
Aug 7 02:33:00.043: MCAST-HA: Allocating MDT tunnel sync request sync request
search for mvrf red result is 0 mvrf at 0x5135FE0
Aug 7 02:33:00.071: MCAST-HA: Executing Bidir RP DF bulk sync.
Aug 7 02:33:00.071: MCAST-HA: Executing register tunnel bulk sync.
Aug 7 02:33:00.071: MCAST-HA: Completed enqueuing of bulk sync messages.
Aug 7 02:33:00.071: MCAST-HA: Bulk sync message queue has drained.
Aug 7 02:33:00.071: MCAST-HA: Received acknowledgement from standby for all bulk sync messages.
Aug 7 02:33:00.071: MCAST-HA Creating bulk sync completion message for peer.
Aug 7 02:33:00.071: MCAST-HA: Primary has notified standby of bulk sync completion. Waiting for final bulk sync ACK from stby.
Aug 7 02:33:00.075: MCAST-HA: Received cf status CHKPT_STATUS_SEND_OK
Aug 7 02:33:00.075: MCAST-HA: Sent message type is 2
Aug 7 02:33:00.075: MCAST-HA Searching for sync request corresponding to the successfully received message.
Aug 7 02:33:00.075: MCAST-HA Transmission from primary and reception by standby confirmed for sync type 2. Cleanup is complete.
Aug 7 02:33:00.075: MCAST-HA: Received cf status CHKPT_STATUS_SEND_OK
Aug 7 02:33:00.075: MCAST-HA: Sent message type is 2
Aug 7 02:33:00.075: MCAST-HA Searching for sync request corresponding to the successfully received message.
Aug 7 02:33:00.075: MCAST-HA Transmission from primary and reception by standby confirmed for sync type 2. Cleanup is complete.
Aug 7 02:33:00.075: MCAST-HA: Received cf status CHKPT_STATUS_SEND_OK
Aug 7 02:33:00.075: MCAST-HA: Sent message type is 2
Aug 7 02:33:00.075: MCAST-HA Searching for sync request corresponding to the successfully received message.
Aug 7 02:33:00.075: MCAST-HA Transmission from primary and reception by standby confirmed for sync type 2. Cleanup is complete.
Aug 7 02:33:00.075: MCAST-HA: Received cf status CHKPT_STATUS_SEND_OK
Aug 7 02:33:00.075: MCAST-HA: Sent message type is 2
Aug 7 02:33:00.075: MCAST-HA Searching for sync request corresponding to the successfully received message.
Aug 7 02:33:00.075: MCAST-HA Transmission from primary and reception by standby confirmed for sync type 2. Cleanup is complete.
Aug 7 02:33:00.075: MCAST-HA: Received cf status CHKPT_STATUS_SEND_OK
Aug 7 02:33:00.075: MCAST-HA: Sent message type is 3
Aug 7 02:33:00.075: MCAST-HA Searching for sync request corresponding to the successfully received message.
Aug 7 02:33:00.075: MCAST-HA Transmission from primary and reception by standby confirmed for sync type 2. Cleanup is complete.
Aug 7 02:33:00.075: MCAST-HA: Received cf status CHKPT_STATUS_SEND_OK
Aug 7 02:33:00.075: MCAST-HA: Sent message type is 3
Aug 7 02:33:00.075: MCAST-HA Searching for sync request corresponding to the successfully received message.
Aug 7 02:33:00.075: MCAST-HA Transmission from primary and reception by standby confirmed for sync type 2. Cleanup is complete.
Aug 7 02:33:00.075: MCAST-HA: Received cf status CHKPT_STATUS_SEND_OK
Aug 7 02:33:00.075: MCAST-HA: Sent message type is 3
Aug 7 02:33:00.075: MCAST-HA Searching for sync request corresponding to the successfully received message.
for sync type 3. Cleanup is complete.
*Aug 7 02:33:00.087: MCAST-HA: Received cf status CHKPT_STATUS_SEND_OK
*Aug 7 02:33:00.087: MCAST-HA: Sent message type is 3
*Aug 7 02:33:00.087: MCAST-HA Searching for sync request corresponding to the successfully received message.
*Aug 7 02:33:00.087: MCAST-HA Transmission from primary and reception by standby confirmed for sync type 3. Cleanup is complete.
*Aug 7 02:33:00.087: MCAST-HA: Received cf status CHKPT_STATUS_SEND_OK
*Aug 7 02:33:00.087: MCAST-HA: Sent message type is 3
*Aug 7 02:33:00.087: MCAST-HA Searching for sync request corresponding to the successfully received message.
*Aug 7 02:33:00.087: MCAST-HA Transmission from primary and reception by standby confirmed for sync type 3. Cleanup is complete.
*Aug 7 02:33:00.087: MCAST-HA: Received cf status CHKPT_STATUS_SEND_OK
*Aug 7 02:33:00.087: MCAST-HA: Sent message type is 3
*Aug 7 02:33:00.087: MCAST-HA Searching for sync request corresponding to the successfully received message.
*Aug 7 02:33:00.087: MCAST-HA Transmission from primary and reception by standby confirmed for sync type 3. Cleanup is complete.
*Aug 7 02:33:00.087: MCAST-HA: Received cf status CHKPT_STATUS_SEND_OK
*Aug 7 02:33:00.087: MCAST-HA: Sent message type is 8
*Aug 7 02:33:00.087: MCAST-HA Searching for sync request corresponding to the successfully received message.
*Aug 7 02:33:00.087: MCAST-HA Transmission from primary and reception by standby confirmed for sync type 8. Cleanup is complete.
*Aug 7 02:33:00.087: MCAST-HA: Received cf status CHKPT_STATUS_SEND_OK
*Aug 7 02:33:00.087: MCAST-HA: Sent message type is 8
*Aug 7 02:33:00.087: MCAST-HA Searching for sync request corresponding to the successfully received message.
*Aug 7 02:33:00.087: MCAST-HA Transmission from primary and reception by standby confirmed for sync type 8. Cleanup is complete.
*Aug 7 02:33:00.087: MCAST-HA: Received cf status CHKPT_STATUS_SEND_OK
*Aug 7 02:33:00.087: MCAST-HA: Sent message type is 8
*Aug 7 02:33:00.087: MCAST-HA Searching for sync request corresponding to the successfully received message.
*Aug 7 02:33:00.087: MCAST-HA Transmission from primary and reception by standby confirmed for sync type 8. Cleanup is complete.
*Aug 7 02:33:00.087: MCAST-HA: Received cf status CHKPT_STATUS_SEND_OK
*Aug 7 02:33:00.087: MCAST-HA: Sent message type is 11
*Aug 7 02:33:00.087: MCAST-HA Process: Primary RP received standby ACK for reception of bulk sync completion message.
*Aug 7 02:33:00.087: MCAST-HA Notifying RF to continue progression.
*Aug 7 02:33:00.087: MCAST-HA: Wakeup received for bulk sync completion.
  major = 4, minor = 2.
  *Aug 7 02:33:00.091: MCAST-HA Process: Primary RP received bulk sync completion confirmation from standby.
  *Aug 7 02:33:00.091: MCAST-HA RF notification previously sent.
  *Aug 7 02:33:00.455: MCAST-HA-RF: Progression event: RF_Event=RF_PROG_STANDBY_HOT
RFState=ACTIVE
00:12:05: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeeded
00:12:05: %HA-6-STANDBY_READY: Standby RP in slot 7 is operational in SSO mode
00:12:05: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
debug ip multicast rpf tracked

To enable debugging output for IP multicast Return Path Forwarding (RPF) tracked events, use the `debug ip multicast rpf tracked` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
d debug ip multicast rpf tracked
no debug ip multicast rpf tracked
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command when IP multicast RPF appears not to be functioning.

**Examples**

The following example shows how to enable debugging output for IP multicast RPF tracked events:

```
Router# debug ip multicast rpf tracked
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip multicast rpf tracked</code></td>
<td>Displays IP multicast RPF tracked information.</td>
</tr>
</tbody>
</table>
debug ip multicast topology

To enable debugging output for IP multicast stream topology creation events, deletion events, and IP multicast stream access control list (ACL) matching events, use the debug ip multicast topology command in privileged EXEC mode. To disable debugging output, use the no form of this command.

```
debug ip multicast topology
no debug ip multicast topology
```

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.2S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command when IP multicast stream topology creation, IP multicast stream topology deletion, or IP multicast stream ACL matching appears not to be functioning.

Examples

The following example shows how to enable debugging output for IP multicast stream topology creation events, IP multicast stream topology deletion events, and IP multicast stream ACL matching events:

```
Router# debug ip multicast topology
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip multicast rpf select topology</td>
<td>Associates a multicast topology with a multicast group with a specific mroute entry.</td>
</tr>
<tr>
<td>ip multicast topology</td>
<td>Configures topology selection for multicast streams.</td>
</tr>
<tr>
<td>show ip multicast topology</td>
<td>Displays IP multicast topology information.</td>
</tr>
</tbody>
</table>
### debug ip nat

To display information about IP packets translated by the IP Network Address Translation (NAT) feature, use the `debug ip nat` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
[debug ip nat] [access-list] [cce] [detailed] [h323] [error] [fragment] [generic] [ipsec] [multipart] [nvi] [piggy-back] [port] [pptp] [route] [sbc] [sip] [skinny] [tcp-alg] [vrf] [wlan-nat]
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list</code></td>
<td>(Optional) Standard IP access list number. If the datagram is not permitted by the specified access list, the related debugging output is suppressed.</td>
</tr>
<tr>
<td><code>cce</code></td>
<td>(Optional) Displays debug information for all Common Classification Engine (CCE) events.</td>
</tr>
<tr>
<td><code>detailed</code></td>
<td>(Optional) Displays debugging information in a detailed format.</td>
</tr>
<tr>
<td><code>h323</code></td>
<td>(Optional) Displays H.225, H.245, and H.323 protocol information.</td>
</tr>
<tr>
<td><code>error</code></td>
<td>(Optional) Displays debug information for error conditions in NAT-Application Layer Gateway (ALG) segmentation with Layer 4 forwarding.</td>
</tr>
<tr>
<td><code>fragment</code></td>
<td>(Optional) Displays fragment events.</td>
</tr>
<tr>
<td><code>generic</code></td>
<td>(Optional) Displays generic ALG handler events.</td>
</tr>
<tr>
<td><code>ipsec</code></td>
<td>(Optional) Displays IPsec packet information.</td>
</tr>
<tr>
<td><code>multipart</code></td>
<td>(Optional) Displays multipart processing information.</td>
</tr>
<tr>
<td><code>nvi</code></td>
<td>(Optional) Displays NAT Virtual Interface (NVI) events.</td>
</tr>
<tr>
<td><code>piggy-back</code></td>
<td>(Optional) Displays piggyback support events.</td>
</tr>
<tr>
<td><code>port</code></td>
<td>(Optional) Displays port information.</td>
</tr>
<tr>
<td><code>pptp</code></td>
<td>(Optional) Displays Point-to-Point Tunneling Protocol (PPTP) information.</td>
</tr>
<tr>
<td><code>route</code></td>
<td>(Optional) Displays route information.</td>
</tr>
<tr>
<td><code>sbc</code></td>
<td>(Optional) Displays NAT Session Initiation Protocol (SIP) Session Border Controller (SBC) events.</td>
</tr>
<tr>
<td><code>sip</code></td>
<td>(Optional) Displays SIP information.</td>
</tr>
<tr>
<td><code>skinny</code></td>
<td>(Optional) Displays skinny protocol debug information.</td>
</tr>
<tr>
<td><code>tcp-alg</code></td>
<td>(Optional) Displays debug information for NAT-ALG segmentation with Layer 4 forwarding.</td>
</tr>
<tr>
<td><code>vrf</code></td>
<td>(Optional) Displays VPN routing and forwarding (VRF) traffic-related information.</td>
</tr>
<tr>
<td><code>wlan-nat</code></td>
<td>(Optional) Displays Wireless LAN (WLAN) information.</td>
</tr>
</tbody>
</table>
Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(5)T</td>
<td>This command was modified. The h323 keyword was added.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td>This command was modified. The sip keyword was added.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was modified. The ipsec and vrf keywords were added.</td>
</tr>
<tr>
<td>12.3(2)XE</td>
<td>This command was modified. The wlan-nat keyword was added.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>This command was modified. The wlan-nat keyword was implemented in Cisco IOS Release 12.3(7)T.</td>
</tr>
<tr>
<td>12.3(11)T</td>
<td>This command was modified. The output of the h323 keyword was expanded to include H.245 tunneling.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was modified. The multipart keyword was added.</td>
</tr>
<tr>
<td>15.1(3)T</td>
<td>This command was modified. The cce keyword was removed and the tcp-alg keyword was added.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The NAT feature reduces the need for unique, registered IP addresses. It can also save private network administrators from needing to renumber the hosts and routers that do not conform to global IP addressing.

Use the debug ip nat command to verify the operation of the NAT feature by displaying information about each packet that the router translates. The debug ip nat detailed command generates a description of each packet considered for translation. This command also displays information about certain errors or exception conditions, such as the failure to allocate a global address. To display messages related to the processing of H.225 signaling and H.245 messages, use the debug ip nat h323 command. To display messages related to the processing of SIP messages, use the debug ip nat sip command. To display messages related to the processing of VRF messages, use the debug ip nat vrf command. To display messages related to the processing of SIP multipart messages, use the debug ip nat sip command.

Caution

Because the debug ip nat command generates a substantial amount of output, use it only when traffic on the IP network is low, so that the other activity on the system is not adversely affected.

Examples

The following is sample output from the debug ip nat command. In this example, the first two lines show the Domain Name System (DNS) request and reply debugging output. The remaining lines show debugging output from a Telnet connection from a host on the inside of the network to a host on the outside of the network. All Telnet packets, except for the first packet, were translated in the fast path, as indicated by the asterisk (*).

Router# debug ip nat
The table below describes the significant fields shown in the display.

Table 36: debug ip nat Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT</td>
<td>Indicates that the packet is being translated by NAT. An asterisk (*) indicates that the translation is occurring in the fast path. The first packet in a conversation always goes through the slow path (that is, it is process switched). The remaining packets go through the fast path if a cache entry exists.</td>
</tr>
<tr>
<td>s=192.0.2.1-&gt;203.0.112.1</td>
<td>Source address of the packet and how it is being translated.</td>
</tr>
<tr>
<td>d=203.0.112.254</td>
<td>Destination address of the packet.</td>
</tr>
<tr>
<td>[6825]</td>
<td>IP identification number of the packet. Might be useful in the debugging process to correlate with other packet traces from protocol analyzers.</td>
</tr>
</tbody>
</table>

The following is sample output from the debug ip nat detailed command. In this example, the first two lines show the debugging output produced by a DNS request and reply. The remaining lines show the debugging output from a Telnet connection from a host on the inside of the network to a host on the outside of the network. In this example, the inside host 192.168.1.95 was assigned the global address 172.31.233.193. The output fields are self-explanatory.

Router# debug ip nat detailed
NAT: i: udp (192.168.1.95, 1493) -> (172.31.2.132, 53) [22399]
NAT: o: udp (172.31.2.132, 53) -> (172.31.233.193, 1493) [63671]
NAT*: i: tcp (192.168.1.95, 1135) -> (172.31.2.75, 23) [22400]
NAT*: o: tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22002]
NAT*: i: tcp (192.168.1.95, 1135) -> (172.31.2.75, 23) [22401]
NAT*: o: tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22060]
NAT*: o: tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22071]

The following is sample output from the debug ip nat h323 command. In this example, an H.323 call is established between two hosts, one host on the inside and the other host on the outside of the network. The debugging output displays the H.323 message names that NAT recognizes and the embedded IP addresses contained in those messages.

Router# debug ip nat h323
NAT:H225: [0] processing a Setup message
NAT:H225: [0] found Setup sourceCallSignalling
NAT:H225: [0] fix transportAddress addr=192.168.122.50 port=11140
NAT:H225: [0] found Setup fastStart
NAT:H225: [0] Setup fastStart PDU length:18
NAT:H245: [0] processing OpenLogicalChannel message, forward channel number 1
NAT:H245: [0] found OLC forward mediaControlChannel
The table below describes the significant fields shown in the display.

**Table 37: debug ip nat h323 Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT</td>
<td>Indicates that the packet is being translated by NAT.</td>
</tr>
<tr>
<td>[0]</td>
<td>Indicates that the packet is moving from a host outside the network to one host inside the network.</td>
</tr>
<tr>
<td>[1]</td>
<td>Indicates that the packet is moving from a host inside the network to one host outside the network.</td>
</tr>
</tbody>
</table>

The following is sample output from the `debug ip nat ipsec` command. The output fields are self-explanatory.

```
Router# debug ip nat ipsec
5d21h:NAT:new IKE going In->Out, source addr 192.168.122.35, destination addr 192.168.22.20, initiator cookie 0x9C4206D5
5d21h:NAT:IPSec:created In->Out ESP translation IL=192.168.122.35 SPI=0xAEE32A0A, IG=192.168.22.40, OL=192.168.22.20, OG=192.168.22.20
5d21h:NAT:IPSec:created Out->In ESP translation OG=192.168.22.20 SPI=0xA64B5BB6,
```
The following is sample output from the `debug ip nat sip` command. In this example, one IP phone registers with a Cisco SIP proxy and then calls another IP phone. The debugging output displays the SIP messages that NAT recognizes and the embedded IP addresses contained in those messages.

```
Router# debug ip nat sip
NAT:SIP:[0] processing REGISTER message
NAT:SIP:[0] translated embedded address 192.168.122.3->10.1.1.1
NAT:SIP:[0] translated embedded address 192.168.122.3->10.1.1.1
NAT:SIP:[0] message body found
NAT:SIP:[0] found address/port in SDP body:192.168.122.20 20332
NAT:SIP:[1] processing SIP/2.0 100 Trying reply message
NAT:SIP:[1] translated embedded address 10.1.1.1->192.168.122.3
NAT:SIP:[1] processing SIP/2.0 200 OK reply message
NAT:SIP:[1] translated embedded address 10.1.1.1->192.168.122.3
NAT:SIP:[1] translated embedded address 10.1.1.1->192.168.122.3
NAT:SIP:[1] message body found
NAT:SIP:[1] found address/port in SDP body:192.168.22.20
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT</td>
<td>Indicates that the packet is being translated by NAT.</td>
</tr>
<tr>
<td>SIP</td>
<td>Protocol of the packet.</td>
</tr>
<tr>
<td>[0]</td>
<td>Indicates that the packet is moving from a host outside the network to one host inside the network.</td>
</tr>
<tr>
<td>[1]</td>
<td>Indicates that the packet is moving from a host inside the network to one host outside the network.</td>
</tr>
</tbody>
</table>

The following is sample output from the `debug ip nat tcp-alg` command:

```
Router# debug ip nat tcp-alg
```
*Oct 6 04:56:13.411: NAT-L4F : Still in the spoofing mode, tcpflags = 0x4
*Oct 6 04:56:13.411: NAT-L4F : Close notify from L4F
*Oct 6 04:56:23.807: NAT-L4F: received fd1: 1073741825 and tcp flags = 0x2, payload_len = 0
*Oct 6 04:56:23.807: NAT-L4F: received fd2: 1073741826 and tcp flags = 0x12, payload_len = 0
*Oct 6 04:56:23.807: NAT-L4F: received fd1: 1073741825 and tcp flags = 0x10
*Oct 6 04:56:23.811: NAT-L4F:Translationing to proxy: rc 0 error 0
*Oct 6 04:56:23.811: NAT-L4F: Successfully proxied this flow
*Oct 6 04:56:23.811: NAT-L4F: remaining_hdr_sz=0
*Oct 6 04:56:23.811: NAT-L4F: remaining_payl_sz=0
*Oct 6 04:56:23.811: NAT-L4F: tcp_alg_state=0
*Oct 6 04:56:23.811: NAT-L4F: complete_msg_len=12
*Oct 6 04:56:23.811: l4f_send returns 12 bytes
*Oct 6 04:56:23.811: Complete buffer written to proxy
*Oct 6 04:56:23.811: NAT-L4F: NO DATA to read
*Oct 6 04:56:24.027: NAT-L4F: lookup=0 l7_bytes_recd=56 appl_type=5
*Oct 6 04:56:24.027: NAT-L4F: Skinny l7_msg_size = 56
*Oct 6 04:56:24.027: NAT-L4F: after state machine:
*Oct 6 04:56:24.027: NAT-L4F: remaining_hdr_sz=0
*Oct 6 04:56:24.027: NAT-L4F: remaining_payl_sz=0
*Oct 6 04:56:24.027: NAT-L4F: tcp_alg_state=0
*Oct 6 04:56:24.027: NAT-L4F: complete_msg_len=56
*Oct 6 04:56:24.027: l4f_send returns 56 bytes
*Oct 6 04:56:24.027: Complete buffer written to proxy
*Oct 6 04:56:24.027: NO DATA to read
*Oct 6 04:56:24.239: NAT-L4F: received fd1: 1073741825 and tcp flags = 0x10
*Oct 6 04:56:24.239: NAT-L4F: Successfully proxied this flow
*Oct 6 04:56:24.239: NAT-L4F: remaining_hdr_sz=0
*Oct 6 04:56:24.239: NAT-L4F: remaining_payl_sz=0
*Oct 6 04:56:24.239: NAT-L4F: tcp_alg_state=0
*Oct 6 04:56:24.239: NAT-L4F: complete_msg_len=16
*Oct 6 04:56:24.239: l4f_send returns 16 bytes
*Oct 6 04:56:24.239: Complete buffer written to proxy
*Oct 6 04:56:24.239: NO DATA to read
*Oct 6 04:56:24.239: NAT-L4F:setting ALG_NEEDED flag in subblock
*Oct 6 04:56:24.239: NAT-L4F: Skinny l7_msg_size = 116
*Oct 6 04:56:24.239: NAT-L4F: after state machine:
*Oct 6 04:56:24.239: NAT-L4F: remaining_hdr_sz=0
*Oct 6 04:56:24.239: NAT-L4F: remaining_payl_sz=0
*Oct 6 04:56:24.239: NAT-L4F: tcp_alg_state=0
*Oct 6 04:56:24.239: NAT-L4F: complete_msg_len=116
*Oct 6 04:56:24.239: l4f_send returns 116 bytes
*Oct 6 04:56:24.239: Complete buffer written to proxy
*Oct 6 04:56:24.239: NO DATA to read
*Oct 6 04:56:24.239: NAT-L4F:setting ALG_NEEDED flag in subblock
*Oct 6 04:56:24.239: NAT-L4F: lookup=0 l7_bytes_recd=32 appl_type=5
*Oct 6 04:56:24.239: NAT-L4F: Skinny l7_msg_size = 32
The table below describes the significant fields shown in the display.

**Table 39: debug ip nat tcp-alg Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT-L4F</td>
<td>Indicates that the packet is being processed by the NAT-ALG interface with Layer 4 forwarding.</td>
</tr>
<tr>
<td>NAT-ALG</td>
<td>Indicates that the packet is being processed by NAT-ALG.</td>
</tr>
</tbody>
</table>

The following is sample output from the `debug ip nat vrf` command:

```
Router# debug ip nat vrf
6d00h:NAT:address not stolen for 192.168.121.113, proto 1 port 7224
6d00h:NAT:creating portlist proto 1 globaladdr 10.1.1.10
6d00h:NAT:Allocated Port for 192.168.121.113 -> 10.1.1.10: wanted 7224 got 7224
6d00h:NAT:i:icmp (192.168.121.113, 7224) -> (172.28.88.2, 7224) [2460]
6d00h:NAT:s=192.168.121.113->10.1.1.10, d=172.28.88.2 [2460] vrf=> shop
6d00h:NAT*:o:icmp (172.28.88.2, 7224) -> (10.1.1.10, 7224) [2460] vrf=> shop
6d00h:NAT*:s=172.28.88.2, d=10.1.1.10->192.168.121.113 [2460] vrf=> shop
6d00h:NAT:Allocated Port for 192.168.121.113 -> 10.1.1.10: wanted 7225 got 7225
6d00h:NAT:Allocated Port for 192.168.121.113 -> 10.1.1.10: wanted 7226 got 7226
6d00h:NAT*:o:icmp (192.168.121.113, 7225) -> (172.28.88.2, 7225) [2461]
6d00h:NAT:s=192.168.121.113->10.1.1.10, d=172.28.88.2 [2461] vrf=> shop
6d00h:NAT*:o:icmp (172.28.88.2, 7225) -> (10.1.1.10, 7225) [2461] vrf=> shop
6d00h:NAT*:s=172.28.88.2, d=10.1.1.10->192.168.121.113 [2461] vrf=> shop
6d00h:NAT:Allocated Port for 192.168.121.113 -> 10.1.1.10: wanted 7226 got 7226
6d00h:NAT:Allocated Port for 192.168.121.113 -> 10.1.1.10: wanted 7226 got 7226
6d00h:NAT:Allocated Port for 192.168.121.113 -> 10.1.1.10: wanted 7226 got 7226
6d00h:NAT:Allocated Port for 192.168.121.113 -> 10.1.1.10: wanted 7226 got 7226
6d00h:NAT:Allocated Port for 192.168.121.113 -> 10.1.1.10: wanted 7226 got 7226
```

The table below describes the significant fields shown in the display.

**Table 40: debug ip nat vrf Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT</td>
<td>Indicates that the packet is being translated by NAT.</td>
</tr>
<tr>
<td>s=192.168.121.113-&gt;10.1.1.10</td>
<td>Source address of the packet and how it is being translated.</td>
</tr>
<tr>
<td>d=172.28.88.2</td>
<td>Destination address of the packet.</td>
</tr>
<tr>
<td>[2460]</td>
<td>IP identification number of the packet.</td>
</tr>
<tr>
<td>vrf=&gt;</td>
<td>Indicates that NAT is applied to a particular VPN.</td>
</tr>
</tbody>
</table>

The following is sample output from the `debug ip nat wlan-nat` command:
Router# **debug ip nat wlan-nat**
WLAN-NAT: Creating secure ARP entry (10.1.1.1,0010.7bc2.9ff6)
WLAN-NAT: Triggered Acct Start for (209.165.201.1,0010.7bc2.9ff6)
WLAN-NAT: Extracting addr:209.165.201.1,input_idb:Ethernet1/2 from pak
WLAN-NAT: Saving address:209.165.201.1,input_idb:Ethernet1/2 in pak

After the WLAN-entry times out, the following debugs will be seen:

WLAN-NAT: Removing secure arp entry (10.1.1.1,0010.7bc2.9ff6)
WLAN-NAT: triggered Acct Stop for (209.165.201.1,0010.7bc2.9ff6)

The table below describes the significant fields shown in the display.

**Table 41: debug ip nat wlan-nat Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN</td>
<td>Indicates that a wireless LAN is being translated.</td>
</tr>
<tr>
<td>NAT</td>
<td>Indicates that the packet is being translated using NAT.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip nat translation</td>
<td>Clears dynamic NAT translations from the translation table.</td>
</tr>
<tr>
<td>ip nat</td>
<td>Designates that traffic originating from or destined for an interface is subject to NAT.</td>
</tr>
<tr>
<td>ip nat inside destination</td>
<td>Enables NAT of the inside destination address.</td>
</tr>
<tr>
<td>ip nat inside source</td>
<td>Enables NAT of the inside source address.</td>
</tr>
<tr>
<td>ip nat outside source</td>
<td>Enables NAT of the outside source address.</td>
</tr>
<tr>
<td>ip nat pool</td>
<td>Defines a pool of IP addresses for NAT.</td>
</tr>
<tr>
<td>ip nat service</td>
<td>Enables a port other than the default port.</td>
</tr>
<tr>
<td>show ip nat statistics</td>
<td>Displays NAT statistics.</td>
</tr>
<tr>
<td>show ip nat translations</td>
<td>Displays active NAT translations.</td>
</tr>
</tbody>
</table>
debug ip nat redundancy

To enable debugging output for the IP Network Address Translation (NAT) redundancy, use the `debug ip nat redundancy` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip nat redundancy {rf | db} [errors] | messages | {detailed | errors} | cf | packets
no debug ip nat redundancy {rf | db} [errors] | messages | {detailed | errors} | cf | packets
```

**Syntax Description**

- `rf` Specifies debugging for Redundancy Framework (RF).
- `db` Specifies debugging for the database.
- `errors` Specifies debugging for errors cases.
- `messages` Specifies debugging for messages.
- `detailed` Specifies detailed debugging for messages.
- `cf` Specifies debugging for the checkpointing facility.
- `packets` Specifies debugging for packet information.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3(2T)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ip nat redundancy` command to enable debugging output for NAT redundancy.

The following example shows how to enable debugging output for CF.

```
Device# debug ip nat redundancy cf
IP NAT HA Checkpointing Facility debugging is on
Device# show debugging
*Nov 6 18:41:42.669: NAT-HA-CF: ipnat_ha_cf_msg_callback cf_hndl=33554611 ent_hndl=0
cf_msg=0xE4007230
*Nov 6 18:41:42.669: NAT-HA-CF: Received msg: payload=0xE4007270 len=152
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip nat redundancy</td>
<td>Displays NAT redundancy information.</td>
</tr>
<tr>
<td>show ip nat translations redundancy</td>
<td>Displays active NAT translations.</td>
</tr>
</tbody>
</table>
debug ip nbar trace

To enable detailed debugging of packets per flow on a data plane, use the `debug ip nbar trace` command in privileged EXEC mode. To disable debugging, use the `no` form of this command.

```
detail acl-name [packets] [packets-per-flow] summary [number-of-flows]
```

---

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Enables detailed debugging of packets per flow.</td>
</tr>
<tr>
<td>acl-name</td>
<td>Specifies the name of the access control list (ACL) configured on the device.</td>
</tr>
<tr>
<td>packets</td>
<td>(Optional) Specifies the total number of packets.</td>
</tr>
<tr>
<td>packets-per-flow</td>
<td>(Optional) Specifies the number of packets in a flow.</td>
</tr>
<tr>
<td>summary</td>
<td>Captures Network-Based Application Recognition (NBAR) classification summary.</td>
</tr>
<tr>
<td>number-of-flows</td>
<td>(Optional) Specifies the number of flows.</td>
</tr>
</tbody>
</table>

---

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(4)M</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An ACL name must be configured and NBAR must be enabled.

**Examples**

The following is sample output from the `debug ip nbar trace detail acl 100 200` command:

```
Device# debug ip nbar trace detail acl 100 200

Graph Id 1
Classification: 82, flag: 163
Packet No: 1
String: Searching Source V4 WKP
String: Searching Destination V4 WKP
String: Entering loop core from Heuristic RegEx
State Node:http-verify-heuristic-entry-point-get
State Node:http-verify-heuristic-entry-point-get
State Node:HTTP-url-get-check
State Node:HTTP-url-get-check
State Node:HTTP-url-get-check
State Node:HTTP-url-get-check
State Node:youtube-found-url
State Node:http-check-url-fe
State Node:HTTP-request-advance-packet-pointer-to-next-http-header
State Node:HTTP-request-advance-packet-pointer-to-next-http-header
```
State Node: HTTP-request-advance-packet-pointer-to-next-http-header
State Node: HTTP-request-end-of-request-check
State Node: HTTP-request-check-end-of-packet
State Node: HTTP-request-check-end-of-packet
State Node: HTTP-request-headers-parser
State Node: HTTP-request-headers-parser

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip nbar trace</td>
<td>Displays the path traversed by a packet.</td>
</tr>
</tbody>
</table>
**debug ip nbar clients**

To enable debugging of application programming interfaces (APIs) pertaining to Network-Based Application Recognition (NBAR) on a control plane, use the **debug ip nbar clients** command in privileged EXEC mode. To disable debugging, use the **no** form of the command.

```
debug ip nbar clients {high | low | medium}
no debug ip nbar clients
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>high</th>
<th>Enables high-level debugging.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>low</td>
<td>Enables low-, medium-, and high-level debugging.</td>
</tr>
<tr>
<td></td>
<td>medium</td>
<td>Enables medium- and low-level debugging.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(4)M</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

NBAR must be enabled for debugging.

**Examples**

The following is sample output from the **debug ip nbar clients low** command:

```
Device# debug ip nbar clients low

*May 14 08:33:37.468: STILE:CLIENT:LOW: intf list: Interface not found
*May 14 08:33:37.468: STILE:CLIENT:LOW: intf list: Interface not found
*May 14 08:33:37.468: STILE:CLIENT:LOW: intf list: Interface not found
*May 14 08:33:37.468: STILE:CLIENT:LOW: intf list: Interface not found
*May 14 08:33:37.468: STILE:CLIENT:LOW: intf list: Interface not found
```
debug ip nbar config

To enable debugging of all commands configured for the activation and deactivation of Network-Based Application Recognition (NBAR) on a control plane, use the `debug ip nbar config` command in privileged EXEC mode. To disable debugging, use the `no` form of this command.

```
debug ip nbar config {high | low | medium}
no debug ip nbar config
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>high</td>
<td>Enables high-level debugging.</td>
</tr>
<tr>
<td>low</td>
<td>Enables low-, medium-, and high-level debugging.</td>
</tr>
<tr>
<td>medium</td>
<td>Enables medium- and low-level debugging.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(4)M</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip nbar config` command:

```
Device# debug ip nbar config high

*May 14 08:36:59.059: STILE:CONF:HIGH: Attempt to add branch to node that does not have branches
*May 14 08:36:59.060: STILE:CONF:HIGH: Attempt to add branch to node that does not have branches
*May 14 08:37:04.314: STILE:CONF:HIGH: Fast flag request for MQC is 1
*May 14 08:37:04.314: STILE:CONF:HIGH: Fast flag request for MQC is 1
*May 14 08:37:04.314: STILE:CONF:HIGH: MQC or P.D set fast flag
```
debug ip nbar platform

To enable debugging of application programming interfaces (APIs) pertaining to Network-Based Application Recognition (NBAR) on a control plane, use the **debug ip nbar platform** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

**debug ip nbar platform** {**high** | **low** | **medium**}

**no debug ip nbar platform**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>high</th>
<th>Enables high-level debugging.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>low</td>
<td>Enables low-, medium-, and high-level debugging.</td>
</tr>
<tr>
<td></td>
<td>medium</td>
<td>Enables medium- and low-level debugging.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.7S Release</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the **debug ip nbar platform** command:

```
Device# debug ip nbar platform low

```
debug ip ospf adj

To display information on adjacency events related to Open Shortest Path First (OSPF), such as packets being dropped due to a Time-to-Live (TTL) security check, use the `debug ip ospf adj` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
depbug ip ospf adj
no debug ip ospf adj
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip ospf adj` command:

```
Router# debug ip ospf adj
Jan 31 00:13:05.175: OSPF: Drop packet on Serial2/0 from 10.1.1.1 with TTL: 1
Mar 27 23:15:03.175: OSPF Drop packet on OSPF_VL0 from 10.1.1.100 with TTL: 253
```

Information in the output includes the day and time the packet was dropped, protocol name, interface on which the packet was dropped, neighbor address, and TTL hop count.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ip ospf events</code></td>
<td>Displays information on OSPF-related events, such as adjacencies, flooding information, designated router selection, and SPF calculation.</td>
</tr>
</tbody>
</table>
**debug ip ospf database-timer rate-limit**

To display when link-state advertisement (LSA) rate-limiting timers will expire, use the `debug ip ospf database-timer rate-limit` command in privileged EXEC mode.

`debug ip ospf database-timer rate-limit [access-list-number]`

**Syntax Description**

| access-list-number | (Optional) Number of the standard or expanded IP access list to apply to the debug output. Standard IP access lists are in the range 1 to 99. Expanded IP access lists are in the range 1300 to 1999. |

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(25)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXD.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command if you need to see when the timers will expire per LSA. Use an access list if you want to limit the output.

**Examples**

The following is sample output from the `debug ip ospf database-timer rate-limit` command for an example configuration that includes the `timers throttle lsa all 100 10000 45000` command. Comments are inserted to explain the preceding output.

```
Router# debug ip ospf database-timer rate-limit
OSPF rate limit timer events debugging is on
*Mar 12 20:18:20.383:OSPF:Starting rate limit timer for 10.10.24.4 10.10.24.4 1 with 100ms delay

The interface is shut down, which causes OSPF to generate a new router LSA. The system starts a timer for 100 milliseconds.

*Mar 12 20:18:20.495:OSPF:Rate limit timer is expired for 10.10.24.4 10.10.24.4 1

The rate limit timer is expired after 100 milliseconds (a small delta is added to the timer).

*Mar 12 20:18:20.495:OSPF:Build router LSA for area 24, router ID 10.10.24.4, seq 0x80000003

The system will generate update a router LSA after the timer expires.
```
**debug ip ospf events**

To display information on Open Shortest Path First (OSPF)-related events, such as adjacencies, flooding information, designated router selection, and shortest path first (SPF) calculation, use the `debug ip ospf events` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip ospf events
no debug ip ospf events
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Examples**

The following is sample output from the `debug ip ospf events` command:

```
Router# debug ip ospf events
OSPF:hello with invalid timers on interface Ethernet0
hello interval received 10 configured 10
net mask received 255.255.255.0 configured 255.255.255.0
dead interval received 40 configured 30
```

The `debug ip ospf events` output shown might appear if any of the following situations occurs:

- The IP subnet masks for routers on the same network do not match.
- The OSPF hello interval for the router does not match that configured for a neighbor.
- The OSPF dead interval for the router does not match that configured for a neighbor.

If a router configured for OSPF routing is not seeing an OSPF neighbor on an attached network, perform the following tasks:

- Make sure that both routers have been configured with the same IP mask, OSPF hello interval, and OSPF dead interval.
- Make sure that both neighbors are part of the same area type.

In the following example line, the neighbor and this router are not part of a stub area (that is, one is a part of a transit area and the other is a part of a stub area, as explained in RFC 1247):

```
OSPF: hello packet with mismatched E bit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ip pgm host</code></td>
<td>Displays information about each OSPF packet received.</td>
</tr>
</tbody>
</table>
debug ip ospf lsa-maxage

To display debug messages about OSPF LSA MaxAge events, use the **debug ip ospf lsa-maxage** command in privileged EXEC mode. To disable the display of debug messages, use the **no** form of this command.

**debug ip ospf lsa-maxage**  [access-list-number]

**no debug ip ospf lsa-maxage**  [access-list-number]

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list-number</td>
<td>(Optional) Number of the standard or expanded IP access list to apply to the debug output.</td>
</tr>
<tr>
<td></td>
<td>Standard IP access lists are in the range 1 to 199.</td>
</tr>
<tr>
<td></td>
<td>Expanded IP access lists are in the range 1300 to 2699.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>By default, debug messages about OSPF LSA MaxAge events are not displayed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>Cisco IOS XE</td>
<td>Command introduced.</td>
</tr>
<tr>
<td>17.1.1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Debug messages are displayed for every LSA for which a MaxAge event occurs. To limit the output, use an access list.</td>
</tr>
</tbody>
</table>

**Example**

```
router#debug ip ospf lsa-maxage
OSPF LSA maxage debugging is on
```
**debug ip ospf mpls traffic-eng advertisements**

To print information about traffic engineering advertisements in Open Shortest Path First (OSPF) link state advertisement (LSA) messages, use the `debug ip ospf mpls traffic-eng advertisements` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
depg ip ospf mpls traffic-eng advertisements
no debug ip ospf mpls traffic-eng advertisements
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)ST</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(3)T</td>
<td>This command was integrated into Cisco IOS Release 12.1(3)T.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(22)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, information about traffic engineering advertisements is printed in OSPF LSA messages:

```
Router# debug ip ospf mpls traffic-eng advertisements
OSPF: IGP delete router node 10.106.0.6 fragment 0 with 0 links
TE Router ID 10.106.0.6
OSPF: IGP update router node 10.110.0.10 fragment 0 with 0 links
TE Router ID 10.110.0.10
OSPF: MPLS announce router node 10.106.0.6 fragment 0 with 1 links
   Link connected to Point-to-Point network
   Link ID :10.110.0.10
   Interface Address :10.1.0.6
   Neighbor Address :10.1.0.10
   Admin Metric :10
   Maximum bandwidth :1250000
   Maximum reservable bandwidth :625000
   Number of Priority :8
   Priority 0 :625000 Priority 1 :625000
   Priority 2 :625000 Priority 3 :625000
   Priority 4 :625000 Priority 5 :625000
   Priority 6 :625000 Priority 7 :625000
   Affinity Bit :0x0
```

The table below describes the significant fields shown in the display.
### Table 42: debug ip ospf mpls traffic-eng advertisements Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link ID</td>
<td>Index of the link being described.</td>
</tr>
<tr>
<td>Interface Address</td>
<td>Address of the interface.</td>
</tr>
<tr>
<td>Neighbor Address</td>
<td>Address of the neighbor.</td>
</tr>
<tr>
<td>Admin Metric</td>
<td>Administrative weight associated with this link.</td>
</tr>
<tr>
<td>Maximum bandwidth</td>
<td>Bandwidth capacity of the link (kbps).</td>
</tr>
<tr>
<td>Maximum reservable bandwidth</td>
<td>Amount of reservable bandwidth on this link.</td>
</tr>
<tr>
<td>Number of Priority</td>
<td>Number of priority levels for which bandwidth is advertised.</td>
</tr>
<tr>
<td>Priority</td>
<td>Bandwidth available at indicated priority level.</td>
</tr>
<tr>
<td>Affinity Bit</td>
<td>Attribute flags of the link that are being flooded.</td>
</tr>
</tbody>
</table>
debug ip ospf nsf

To display debugging messages about Open Shortest Path First (OSPF) during a Cisco nonstop forwarding (NSF) restart, use the **debug ip ospf nsf** command in privileged EXEC mode. To disable the display of debugging output, use the no form of this command.

```
debug ip ospf nsf [detail]
o debug ip ospf nsf [detail]
```

**Syntax Description**

- `detail` (Optional) Displays detailed debug messages.

**Command Modes**

Privileged EXEC

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(22)S</td>
<td>This command was introduced.</td>
<td></td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
<td></td>
</tr>
<tr>
<td>12.2(20)S</td>
<td>Support for the Cisco 7304 router was added.</td>
<td></td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
<td></td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
<td></td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **debug ip ospf nsf** command to diagnose problems with OSPF link-state database (LSDB) resynchronization and NSF operations.

**Examples**

The following example shows that OSPF NSF events debugging is enabled:

```
Router# debug ip ospf nsf
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nsf (OSPF)</td>
<td>Configures NSF operations for OSPF.</td>
</tr>
<tr>
<td>show ip ospf</td>
<td>Displays general information about OSPF routing processes.</td>
</tr>
<tr>
<td>show ip ospf neighbor</td>
<td>Displays OSPF-neighbor information on a per-interface basis.</td>
</tr>
</tbody>
</table>
debug ip ospf packet

To display information about each Open Shortest Path First (OSPF) packet received, use the `debug ip ospf packet` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip ospf packet
no debug ip ospf packet
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Examples**

The following is sample output from the `debug ip ospf packet` command:

```
Router# debug ip ospf packet
OSPF: rcv. v:2 t:1 l:48 rid:200.0.0.117
    aid:0.0.0.0 chk:6AB2 aut:0 auk:
```

The debug ip ospf packet command produces one set of information for each packet received. The output varies slightly depending on which authentication is used. The following is sample output from the `debug ip ospf packet` command when message digest algorithm 5 (MD5) authentication is used.

```
Router# debug ip ospf packet
OSPF: rcv. v:2 t:1 l:48 rid:200.0.0.116
    aid:0.0.0.0 chk:0 aut:2 keyid:1 seq:0x0
```

The table below describes the significant fields shown in the display.

**Table 43: debug ip ospf packet Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>v:</td>
<td>OSPF version.</td>
</tr>
<tr>
<td>t:</td>
<td>OSPF packet type. Possible packet types follow:</td>
</tr>
<tr>
<td></td>
<td>• 1--Hello</td>
</tr>
<tr>
<td></td>
<td>• 2--Data description</td>
</tr>
<tr>
<td></td>
<td>• 3--Link state request</td>
</tr>
<tr>
<td></td>
<td>• 4--Link state update</td>
</tr>
<tr>
<td></td>
<td>• 5--Link state acknowledgment</td>
</tr>
<tr>
<td>l:</td>
<td>OSPF packet length in bytes.</td>
</tr>
<tr>
<td>rid:</td>
<td>OSPF router ID.</td>
</tr>
<tr>
<td>aid:</td>
<td>OSPF area ID.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
chk: | OSPF checksum.
aut: | OSPF authentication type. Possible authentication types follow:
| • 0--No authentication
| • 1--Simple password
| • 2--MD5
keyid: | MD5 key ID.
seq: | Sequence number.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip http client</td>
<td>Displays information on OSPF-related events, such as adjacencies, flooding information, designated router selection, and SPF calculation.</td>
</tr>
</tbody>
</table>
debug ip ospf rib

To display debugging information for Open Shortest Path First (OSPF) Version 2 routes in the global or local Routing Information Base (RIB), use the `debug ip ospf rib` command in privileged EXEC mode. To disable the debugging of OSPF Version 2 routes, use the `no` form of this command.

```
debug ip ospf rib [{local | {redistribution | global [access-list-number]}]}] [detail]
no debug ip ospf rib [{local | {{redistribution | global [access-list-number]}]}] [detail]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>(Optional) Displays debugging information for OSPF Version 2 routes in the local RIB.</td>
</tr>
<tr>
<td>redistribution</td>
<td>(Optional) Displays debugging information about redistributed OSPF Version 2 routes.</td>
</tr>
<tr>
<td>global</td>
<td>(Optional) Displays debugging information for OSPF Version 2 routes in the global RIB.</td>
</tr>
<tr>
<td>access-list-number</td>
<td>(Optional) Number of an access list. This is a decimal number from 1 to 199 or from 1300 to 2699.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays more detailed debug information.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into the Cisco IOS 12.2(33)SB release.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can use the output from the `debug ip ospf rib` command to learn about the function of the local RIB and the interaction between the route redistribution process and the global RIB. For example, you can learn why the routes that OSPF placed in the global RIB are not the same ones that you anticipated.

A Cisco Technical Assistance Center representative may ask you to turn on debugging using the `debug ip ospf rib` command as part of troubleshooting a problem.

To monitor updates from the OSPF database to the OSPF local RIB, use the `local` keyword, and to monitor updates from the OSPF database to the OSPF global RIB, use the `global` keyword.

It is highly recommended that you limit the debugging output to information specific to the IP prefix that is associated with a specific access list by entering the `access-list-number` argument.
Examples

The following is sample output from the `debug ip ospf rib` command with the `access-list-number` argument used in order to limit the debugging output to information specific to the IP prefix that is associated with the specific access list 1:

```plaintext
Router# show running-config | include access-list 1
access-list 112 permit 10.1.1.0 0.0.0.255
! access-list 1 is configured
Router# debug ip ospf rib local detail 1
route 192.168.130.2/255.255.255.0, area 1, dist 10, for interface
Ethernet0/0.1
Router clear
route 192.168.130.2/255.255.255.0, area 1, dist 10, for interface
Ethernet0/0.1
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ip ospf events</code></td>
<td>Displays information on OSPF-related events, such as adjacencies, flooding information, designated router selection, and SPF calculation.</td>
</tr>
</tbody>
</table>
debug ip ospf spf statistic

To display statistical information while running the shortest path first (SPF) algorithm, use the `debug ip ospf spf statistic` command in privileged EXEC mode. To disable the debugging output, use the `no` form of this command.

```
drop ip ospf spf statistic
no debug ip ospf spf statistic
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(12)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ip ospf spf statistic` command displays the SPF calculation times in milliseconds, the node count, and a time stamp.

**Examples**

The following is sample output from the `debug ip ospf spf statistic` command:

```
Router# debug ip ospf spf statistic
00:05:59: OSPF: Begin SPF at 359.216ms, process time 60ms
00:05:59: spf_time 00:05:59.216, wait_interval 0s
00:05:59: OSPF: End SPF at 359.216ms, Total elapsed time 0ms
00:05:59: Intra: 0ms, Inter: 0ms, External: 0ms
00:05:59: R: 4, N: 2, Stubs: 1
00:05:59: SN: 1, SA: 0, X5: 1, X7: 0
00:05:59: SPF suspends: 0 intra, 1 total
```

The table below describes the significant fields shown in the display.

**Table 44: debug ip ospf spf statistic Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Begin SPF at</td>
<td>Absolute time in milliseconds when SPF is started.</td>
</tr>
<tr>
<td>process time</td>
<td>Cumulative time since the process has been created.</td>
</tr>
<tr>
<td>spf_time</td>
<td>Last time SPF was run or an event has happened to run SPF.</td>
</tr>
<tr>
<td>wait_interval</td>
<td>Time waited to run SPF.</td>
</tr>
<tr>
<td>End SPF at</td>
<td>Absolute time in milliseconds when SPF had ended.</td>
</tr>
<tr>
<td>Total elapsed time</td>
<td>Total time take to run SPF.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Intra:</td>
<td>Time taken to process intra-area link-state advertisements (LSAs).</td>
</tr>
<tr>
<td>Inter:</td>
<td>Time taken to process interarea LSAs.</td>
</tr>
<tr>
<td>External:</td>
<td>Time taken to process external LSAs.</td>
</tr>
<tr>
<td>R:</td>
<td>Number of router LSAs.</td>
</tr>
<tr>
<td>N:</td>
<td>Number of network LSAs.</td>
</tr>
<tr>
<td>Stubs:</td>
<td>Number of stub links.</td>
</tr>
<tr>
<td>SN:</td>
<td>Number of summary network LSAs.</td>
</tr>
<tr>
<td>SA:</td>
<td>Number of summary LSAs describing autonomous system boundary routers (ASBRs).</td>
</tr>
<tr>
<td>X5:</td>
<td>Number of external type 5 LSAs.</td>
</tr>
<tr>
<td>X7:</td>
<td>Number of external type 7 LSAs.</td>
</tr>
<tr>
<td>SPF suspend: intra</td>
<td>Number of times process is suspended during intra-area SPF run.</td>
</tr>
<tr>
<td>total</td>
<td>Total number of times process is suspended during SPF run.</td>
</tr>
</tbody>
</table>
debug ip packet

To display general IP debugging information and IP security option (IPSO) security transactions, use the debug ip packet command in privileged EXEC mode. To disable debugging output, use the no form of this command.

```
debug ip packet [access-list-number] [detail] [dump]
no debug ip packet [access-list-number]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>access-list-number</strong></td>
<td>(Optional) The IP access list number that you can specify. If the datagram is not permitted by that access list, the related debugging output is suppressed. Standard, extended, and expanded access lists are supported. The range of standard and extended access lists is from 1 to 199. The range of expanded access lists is from 1300 to 2699.</td>
</tr>
<tr>
<td><strong>detail</strong></td>
<td>(Optional) Displays detailed IP packet debugging information. This information includes the packet types and codes as well as source and destination port numbers.</td>
</tr>
<tr>
<td><strong>dump</strong></td>
<td>(Hidden) Displays IP packet debugging information along with raw packet data in hexadecimal and ASCII forms. This keyword can be enabled with individual access lists and also with the detail keyword.</td>
</tr>
</tbody>
</table>

**Note** The dump keyword is not fully supported and should be used only in collaboration with Cisco Technical Support. See the caution notes below, in the usage guidelines, for more specific information.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

If a communication session is closing when it should not be, an end-to-end connection problem can be the cause. The debug ip packet command is useful for analyzing the messages traveling between the local and remote hosts. IP packet debugging captures the packets that are process switched including received, generated and forwarded packets. IP packets that are switched in the fast path are not captured.

IPSO security transactions include messages that describe the cause of failure each time a datagram fails a security test in the system. This information is also sent to the sending host when the router configuration allows it.

**Caution**

Because the debug ip packet command generates a substantial amount of output and uses a substantial amount of system resources, this command should be used with caution in production networks. It should only be enabled when traffic on the IP network is low, so other activity on the system is not adversely affected. Enabling the detail and dump keywords use the highest level of system resources of the available configuration options for this command, so a high level of caution should be applied when enabling either of these keywords.
The `dump` keyword is not fully supported and should be used only in collaboration with Cisco Technical Support. Because of the risk of using significant CPU utilization, the `dump` keyword is hidden from the user and cannot be seen using the “?” prompt. The length of the displayed packet information may exceed the actual packet length and include additional padding bytes that do not belong to the IP packet. Also note that the beginning of a packet may start at different locations in the dump output depending on the specific router, interface type, and packet header processing that may have occurred before the output is displayed.

**Caution**

The following is sample output from the `debug ip packet` command:

```plaintext
Router# debug ip packet
IP packet debugging is on
IP: s=172.69.13.44 (Fddi0), d=10.125.254.1 (Serial2), g=172.69.16.2, forward
IP: s=172.69.1.57 (Ethernet4), d=10.36.125.2 (Serial2), g=172.69.16.2, forward
IP: s=172.69.1.55 (Ethernet4), d=172.69.2.42 (Fddi0), g=172.69.13.6, forward
IP: s=172.69.89.33 (Ethernet2), d=10.130.2.156 (Serial2), g=172.69.16.2, forward
IP: s=172.69.1.27 (Ethernet4), d=255.255.255.255, rcvd 2
IP: s=172.69.1.27 (Ethernet4), d=172.69.43.126 (Fddi0), g=172.69.13.6, forward
IP: s=172.69.20.32 (Ethernet2), d=255.255.255.255, rcvd 2
IP: s=172.69.1.57 (Ethernet4), d=10.36.125.2 (Serial2), g=172.69.16.2, access denied
```

The output shows two types of messages that the `debug ip packet` command can produce; the first line of output describes an IP packet that the router forwards, and the third line of output describes a packet that is destined for the router. In the third line of output, `rcvd 2` indicates that the router decided to receive the packet.

The table below describes the significant fields shown in the display.

**Table 45: debug ip packet Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP:</td>
<td>Indicates that this is an IP packet.</td>
</tr>
<tr>
<td>s=172.69.13.44 (Fddi0)</td>
<td>Indicates the source address of the packet and the name of the interface that received the packet.</td>
</tr>
<tr>
<td>d=10.125.254.1 (Serial2)</td>
<td>Indicates the destination address of the packet and the name of the interface (in this case, S2) through which the packet is being sent out on the network.</td>
</tr>
<tr>
<td>g=172.69.16.2</td>
<td>Indicates the address of the next-hop gateway.</td>
</tr>
<tr>
<td>forward</td>
<td>Indicates that the router is forwarding the packet. If a filter denies a packet, “access denied” replaces “forward,” as shown in the last line of output.</td>
</tr>
</tbody>
</table>

The following is sample output from the `debug ip packet` command enabled with the `detail` keyword:

```plaintext
Router# debug ip packet detail
IP packet debugging is on (detailed)
001556: 19:59:30: CEF: Try to CEF switch 10.4.9.151 from FastEthernet0/0
001557: 19:59:30: IP: s=10.4.9.6 (FastEthernet0/0), d=10.4.9.151 (FastEthernet03) 001558: 19:59:30: TCP src=179, dst=11001, seq=3736598846, ack=2885081910, WH
```
001559: 20:00:09: CEF: Try to CEF switch 10.4.9.151 from FastEthernet0/0
001560: 20:00:09: IP: s=10.4.9.4 (FastEthernet0/0), d=10.4.9.151 (FastEthernet03
001561: 20:00:09:  TCP src=179, dst=11000, seq=163035693, ack=2948141027, wi
001562: 20:00:14: CEF: Try to CEF switch 10.4.9.151 from FastEthernet0/0
001563: 20:00:14: IP: s=10.4.9.6 (FastEthernet0/0), d=10.4.9.151 (FastEthernet03
001564: 20:00:14:  ICMP type=8, code=0
001565: 20:00:14: IP: s=10.4.9.151 (local), d=10.4.9.6 (FastEthernet0/0), len 1g
001566: 20:00:14:  ICMP type=0, code=0

The format of the output with detail keyword provides additional information, such as the packet type, code, some field values, and source and destination port numbers.

The table below describes the significant fields shown in the display.

Table 46: debug ip packet detail Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEF:</td>
<td>Indicates that the IP packet is being processed by CEF.</td>
</tr>
<tr>
<td>IP:</td>
<td>Indicates that this is an IP packet.</td>
</tr>
<tr>
<td>s=10.4.9.6 (FastEthernet0/0)</td>
<td>Indicates the source address of the packet and the name of the interface that received the packet.</td>
</tr>
<tr>
<td>d=10.4.9.151 (FastEthernet03)</td>
<td>Indicates the destination address of the packet and the name of the interface through which the packet is being sent out on the network.</td>
</tr>
<tr>
<td>TCP src=</td>
<td>Indicates the source TCP port number.</td>
</tr>
<tr>
<td>dst=</td>
<td>Indicates the destination TCP port number.</td>
</tr>
<tr>
<td>seq=</td>
<td>Value from the TCP packet sequence number field.</td>
</tr>
<tr>
<td>ack=</td>
<td>Value from the TCP packet acknowledgement field.</td>
</tr>
<tr>
<td>ICMP type=</td>
<td>Indicates ICMP packet type.</td>
</tr>
<tr>
<td>code=</td>
<td>Indicates ICMP return code.</td>
</tr>
</tbody>
</table>

The following is sample output from the debug ip packet command enabled with the dump keyword:

Router# debug ip packet dump
IP packet debugging is on (detailed) (dump)
21:02:42: IP: s=10.4.9.6 (FastEthernet0/0), d=10.4.9.4 (FastEthernet0/0), len 13
07003A00: 0005 00509C08 ...F..
07003A10: 007855B 4DC00800 45000064 001E0000 ...[M...E...d....
07003A20: FE019669 AA040906 AA040904 0800CF7C ~........O|
07003A30: OD052678 00000000 AOB7145 ABCDABCD ..&x........qE+M+M
07003A40: ABCDABCD ABCDABCD ABCDABCD ABCDABCD +M+M+M+M+M+M+M+M
07003A50: ABCDABCD ABCDABCD ABCDABCD ABCDABCD +M+M+M+M+M+M+M+M
07003A60: ABCDABCD ABCDABCD ABCDABCD ABCDABCD +M+M+M+M+M+M+M+M
07003A70: ABCDABCD ABCDABCD ABCDABCD ABCDABCD +M+M+M+M+M+M+M+M
21:02:42: IP: s=10.4.9.4 (Local), d=10.4.9.6 (FastEthernet0/0), len 100, sending
07003A00: 0005 00509C08 ...F..
07003A10: 007855B 4DC00800 45000064 001E0000 ...[M...E...d....
07003A20: FE019569 AA040906 AA040904 0800D77C ~........O|
07003A30: OD052678 00000000 AOB7145 ABCDABCD ..&x........qE+M+M
07003A40: ABCDABCD ABCDABCD ABCDABCD ABCDABCD +M+M+M+M+M+M+M+M

Cisco IOS Debug Command Reference - Commands I through L
The **dump** keyword is not fully supported and should be used only in collaboration with Cisco Technical Support. See the caution in the usage guidelines section of this command reference page for more specific information.

The output from the **debug ip packet** command, when the **dump** keyword is enabled, provides raw packet data in hexadecimal and ASCII forms. This additional output is displayed in addition to the standard output. The **dump** keyword can be used with all of the available configuration options of this command.

The table below describes the significant fields shown in the display.

**Table 47: debug ip packet dump Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP:</td>
<td>Indicates that this is an IP packet.</td>
</tr>
<tr>
<td>s=10.4.9.6 (FastEthernet0/0)</td>
<td>Indicates the source address of the packet and the name of the interface that received the packet.</td>
</tr>
<tr>
<td>d=10.4.9.4 (FastEthernet0/0) len 13</td>
<td>Indicates destination address and length of the packet and the name of the interface through which the packet is being sent out on the network.</td>
</tr>
<tr>
<td>sending</td>
<td>Indicates that the router is sending the packet.</td>
</tr>
</tbody>
</table>

The calculation on whether to send a security error message can be somewhat confusing. It depends upon both the security label in the datagram and the label of the incoming interface. First, the label contained in the datagram is examined for anything obviously wrong. If nothing is wrong, assume the datagram to be correct. If something is wrong, the datagram is treated as **unclassified genser**. Then the label is compared with the interface range, and the appropriate action is taken, as the table below describes.
Table 48: Security Actions

<table>
<thead>
<tr>
<th>Classification</th>
<th>Authorities</th>
<th>Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>Too low</td>
<td>Too low</td>
<td>No Response</td>
</tr>
<tr>
<td></td>
<td>Good</td>
<td>No Response</td>
</tr>
<tr>
<td></td>
<td>Too high</td>
<td>No Response</td>
</tr>
<tr>
<td>In range</td>
<td>Too low</td>
<td>No Response</td>
</tr>
<tr>
<td></td>
<td>Good</td>
<td>Accept</td>
</tr>
<tr>
<td></td>
<td>Too high</td>
<td>Send Error</td>
</tr>
<tr>
<td>Too high</td>
<td>Too low</td>
<td>No Response</td>
</tr>
<tr>
<td></td>
<td>In range</td>
<td>Send Error</td>
</tr>
<tr>
<td></td>
<td>Too high</td>
<td>Send Error</td>
</tr>
</tbody>
</table>

The security code can only generate a few types of Internet Control Message Protocol (ICMP) error messages. The only possible error messages and their meanings follow:

- ICMP Parameter problem, code 0--Error at pointer
- ICMP Parameter problem, code 1--Missing option
- ICMP Parameter problem, code 2--See Note that follows
- ICMP Unreachable, code 10--Administratively prohibited

Note

The message “ICMP Parameter problem, code 2” identifies a specific error that occurs in the processing of a datagram. This message indicates that the router received a datagram containing a maximum length IP header but no security option. After being processed and routed to another interface, it is discovered that the outgoing interface is marked with “add a security label.” Because the IP header is already full, the system cannot add a label and must drop the datagram and return an error message.

When an IP packet is rejected due to an IP security failure, an audit message is sent via Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) Network Address Translation (NAT). Also, any `debug ip packet` output is appended to include a description of the reason for rejection. This description can be any of the following:

- No basic
- No basic, no response
- Reserved class
- Reserved class, no response
- Class too low, no response
- Class too high
- Class too high, bad authorities, no response
- Unrecognized class
- Unrecognized class, no response
- Multiple basic
- Multiple basic, no response
- Authority too low, no response
- Authority too high
- Compartment bits not dominated by maximum sensitivity level
- Compartment bits do not dominate minimum sensitivity level
- Security failure: extended security disallowed
- NLESO source appeared twice
- ESO source not found
- Postroute, failed xfc out
- No room to add IPSO
debug ip pgm host

Support for the PGM Host feature has been removed. Use of this command is not recommended.

To display debug messages for the Pragmatic General Multicast (PGM) Host feature, use the `debug ip pgm host` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

`debug ip pgm host [{data | nak | spm}]`
`no debug ip pgm host [{data | nak | spm}]`

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>data</code></td>
<td>(Optional) Enables debugging for PGM sent (ODATA) and re-sent (RDATA) data packets.</td>
</tr>
<tr>
<td><code>nak</code></td>
<td>(Optional) Enables debugging for PGM negative acknowledgment (NAK) data packets, NAK confirmation (NCF) data packets, andNull NAK (NNAK) data packets.</td>
</tr>
<tr>
<td><code>spm</code></td>
<td>(Optional) Enables debugging for PGM source path messages (SPMs).</td>
</tr>
</tbody>
</table>

### Command Default

Debugging for PGM Host is not enabled. If the `debug ip pgm host` command is used with no additional keywords, debugging is enabled for all PGM Host message types.

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `debug ip pgm host` command:

Router# `debug ip pgm host`

Host SPM debugging is on
Host NAK/NCF debugging is on
Host ODATA/RDATA debugging is on

The following is sample output from the `debug ip pgm host` command when the `data` keyword is used:

Router# `debug ip pgm host data`

02:50:23: PGM Host:Received ODATA from 10.0.30.2 to 224.3.3.3 (74 bytes)
02:50:23: ODATA TSI 00000A001E02-0401 data-dport BBBB csum 9317 tlen 74
tsqn  31 dsqn  39
The following example shows output of the `debug ip pgm host` command when the `nak` keyword is used. In the following example, the host sends a NAK to the source for a missing packet and the source returns an NCF to the host followed by an RDAT data packet.

Router# debug ip pgm host nak

02:50:24: PGM Host: Sending NAK from 10.0.32.2 to 10.0.32.1 (36 bytes)
02:50:24:  NAK TSI 00000A001E02-0401 data-dport BBBB csum 04EC tlen 36
02:50:24:  dsqn 38 data source 10.0.30.2 group 224.3.3.3
02:50:24: PGM Host: Received NCF from 10.0.30.2 to 224.3.3.3 (36 bytes)
02:50:24:  NCF TSI 00000A001E02-0401 data-dport BBBB csum 02EC tlen 36
02:50:24:  dsqn 38 data source 10.0.30.2 group 224.3.3.3
02:50:24: PGM Host: Received RDAT from 10.0.30.2 to 224.3.3.3 (74 bytes)
02:50:24:  RDAT TSI 00000A001E02-0401 data-dport BBBB csum 9218 tlen 74
02:50:24:  tsqn 31 dsqn 38

The following is sample output from the `debug ip pgm host` command with the `spm` keyword is used:

Router# debug ip pgm host spm

02:49:39: PGM Host: Received SPM from 10.0.30.2 to 224.3.3.3 (36 bytes)
02:49:39:  SPM TSI 00000A001E02-0401 data-dport BBBB csum EA08 tlen 36
02:49:39:  dsqn 980 tsqn 31 lsqn 31 NLA 10.0.32.1

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip pgm host</td>
<td>Resets PGM Host connections to their default values and clears traffic statistics.</td>
</tr>
<tr>
<td>ip pgm host</td>
<td>Enables the PGM Host feature.</td>
</tr>
<tr>
<td>show ip pgm host defaults</td>
<td>Displays the default values for PGM Host traffic.</td>
</tr>
<tr>
<td>show ip pgm host sessions</td>
<td>Displays open PGM Host traffic sessions.</td>
</tr>
<tr>
<td>show ip pgm host traffic</td>
<td>Displays PGM Host traffic statistics.</td>
</tr>
</tbody>
</table>
**debug ip pgm router**

To display debug messages for Pragmatic General Multicast (PGM), use the `debug ip pgm router` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip pgm router [{spm | nak | data}]
no debug ip pgm router [{spm | nak | data}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spm</td>
<td>(Optional) Enables debugging for Source Path Messages (SPMs).</td>
</tr>
<tr>
<td>nak</td>
<td>(Optional) Enables debugging for negative acknowledgments (NAKs), NAK confirmations (NCFs), and Null NAKs (NNAKs).</td>
</tr>
<tr>
<td>data</td>
<td>(Optional) Enables debugging for Retransmissions (RDATA).</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging for PGM is not enabled. If the `debug ip pgm router` command is used with no additional keywords, debugging is enabled for all PGM message types.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following shows sample output from the `debug ip pgm router` command:

```
Router# debug ip pgm router
SPM debugging is on
NAK/NNAK/NCF debugging is on
RDATA debugging is on
```

The following shows sample output from the `debug ip pgm router` command when the `spm` keyword is used:

```
Router# debug ip pgm router spm
PGM: Received SPM on Ethernet1/0/5 from 10.7.0.200 to 227.7.7.7 (52 bytes)
  SPM TSI 0A0700C85555-1000 data-dport 1001 csum CCCC tlen 52
  dsqn 3758096779 tsqn 1954 isqn 1979 lsqn 1990
  NLA 10.7.0.200
  SPM from source/RPF-neighbour 10.7.0.200 for 10.7.0.200 (SPT)
  Forwarded SPM from 10.7.0.200 to 227.7.7.7
```

The following is a debugging message for a selective SPM:

```
Router# debug ip pgm router spm
PGM: Received SPM on Ethernet1/0/5 from 10.7.0.200 to 234.4.3.2 (52 bytes)
  SPM TSI 0A0700C85555-2000 data-dport 2001 csum CCCC tlen 52
  Options P N O
dsqn 3758096768 tsqn 1986 isqn 1994 lsqn 2006
```
The “P N O” flags indicate which options are present in this packet:

- \( P \) indicates that this is a parity packet.
- \( N \) indicates that options are network significant.
- \( O \) indicates that options are present.

The following shows sample output from the `debug ip pgm router` command when the `nak` keyword is used:

```
Router# debug ip pgm router nak
PGM: Received NAK on Ethernet1/0/0 from 10.1.0.4 to 10.1.0.2 (36 bytes)
   NAK TSI OA0700C85555-1000 data-dport 1001 csum CCCC tlen 36
dsqn  1990 data source 10.7.0.200 group 227.7.7.7
   NAK unicast routed to RPF neighbour 10.4.0.1
   Forwarding NAK from 10.1.0.4 to 10.4.0.1 for 10.7.0.200
PGM: Received NCF on Ethernet1/0/5 from 10.7.0.200 to 227.7.7.7 (36 bytes)
   NCF TSI OA0700C85555-1000 data-dport 1001 csum CACC tlen 36
dsqn  1990 data source 10.7.0.200 group 227.7.7.7
   NAK retrans canceled for TSI OA0700C85555-1000 dsqn 1990
   NAK elimination started for TSI OA0700C85555-1000 dsqn 1990
PGM: Received NCF on Ethernet1/0/5 from 10.7.0.200 to 227.7.7.7 (36 bytes)
   NCF TSI OA0700C85555-1000 data-dport 1001 csum CACC tlen 36
dsqn  1991 data source 10.7.0.200 group 227.7.7.7
   No NAK retrans outstanding for TSI OA0700C85555-1000 dsqn 1991
   NAK anticipated for TSI OA0700C85555-1000 dsqn 1991
```

The following example shows output of the `debug ip pgm router` command with the `data` keyword. The debugging message is for an RDATA packet for which the router has only anticipated state, sqn 1991. Because it did not actually get a NAK, this RDATA is not forwarded by the PGM router.

```
Router# debug ip pgm router data
PGM: Received RDATA on Ethernet1/0/5 from 10.7.0.200 to 227.7.7.7 (70 bytes)
   RDATA TSI OA0700C85555-1000 data-dport 1001 csum CCCC tlen 32
tsqn  1954 dsqn  1990
   Marking Ethernet1/0/0 for forwarding
   Marking Serial5/0 for skipping
   Forwarded RDATA from 10.7.0.200 to 227.7.7.7
Debug message for RDATA packet corresponding to a NAK for sqn 1990. Since the NAK was received on Ethernet1/0/0, RDATA is forwarded out only that interface and another interface in the multicast olist Serial5/0 is skipped.
PGM: Received RDATA on Ethernet1/0/5 from 10.7.0.200 to 227.7.7.7 (70 bytes)
   RDATA TSI OA0700C85555-1000 data-dport 1001 csum CCCC tlen 32
tsqn  1954 dsqn  1991
   Eliminated RDATA (null oif) from 10.7.0.200 to 227.7.7.7
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip pgm router</code></td>
<td>Enables the PGM Router Assist feature for the interface.</td>
</tr>
<tr>
<td><code>show ip pgm router</code></td>
<td>Displays PGM traffic statistics and TSI state.</td>
</tr>
</tbody>
</table>
debug ip pim

To display Protocol Independent Multicast (PIM) packets received and sent, and to display PIM-related events, use the `debug ip pim` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip pim [vrf vrf-name] [{group-address | atm | auto-rp | bsr | df [rp-address] | hello | tag}]
no debug ip pim [vrf vrf-name] [{group-address | atm | auto-rp | bsr | df [rp-address] | hello | tag}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vrf vrf-name</strong></td>
<td>(Optional) Displays PIM-related events associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the <code>vrf-name</code> argument.</td>
</tr>
<tr>
<td><strong>group-address</strong></td>
<td>(Optional) IP address or Domain Name System (DNS) name of a multicast group. Entering a multicast group address restricts the output to display only PIM-related events associated with the multicast group address specified for the optional <code>group-address</code> argument.</td>
</tr>
<tr>
<td><strong>atm</strong></td>
<td>(Optional) Displays PIM ATM signaling activity.</td>
</tr>
<tr>
<td><strong>auto-rp</strong></td>
<td>(Optional) Displays the contents of each PIM packet used in the automatic discovery of group-to-rendezvous point (RP) mapping and the actions taken on the address-to-RP mapping database.</td>
</tr>
<tr>
<td><strong>bsr</strong></td>
<td>(Optional) Displays candidate-RPs and Bootstrap Router (BSR) activity.</td>
</tr>
<tr>
<td><strong>df</strong></td>
<td>(Optional) When bidirectional PIM is used, displays all designated forwarder (DF) election messages.</td>
</tr>
<tr>
<td><strong>rp-address</strong></td>
<td>(Optional) The rendezvous point IP address.</td>
</tr>
<tr>
<td><strong>hello</strong></td>
<td>(Optional) Displays events associated with PIM hello messages.</td>
</tr>
<tr>
<td><strong>tag</strong></td>
<td>(Optional) Displays tag-switching-related activity.</td>
</tr>
</tbody>
</table>

**Command Default**

All PIM packets are displayed.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.1</td>
<td>The <code>auto-rp</code> keyword was added.</td>
</tr>
<tr>
<td>11.3</td>
<td>The <code>atm</code> and <code>tag</code> keywords were added.</td>
</tr>
<tr>
<td>12.1(2)T</td>
<td>The <code>df</code> keyword was added.</td>
</tr>
<tr>
<td>12.1(3)T</td>
<td>The <code>bsr</code> keyword was added.</td>
</tr>
</tbody>
</table>
The `vrf` keyword, `vrf-name` argument, and `hello` keyword were added.

The `vrf` keyword and `vrf-name` argument were added.

This command was integrated into Cisco IOS Release 12.2(14)S.

The `hello` keyword was added.

This command was integrated into Cisco IOS Release 12.2(28)SB.

This command was integrated into Cisco IOS Release 12.2(33)SRA.

This command was integrated into Cisco IOS Release 12.2(33)SXH.

**Usage Guidelines**

PIM uses Internet Group Management Protocol (IGMP) packets to communicate with routers and advertise reachability information.

Use this command with the `debug ip igmp` and `debug ip mrouter` commands to display additional multicast routing information.

**Examples**

The following is sample output from the `debug ip pim` command:

```
Router# debug ip pim 224.2.0.1
PIM: Received Join/Prune on Ethernet1 from 172.16.37.33
PIM: Received Join/Prune on Ethernet1 from 172.16.37.33
PIM: Received Join/Prune on Tunnel0 from 10.3.84.1
PIM: Received Join/Prune on Ethernet1 from 172.16.37.33
PIM: Received Join/Prune on Ethernet1 from 172.16.37.33
PIM: Received RP-Reachable on Ethernet1 from 172.16.20.31
PIM: Update RP expiration timer for 224.2.0.1
PIM: Forward RP-reachability packet for 224.2.0.1 on Tunnel0
PIM: Received Join/Prune on Ethernet1 from 172.16.37.33
PIM: Prune-list (10.221.196.51/32, 224.2.0.1)
PIM: Set join delay timer to 2 seconds for (10.221.0.0/16, 224.2.0.1) on Ethernet1
PIM: Received Join/Prune on Ethernet1 from 172.16.37.6
PIM: Received Join/Prune on Tunnel0 from 10.3.84.1
PIM: Join-list: (*, 224.2.0.1) RP 172.16.20.31
PIM: Add Tunnel0 to (*, 224.2.0.1), Forward state
PIM: Join-list: (10.0.0.0/8, 224.2.0.1)
PIM: Add Tunnel0 to (10.0.0.0/8, 224.2.0.1), Forward state
PIM: Join-list: (10.4.0.0/16, 224.2.0.1)
PIM: Prune-list (172.16.84.16/28, 224.2.0.1) RP-bit set RP 172.16.84.16
PIM: Send Prune on Ethernet1 to 172.16.37.6 for (172.16.84.16/28, 224.2.0.1), RP
PIM: For RP, Prune-list: 10.9.0.0/16
PIM: For RP, Prune-list: 10.16.0.0/16
PIM: For RP, Prune-list: 10.49.0.0/16
PIM: For RP, Prune-list: 10.84.0.0/16
PIM: For RP, Prune-list: 10.146.0.0/16
PIM: For 10.3.84.1, Join-list: 172.16.84.16/28
PIM: Send periodic Join/Prune to RP via 172.16.37.6 (Ethernet1)
```

The following lines appear periodically when PIM is running in sparse mode and indicate to this router the multicast groups and multicast sources in which other routers are interested:
The following lines appear when a rendezvous point (RP) message is received and the RP timer is reset. The expiration timer sets a checkpoint to make sure the RP still exists. Otherwise, a new RP must be discovered.

PIM: Received RP-Reachable on Ethernet1 from 172.16.20.31
PIM: Update RP expiration timer for 224.2.0.1
PIM: Forward RP-reachability packet for 224.2.0.1 on Tunnel0

The prune message in the following line states that this router is not interested in the Source-Active (SA) information. This message tells an upstream router to stop forwarding multicast packets from this source. The address 10.221.196.51/32 indicates a host route with 32 bits of mask.

PIM: Prune-list (10.221.196.51/32, 224.2.0.1)

In the following line, a second router on the network wants to override the prune message that the upstream router just received. The timer is set at a random value so that if additional routers on the network still want to receive multicast packets for the group, only one will actually send the message. The other routers will receive the join message and then suppress sending their own message.

PIM: Set join delay timer to 2 seconds for (10.221.0.0/16, 224.2.0.1) on Ethernet1

In the following line, a join message is sent toward the RP for all sources:

PIM: Join-list: (*, 224.2.0.1) RP 172.16.20.31

In the following lines, the interface is being added to the outgoing interface (OIF) of the (*, G) and (S, G) multicast route (mroute) table entry so that packets from the source will be forwarded out that particular interface:

PIM: Add Tunnel0 to (*, 224.2.0.1), Forward state
PIM: Add Tunnel0 to {10.0.0.0/8, 224.2.0.1}, Forward state

The following line appears in sparse mode only. There are two trees on which data may be received: the RP tree and the source tree. In dense mode there is no RP. After the source and the receiver have discovered one another at the RP, the first-hop router for the receiver will usually join to the source tree rather than the RP tree.

PIM: Prune-list (172.16.84.16/28, 224.2.0.1) RP-bit set RP 172.16.84.16

The send prune message in the next line shows that a router is sending a message to a second router saying that the first router should no longer receive multicast packets for the (S, G). The RP at the end of the message indicates that the router is pruning the RP tree and is most likely joining the source tree, although the router may not have downstream members for the group or downstream routers with members of the group. The output shows the specific sources from which this router no longer wants to receive multicast messages.

PIM: Send Prune on Ethernet1 to 172.16.37.6 for {172.16.84.16/28, 224.2.0.1}, RP

The following lines indicate that a prune message is sent toward the RP so that the router can join the source tree rather than the RP tree:

PIM: For RP, Prune-list: 10.9.0.0/16
PIM: For RP, Prune-list: 10.16.0.0/16
PIM: For RP, Prune-list: 10.49.0.0/16

In the following line, a periodic message is sent toward the RP. The default period is once per minute. Prune and join messages are sent toward the RP or source rather than directly to the RP or source. It is the responsibility of the next hop router to take proper action with this message, such as continuing to forward it to the next router in the tree.

PIM: Send periodic Join/Prune to RP via 172.16.37.6 (Ethernet1)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip dvmrp</td>
<td>Displays information on DVMRP packets received and sent.</td>
</tr>
<tr>
<td>debug ip igmp</td>
<td>Displays IGMP packets received and sent, and displays IGMP host-related events.</td>
</tr>
<tr>
<td>debug ip igrp transactions</td>
<td>Displays transaction information on IGRP routing transactions.</td>
</tr>
<tr>
<td>debug ip mrouting</td>
<td>Displays changes to the IP multicast routing table.</td>
</tr>
<tr>
<td>debug ip sd</td>
<td>Displays all SD announcements received.</td>
</tr>
</tbody>
</table>
**debug ip pim atm**

To log Protocol Independent Multicast (PIM) ATM signalling activity, use the **debug ip pim atm** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip pim atm
no debug ip pim atm
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Examples**

The following sample output shows a new group being created and the router toward the rendezvous point (RP) opening a new virtual circuit (VC). Because there are now two groups on this router, there are two VCs open, as reflected by the “current count.”

The following is sample output from the **debug ip pim atm** command:

```
Router# debug ip pim atm
Jan 28 19:05:51: PIM-ATM: Max VCs 200, current count 1
Jan 28 19:05:51: PIM-ATM: Send SETUP on ATM2/0 for 239.254.254.253/171.69.214.43
Jan 28 19:05:51: PIM-ATM: Received CONNECT on ATM2/0 for 239.254.254.253, vcd 19
Jan 28 19:06:35: PIM-ATM: Max VCs 200, current count 2
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 28 19:05:51</td>
<td>Current date and time (in hours:minutes:seconds).</td>
</tr>
<tr>
<td>PIM-ATM</td>
<td>Indicates what PIM is doing to set up or monitor an ATM connection (vc).</td>
</tr>
<tr>
<td>current count</td>
<td>Current number of open virtual circuits.</td>
</tr>
</tbody>
</table>

The resulting **show ip mroute** output follows:

```
Router# show ip mroute 239.254.254.253
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 239.254.254.253), 00:00:04/00:02:53, RP 171.69.214.50, flags: S
   Incoming interface: Ethernet1/1, RFF nbr 171.69.214.50
   Outgoing interface list:
      ATM2/0, VCD 19, Forward/Sparse-Dense, 00:00:04/00:02:52
```
debug ip pim auto-rp

To display the contents of each Protocol Independent Multicast (PIM) packet used in the automatic discovery of group-to-rendezvous point (RP) mapping and the actions taken on the address-to-RP mapping database, use the `debug ip pim auto-rp` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip pim auto-rp [vrf vrf-name]
no debug ip pim auto-rp [vrf vrf-name]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>(Optional) Supports the Multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td>vrf-name</td>
<td>(Optional) Name assigned to the VRF.</td>
</tr>
</tbody>
</table>

| Command Default     | No default behavior or values. |
| Command Modes       | Privileged EXEC |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(23)S</td>
<td></td>
<td>The <code>vrf</code> keyword and <code>vrf-name</code> argument were added.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td></td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td></td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td></td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td></td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Examples</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# debug ip pim auto-rp</td>
<td></td>
</tr>
<tr>
<td>Auto-RP: Received RP-announce, from 172.16.214.66, RP_cnt 1, holdtime 180 secs</td>
<td></td>
</tr>
<tr>
<td>Auto-RP: Build RP-Discovery packet</td>
<td></td>
</tr>
<tr>
<td>Auto-RP: Build mapping (192.168.248.0/24, RP:172.16.214.66),</td>
<td></td>
</tr>
<tr>
<td>Auto-RP: Send RP-discovery packet (3 RP entries)</td>
<td></td>
</tr>
<tr>
<td>Auto-RP: Build RP-Announce packet for 172.16.214.2</td>
<td></td>
</tr>
<tr>
<td>Auto-RP: Build announce entry for (192.168.254.0/24)</td>
<td></td>
</tr>
<tr>
<td>Auto-RP: Send RP-Announce packet, IP source 172.16.214.2, ttl 8</td>
<td></td>
</tr>
</tbody>
</table>

The first two lines show a packet received from 172.16.214.66 announcing that it is the RP for the groups in 192.168.248.0/24. This announcement contains one RP address and is valid for 180 seconds. The RP-mapping agent then updates its mapping database to include the new information.
In the next five lines, the router creates an RP-discovery packet containing three RP mapping entries. The packet is sent to the well-known CISCO-RP-DISCOVERY group address (224.0.1.40).

The final three lines show the router announcing that it intends to be an RP for the groups in 192.168.254.0/24. Only routers inside the scope “ttl 8” receive the advertisement and use the RP for these groups.

The following is sample output from the debug ip pim auto-rp command when a router receives an update. In this example, the packet contains three group-to-RP mappings, which are valid for 180 seconds. The RP-mapping agent then updates its mapping database to include the new information.
**debug ip policy**

To display IP policy routing packet activity, use the `debug ip policy` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip policy [access-list-name]
no debug ip policy [access-list-name]
```

**Syntax Description**

- `access-list-name` *(Optional)* The name of the access list. Displays packets permitted by the access list that are policy routed in process level, Cisco Express Forwarding (CEF), and distributed CEF (DCEF) with NetFlow enabled or disabled.

  If no access list is specified, information about all policy-matched and policy-routed packets is displayed.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(3)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

After you configure IP policy routing with the `ip policy` and `route-map` commands, use the `debug ip policy` command to ensure that the IP policy is configured correctly.

Policy routing looks at various parts of the packet and then routes the packet based on certain user-defined attributes in the packet.

The `debug ip policy` command helps you determine what policy routing is following. It displays information about whether a packet matches the criteria, and if so, the resulting routing information for the packet.

**Caution**

Because the `debug ip policy` command generates a substantial amount of output, use it only when traffic on the IP network is low, so other activity on the system is not adversely affected.

**Examples**

The following is sample output from the `debug ip policy` command:

```
Router# debug ip policy 3
IP: s=30.0.0.1 (Ethernet0/0/1), d=40.0.0.7, len 100, FIB flow policy match
IP: s=30.0.0.1 (Ethernet0/0/1), d=40.0.0.7, len 100, FIB PR flow accelerated!
IP: s=30.0.0.1 (Ethernet0/0/1), d=40.0.0.7, g=10.0.0.8, len 100, FIB policy routed
```

The table below describes the significant fields shown in the display.
### Table 50: `debug ip policy` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>s=</td>
<td>IP source address and interface of the packet being routed.</td>
</tr>
<tr>
<td>d=</td>
<td>IP destination address of the packet being routed.</td>
</tr>
<tr>
<td>len</td>
<td>Length of the packet.</td>
</tr>
<tr>
<td>g=</td>
<td>IP gateway address of the packet being routed.</td>
</tr>
</tbody>
</table>
debug ip rbscp

To display general error messages about access list-based Rate-Based Satellite Control Protocol (RBSCP), use the `debug ip rbscp` command in privileged EXEC mode. To disable debug output, use the `no` form of this command.

```
debug ip rbscp
no debug ip rbscp
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

RBSCP debugging is disabled by default.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

⚠️ **Caution**

Using this command will impact the router’s forwarding performance.

**Examples**

The following is sample output from the `debug ip rbscp` command. The hexadecimal number is the sequence number to keep track of the flow.

```
Router# debug ip rbscp
*May 11 02:17:01.407: RBSCP process: 0x662852D0 passed access list
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip rbscp ack-split</td>
<td>Displays information about TCP ACK splitting done in conjunction with RBSCP.</td>
</tr>
<tr>
<td>ip rbscp ack-split</td>
<td>Configures the TCP ACK splitting feature of RBSCP on an outgoing interface for packets that are permitted by a specified access list.</td>
</tr>
</tbody>
</table>
### debug ip rbscp ack-split

To display information about TCP ACK splitting done in conjunction with Rate-Based Satellite Control Protocol (RBSCP), use the debug ip rbscp ack-split command in privileged EXEC mode. To disable debug output, use the no form of this command.

```plaintext
debug ip rbscp ack-split
no debug ip rbscp ack-split
```

#### Syntax Description

This command has no arguments or keywords.

#### Command Default

RBSCP debugging for TCP ACKs is disabled by default.

#### Command Modes

Privileged EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

Caution

Using this command will impact the router’s forwarding performance.

#### Examples

The following is sample output from the debug ip rbscp ack-split command when the packets match the access list applied to RBSCP. The output includes the source and destination IP addresses and port numbers, the hexadecimal sequence number, and the cumulative ACK that acknowledges bytes up to that number.

```plaintext
Router# debug ip rbscp ack-split
*May 11 02:17:01.407: RBSCP ACK split: 0x662852D0, input FastEthernet1/0 -> output FastEthernet1/1
*May 11 02:17:01.407: RBSCP ACK split: rcvd src 1.1.1.1:30481 -> dst 3.3.3.1:21, cumack 2336109115
*May 11 02:17:01.407: RBSCP ACK split: generated 0x65FC0874 cumack 2336109112
*May 11 02:17:01.407: RBSCP ACK split: generated 0x66762A78 cumack 2336109113
*May 11 02:17:01.407: RBSCP ACK split: generated 0x6676442C cumack 2336109114
*May 11 02:17:01.407: RBSCP ACK split: releasing original ACK 2336109115
*May 11 02:17:01.415: RBSCP process: 0x662852D0 passed access list
*May 11 02:17:01.415: RBSCP ACK split: 0x662852D0, input FastEthernet1/0 -> output FastEthernet1/1
*May 11 02:17:01.415: RBSCP ACK split: rcvd src 1.1.1.1:36022 -> dst 3.3.3.1:20240, cumack 4024420742
*May 11 02:17:01.415: RBSCP ACK split: generated 0x65FC1E7C cumack 4024420739
*May 11 02:17:01.415: RBSCP ACK split: generated 0x65FC2980 cumack 4024420740
*May 11 02:17:01.415: RBSCP ACK split: generated 0x65FC3484 cumack 4024420741
*May 11 02:17:01.415: RBSCP ACK split: releasing original ACK 4024420742
*May 11 02:17:01.419: RBSCP process: 0x662852D0 passed access list
*May 11 02:17:01.419: RBSCP ACK split: 0x662852D0, input FastEthernet1/0 -> output FastEthernet1/1
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip rbscp</td>
<td>Displays general error messages about access list-based RBSCP.</td>
</tr>
<tr>
<td>ip rbscp ack-split</td>
<td>Configures the TCP ACK splitting feature of RBSCP on an outgoing interface for packets that are permitted by a specified access list.</td>
</tr>
</tbody>
</table>
debug ip rgmp

To log debugging messages sent by a Router-Port Group Management Protocol (RGMP)-enabled router, use the `debug ip rgmp` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip rgmp [{group-namegroup-address}]
no debug ip rgmp
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group-name</code></td>
<td>(Optional) The name of a specific IP multicast group.</td>
</tr>
<tr>
<td><code>group-address</code></td>
<td>(Optional) The IP address of a specific IP multicast group.</td>
</tr>
</tbody>
</table>

### Command Default

Debugging for RGMP is not enabled. If the `debug ip rgmp` command is used without arguments, debugging is enabled for all RGMP message types.

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(10)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(1)E</td>
<td>The command was integrated into Cisco IOS Release 12.1(1)E.</td>
</tr>
<tr>
<td>12.1(5)T</td>
<td>The command was integrated into Cisco IOS Release 12.1(5)T.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Examples

The following shows sample output from the `debug ip rgmp` command:

```
Router# debug ip rgmp
RGMP: Sending a Hello packet on Ethernet1/0
RGMP: Sending a Join packet on Ethernet1/0 for group 224.1.2.3
RGMP: Sending a Leave packet on Ethernet1/0 for group 224.1.2.3
RGMP: Sending a Bye packet on Ethernet1/0
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip rgmp</td>
<td>Enables the RGMP on IEEE 802.3 Ethernet interfaces.</td>
</tr>
<tr>
<td>show ip igmp interface</td>
<td>Displays multicast-related information about an interface.</td>
</tr>
</tbody>
</table>
debug ip rip

To display information on Routing Information Protocol (RIP) routing transactions, use the `debug ip rip` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
default ip rip
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bfd events</code></td>
<td>(Optional) Displays information on RIP Bidirectional Forwarding Detection (BFD)-related events.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (``#``)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(21)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 12.0(21)M.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was modified. The <code>bfd</code> keyword was added.</td>
</tr>
<tr>
<td>15.1(2)S</td>
<td>This command was integrated into Cisco IOS Release 15.1(2)S.</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, the router being debugged has received updates from a router at source address 10.89.80.28. In this scenario, information has been sent to about five destinations in the routing table update. Notice that the fourth destination address in the update, 172.31.0.0, is inaccessible because it is more than 15 hops away from the router from which the update was sent. The router being debugged also sends updates, in both cases to broadcast address 255.255.255.255 as the destination.

```
Router# debug ip rip
RIP: received update from 10.89.80.28 on Ethernet0
    10.89.95.0 in 1 hops
    10.89.81.0 in 1 hops
    10.89.66.0 in 2 hops
    172.31.0.0 in 16 hops (inaccessible)
    0.0.0.0 in 7 hop
RIP: sending update to 255.255.255.255 via Ethernet0 (10.89.64.31)
    subnet 10.89.94.0, metric 1
    172.31.0.0 in 16 hops (inaccessible)
RIP: sending update to 255.255.255.255 via Serial1 (10.89.94.31)
    subnet 10.89.64.0, metric 1
    subnet 10.89.66.0, metric 3
    172.31.0.0 in 16 hops (inaccessible)
    default 0.0.0.0, metric 8
```

The second line is an example of a routing table update. It shows the number of hops between a given Internet address and the router.

The entries show that the router is sending updates that are similar, except that the number in parentheses is the source address encapsulated into the IP header.
The following are examples for the `debug ip rip` command of entries that appear at startup, during an interface transition event, or when a user manually clears the routing table:

RIP: broadcasting general request on Ethernet0
RIP: broadcasting general request on Ethernet1

The following entry is most likely caused by a malformed packet from the sender:

RIP: bad version 128 from 160.89.80.43

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip rip neighbor</code></td>
<td>Displays RIP neighbors for which BFD sessions are created.</td>
</tr>
</tbody>
</table>
debug ip routing

To display information on Routing Information Protocol (RIP) routing table updates and route cache updates, use the `debug ip routing` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip routing
no debug ip routing
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13) T</td>
<td>Support for Interior Gateway Routing Protocol (IGRP) was removed.</td>
</tr>
<tr>
<td>12.2(33) SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33) SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip routing` command:

```
Router# debug ip routing
RT: add 172.25.168.0 255.255.255.0 via 172.24.76.30, igrp metric [100/3020]
RT: metric change to 172.25.168.0 via 172.24.76.30, igrp metric [100/3020]
   new metric [100/2930]
IP: cache invalidation from 0x115248 0x1378A, new version 5736
RT: add 172.26.219.0 255.255.255.0 via 172.24.76.30, igrp metric [100/16200]
RT: metric change to 172.26.219.0 via 172.24.76.30, igrp metric [100/16200]
   new metric [100/10816]
RT: delete route to 172.26.219.0 via 172.24.76.30, igrp metric [100/10816]
RT: no routes to 172.26.219.0, entering holddown
IP: cache invalidation from 0x115248 0x1378A, new version 5737
RT: 172.26.219.0 came out of holddown
RT: garbage collecting entry for 172.26.219.0
IP: cache invalidation from 0x115248 0x1378A, new version 5738
RT: add 172.26.219.0 255.255.255.0 via 172.24.76.30, igrp metric [100/10816]
RT: delete route to 172.26.219.0 via 172.24.76.30, igrp metric [100/10816]
RT: no routes to 172.26.219.0, entering holddown
IP: cache invalidation from 0x115248 0x1378A, new version 5739
RT: 172.26.219.0 came out of holddown
RT: garbage collecting entry for 172.26.219.0
IP: cache invalidation from 0x115248 0x1378A, new version 5740
RT: add 172.26.219.0 255.255.255.0 via 172.24.76.30, igrp metric [100/16200]
RT: metric change to 172.26.219.0 via 172.24.76.30, igrp metric [100/16200]
   new metric [100/10816]
RT: delete route to 172.26.219.0 via 172.24.76.30, igrp metric [100/10816]
RT: no routes to 172.26.219.0, entering holddown
IP: cache invalidation from 0x115248 0x1378A, new version 5741
```

In the following lines, a newly created entry has been added to the IP routing table. The “metric change” indicates that this entry existed previously, but its metric changed and the change was
reported by means of IGRP. The metric could also be reported via RIP, OSPF, or another IP routing protocol. The numbers inside the brackets report the administrative distance and the actual metric.

RT: add 172.25.168.0 255.255.255.0 via 172.24.76.30, igrp metric [100/3020]
RT: metric change to 172.25.168.0 via 172.24.76.30, igrp metric [100/3020]
    new metric [100/2930]
IP: cache invalidation from 0x115248 0x1378A, new version 5736

“Cache invalidation” means that the fast-switching cache was invalidated due to a routing table change. “New version” is the version number of the routing table. When the routing table changes, this number is incremented. The hexadecimal numbers are internal numbers that vary from version to version and software load to software load.

In the following output, the “holddown” and “cache invalidation” lines are displayed. Most of the distance vector routing protocols use “holddown” to avoid typical problems like counting to infinity and routing loops. If you look at the output of the `show ip protocols` command you will see the timer values for “holddown” and “cache invalidation.” “Cache invalidation” corresponds to “came out of holddown.” “Delete route” is triggered when a better path appears. It removes the old inferior path.

RT: delete route to 172.26.219.0 via 172.24.76.30, igrp metric [100/10816]
RT: no routes to 172.26.219.0, entering holddown
IP: cache invalidation from 0x115248 0x1378A, new version 5737
RT: 172.26.219.0 came out of holddown
debug ip routing static bfd

To enable debugging output on IP static Bidirectional Forwarding Detection (BFD) neighbor events, use the `debug ip routing static bfd` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip routing static bfd
no debug ip routing static bfd
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRC</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip routing static bfd` command:

```
Router# debug ip routing static bfd
Ethernet1/1, gw 10.1.1.1 *Dec 18 19:01:48.416: IP-ST: Entering ipstatic_bfd_neighbor_add
Router(config)# ip route 10.2.0.0 255.255.0.0 Ethernet1/1 10.1.1.1
*Dec 18 19:02:06.348: IP-ST: head_gwif: NULL *Dec 18 19:02:06.348: IP-ST: Inserted to GWIF tree (head): 10.2.0.0/16 Et1/1 10.1.1.1 *Dec 18 19:02:16.852: RT: updating static 10.2.0.0/16 (0x0) via 10.1.1.1 Et1/1 *Dec 18 19:02:16.856: RT: add 10.2.0.0/16 via 10.1.1.1, static metric [1/0] RtrB(config)#end RouterB#
```
debug ip rsvp

⚠️

Use this command with a small number of tunnels or Resource Reservation Protocol (RSVP) reservations. Too much data can overload the CPU.

To display debug messages for RSVP categories, use the `debug ip rsvp` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

ddebug ip rsvp [{ all | api | authentication | cli | data-pkts | database | detail | dump-messages | errors | events | fast-reroute | filter [{ acl | vrf * | vrf-name [acl]}]} | function | handles | hello | messages | msg-mgr | path | policy | proxy | rate-limit | reliable-msg | resv | routing | sbm | signalling | snmp | summary-refresh | svc | timeouts | timer | traffic-control | wfq]`

no debug ip rsvp

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>(Optional) RSVP messages for all categories.</td>
</tr>
<tr>
<td>api</td>
<td>(Optional) RSVP application programming interface (API) events.</td>
</tr>
<tr>
<td>authentication</td>
<td>(Optional) RSVP authentication.</td>
</tr>
<tr>
<td>cli</td>
<td>(Optional) RSVP command-line interface (CLI).</td>
</tr>
<tr>
<td>data-pkts</td>
<td>(Optional) RSVP data processing.</td>
</tr>
<tr>
<td>database</td>
<td>(Optional) RSVP database debugging.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) RSVP packet content.</td>
</tr>
<tr>
<td>dump-messages</td>
<td>(Optional) Dump RSVP message content.</td>
</tr>
<tr>
<td>errors</td>
<td>(Optional) Informational debugging messages and messages about irregular events.</td>
</tr>
<tr>
<td>events</td>
<td>(Optional) RSVP process events.</td>
</tr>
<tr>
<td>fast-reroute</td>
<td>(Optional) RSVP fast-reroute support for label-switched paths (LSPs).</td>
</tr>
<tr>
<td>filter</td>
<td>(Optional) RSVP debug message filter.</td>
</tr>
<tr>
<td>acl</td>
<td>(Optional) Number (1 to 199) of the access control list (ACL).</td>
</tr>
<tr>
<td>vrf *</td>
<td>(Optional) A virtual routing and forwarding (VFR) instance. * = A wildcard to display all VRFs.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) A VFR instance. vrf-name = The name of a VRF.</td>
</tr>
<tr>
<td>acl</td>
<td>(Optional) Number (1 to 199) of the ACL for the VRF.</td>
</tr>
<tr>
<td>function</td>
<td>(Optional) RSVP function names.</td>
</tr>
<tr>
<td>handles</td>
<td>(Optional) RSVP database handles event.</td>
</tr>
</tbody>
</table>
debug ip http all through debug ip rsvp

<table>
<thead>
<tr>
<th>hello</th>
<th>(Optional) RSVP hello events.</th>
</tr>
</thead>
<tbody>
<tr>
<td>messages</td>
<td>(Optional) Brief information about all RSVP messages that are sent and received via IP debugging.</td>
</tr>
<tr>
<td>msg-mgr</td>
<td>(Optional) RSVP message-manager events.</td>
</tr>
<tr>
<td>path</td>
<td>(Optional) RSVP PATH messages.</td>
</tr>
<tr>
<td>policy</td>
<td>(Optional) RSVP policy information.</td>
</tr>
<tr>
<td>proxy</td>
<td>(Optional) Proxy API trace.</td>
</tr>
<tr>
<td>rate-limit</td>
<td>(Optional) RSVP rate-limiting events.</td>
</tr>
<tr>
<td>reliable-msg</td>
<td>(Optional) RSVP reliable messages events.</td>
</tr>
<tr>
<td>resv</td>
<td>(Optional) RSVP RESV messages.</td>
</tr>
<tr>
<td>routing</td>
<td>(Optional) RSVP routing messages.</td>
</tr>
<tr>
<td>sbm</td>
<td>(Optional) RSVP subnet bandwidth manager (SBM) messages.</td>
</tr>
<tr>
<td>signalling</td>
<td>(Optional) RSVP signalling (PATH and RESV) messages.</td>
</tr>
<tr>
<td>snmp</td>
<td>(Optional) RSVP Simple Network Management Protocol (SNMP) events.</td>
</tr>
<tr>
<td>sso</td>
<td>(Optional) RSVP stateful switchover (SSO) events.</td>
</tr>
<tr>
<td>summary-refresh</td>
<td>(Optional) RSVP summary refresh and bundle messages events.</td>
</tr>
<tr>
<td>svc</td>
<td>(Optional) Switched virtual circuit (SVC) events.</td>
</tr>
<tr>
<td>timeouts</td>
<td>(Optional) RSVP refresh timeouts.</td>
</tr>
<tr>
<td>timer</td>
<td>(Optional) RSVP timer events.</td>
</tr>
<tr>
<td>traffic-control</td>
<td>(Optional) RSVP traffic control events.</td>
</tr>
<tr>
<td>wfq</td>
<td>(Optional) RSVP weighted fair queueing (WFQ) events.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>The <code>dump-messages</code>, <code>msg-mgr</code>, <code>proxy</code>, <code>rate-limit</code>, <code>reliable-msg</code>, and <code>summary-refresh</code> keywords were added.</td>
</tr>
<tr>
<td>12.0(23)S</td>
<td>The <code>timeouts</code> keyword was added.</td>
</tr>
<tr>
<td>12.0(24)S</td>
<td>The <code>hello</code> keyword was added.</td>
</tr>
</tbody>
</table>
### Modifications

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>The command output was modified to display RSVP source address and interface information.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was modified. The optional <code>vrf</code> and <code>*</code> keywords and <code>vrf-name</code> argument were added.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was modified. For point-to-multipoint traffic engineering tunnels, the output displays the destination address of the sub-label switched path (LSP).</td>
</tr>
</tbody>
</table>

### Examples

#### RSVP Source Address and Interface Examples

The following output appears in `source-address`: `source-address` format after you configure a source address and enable the `debug ip rsvp cli` command:

```
Router# debug ip rsvp cli
RSVP cli debugging is on

*Sep 11 06:33:27.203: RSVP: RSVP source-address is enabled on interface Ethernet1/0.
source-address: 10.1.3.13
```

The following output appears in `source-interface::address`: `source-interface::address` format after you configure a source interface address and enable the `debug ip rsvp cli` command:

```
*Sep 11 06:33:27.203: RSVP: RSVP source-interface is enabled on interface Ethernet1/0.
source-interface::address: Loopback0::10.1.1.1
```

The following output appears when you enable the `debug ip rsvp path` command and configure a source address in the HOP object of PATH, PATHTEAR, or PATHERROR messages:

```
*Sep 12 08:56:46.267: RSVP: 10.1.1.1_200->10.4.4.4_100[0.0.0.0]: building hop object with src addr: 10.2.3.23
```

#### RSVP Signaling and Messages Examples

The following commands show how to enable debugging for RSVP signaling and messages:

```
Router# debug ip rsvp signalling
RSVP signalling messages (Summary) debugging is on
Router# debug ip rsvp messages
RSVP messages (sent/received via IP) debugging is on
```
The following output displays RSVP signaling-related events that include sending and receiving PATH and RESV messages, admitting new reservations, establishing sessions, sending and receiving acknowledgments (ACKs), and sending and receiving summary refresh messages:

```
01:14:56:RSVP 10.20.1.1_19->10.75.1.1_100[10.20.1.1]:Received Path message from 10.20.1.1 (on sender host)
01:14:56:RSVP: new path message passed parsing, continue...
01:14:56:RSVP 10.20.1.1_19->10.75.1.1_100[10.20.1.1]:Refresh Path psb = 6164BB0 refresh interval = 0mSec
01:14:56:RSVP 10.20.1.1_19->10.75.1.1_100[10.20.1.1]:Sending Path message to 10.4.4.2
01:14:56:RSVP session 10.75.1.1_100[10.20.1.1]:Path sent by IP to 10.4.4.2 length=216 checksum=B1E4 TOS=0xC0 prerouted=YES router_alert=YES udp=NO (Ethernet1)
01:14:57:RSVP:Resv received from IP layer (IP HDR 10.4.4.2->10.4.4.1)
01:14:57:RSVP session 10.75.1.1_100[10.20.1.1]:Received RESV for 10.75.1.1 (Ethernet1) from 10.4.4.2
01:14:57:RSVP 10.20.1.1_19->10.75.1.1_100[10.20.1.1]:reservation not found--new one
01:14:57:RSVP-RESV:Admitting new reservation:6165D0E4
01:14:57:RSVP 10.20.1.1_19->10.75.1.1_100[10.20.1.1]:RSVP bandwidth is available
01:14:57:RSVP-RESV:reservation was installed:6165D0E4
01:14:57:RSVP:Sending Unknown message to 10.4.4.2
01:14:57:RSVP:Ack sent by IP to 10.4.4.2 length=20 checksum=34A7 TOS=0x00 prerouted=NO router_alert=NO udp=NO (Ethernet1)
01:14:57:RSVP 10.20.1.1_19->10.75.1.1_100[10.20.1.1]:Refresh Path psb = 6164BB0 refresh interval = 937mSec
01:15:26:RSVP 10.20.1.1_19->10.75.1.1_100[10.20.1.1]:Sending Path message to 10.4.4.2
01:15:26:RSVP session 10.75.1.1_100[10.20.1.1]:Path sent by IP to 10.4.4.2 length=216 checksum=B1E4 TOS=0xC0 prerouted=YES router_alert=NO udp=NO (Ethernet1)
01:15:26:RSVP:Resv received from IP layer (IP HDR 10.4.4.2->10.4.4.1)
01:15:26:RSVP session 10.75.1.1_100[10.20.1.1]:Received RESV for 10.75.1.1 (Ethernet1) from 10.4.4.2
01:15:26:RSVP 10.20.1.1_19->10.75.1.1_100[10.20.1.1]:reservation found--processing possible change:6165D0E4
01:15:26:RSVP 10.20.1.1_19->10.75.1.1_100[10.20.1.1]:No change in reservation
01:15:27:RSVP:Sending Ack message to 10.4.4.2
01:15:27:RSVP:Ack sent by IP to 10.4.4.2 length=20 checksum=34A7 TOS=0x00 prerouted=NO router_alert=NO udp=NO (Ethernet1)
01:15:27:RSVP 10.20.1.1_19->10.75.1.1_100[10.20.1.1]:Reservation state is being refreshed for 0x91
01:15:27:RSVP:Sending Ack message to 10.4.4.2
01:15:27:RSVP:Ack sent by IP to 10.4.4.2 length=20 checksum=34A5 TOS=0x00 prerouted=NO router_alert=NO udp=NO (Ethernet1)
01:15:56:RSVP 10.20.1.1_19->10.75.1.1_100[10.20.1.1]:Sending Srefresh message to 10.4.4.2
01:15:56:RSVP:Srefresh sent by IP to 10.4.4.2 length=32 checksum=CA0D TOS=0x00 prerouted=NO router_alert=NO udp=NO (Ethernet1)
01:15:56:RSVP:Ack received from IP layer (IP HDR 10.4.4.2->10.4.4.1)
01:15:56:RSVP:Srefresh received from IP layer (IP HDR 10.4.4.2->10.4.4.1)
01:15:56:RSVP:Srefresh:Resv state is being refreshed for 0x91
01:15:56:RSVP:Sending Ack message to 10.4.4.2
01:15:56:RSVP:Ack sent by IP to 10.4.4.2 length=20 checksum=34A5 TOS=0x00 prerouted=NO router_alert=NO udp=NO (Ethernet1)
01:16:26:RSVP 10.20.1.1_19->10.75.1.1_100[10.20.1.1]:Sending Srefresh message to 10.4.4.2
01:16:26:RSVP:Srefresh sent by IP to 10.4.4.2 length=32 checksum=CA0C TOS=0x00 prerouted=NO router_alert=NO udp=NO (Ethernet1)
01:16:26:RSVP:Ack received from IP layer (IP HDR 10.4.4.2->10.4.4.1)
01:16:26:RSVP:Srefresh received from IP layer (IP HDR 10.4.4.2->10.4.4.1)
01:16:26:RSVP:Srefresh:Resv state is being refreshed for 0x91
01:16:26:RSVP:Sending Ack message to 10.4.4.2
01:16:26:RSVP:Ack sent by IP to 10.4.4.2 length=20 checksum=34A3 TOS=0x00 prerouted=NO router_alert=NO udp=NO (Ethernet1)
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show debug</td>
<td>Displays active debug output.</td>
</tr>
</tbody>
</table>
**debug ip rsvp aggregation**

To display debugging output for Resource Reservation Protocol (RSVP) aggregation sessions, use the `debug ip rsvp aggregation` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip rsvp aggregation
no debug ip rsvp aggregation
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.6</td>
<td>This command was integrated into Cisco IOS XE Release 2.6.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays information about RSVP aggregation sessions.

RSVP aggregation maintains a Finite State Machine (FSM) for each aggregate session. The RSVP code uses the FSM to maintain aggregate states and transition between the states of an aggregate. For example, after the aggregator sends out the aggregate PATH message, a new state will be entered for the aggregate session (RESV_WAIT) to reflect that an aggregate RESV message is expected. If an aggregate RESV message is received, the session enters the ESTABLISHED state. If an aggregate RESV is not received within a timeout, the aggregate session is cleaned and the process starts again.

Each aggregate reservation can be in one of the following states:

- **PATH_WAIT**—Valid at the deaggregator only. The aggregate reservation at the deaggregator enters this state after the deaggregator has sent a PATHERROR message requesting a new aggregate needed.
- **RESV_WAIT**—Valid at the aggregator only. The aggregate reservation at the aggregator enters this state after the aggregator has sent a PATH message for the aggregate reservation.
- **RESVCONF_WAIT**—Valid at the deaggregator only. The aggregate reservation at the deaggregator enters this state after the deaggregator has sent a RESV message for the aggregate reservation.
- **ESTABLISHED**—Valid at both the aggregator and the deaggregator. The aggregator enters this state after a RESVCONF message has been sent. The deaggregator enters this state after it receives a RESVCONF message for the aggregate reservation.
- **SHUT_DELAY**—Valid at both the aggregator and the deaggregator. The aggregator and the deaggregator enter this state after the last end-to-end (E2E) reservation has been removed.

There are timers associated with the PATH_WAIT, RESV_WAIT, RESVCONF_WAIT, and SHUT_DELAY states. For example, if an event that is needed to move the FSM out of the PATH_WAIT, RESV_WAIT, or RESVCONF_WAIT state does not occur, (that is, an aggregate PATH message is not received when in the PATH_WAIT state), the timer expires and the aggregate is cleared.
In the successful scenario, the aggregate stays in the ESTABLISHED state as long as some E2E flows are aggregated. Both the aggregator and the deaggregator stay in the SHUT_DELAY state until the timer expires or an aggregate RESVTEAR or PATHTEAR message is received.

**Examples**

The following example shows output from the `debug ip rsvp aggregation` command taken at an aggregator:

```
Router# debug ip rsvp aggregation
RSVP aggregation debugging is on
* Jan 25 18:40:03.385: RSVP-AGG-3175: 10.3.3.3->10.4.4.4_46[A][4AB8208]:
  event=NEW_AGG_NEEDED, current state=START
* Jan 25 18:40:03.385: RSVP-AGG-3175: 10.3.3.3->10.4.4.4_46[A][4AB8208]: triggered Aggregate Path to 10.4.4.4
* Jan 25 18:40:03.385: RSVP-AGG-3175: 10.3.3.3->10.4.4.4_46[A][4AB8208]: new state=RESV_WAIT
* Jan 25 18:40:03.441: RSVP-AGG-3175: 10.3.3.3->10.4.4.4_46[A][4AB8208]:
  event=AGG_RESV_STATE_CREATED, current state=RESV_WAIT
* Jan 25 18:40:03.441: RSVP-AGG-3175: 10.3.3.3->10.4.4.4_46[A][4AB8208]: new state=ESTABLISHED
* Jan 25 18:40:03.465: RSVP-AGG-3175: 10.3.3.3->10.4.4.4_46[A][4AB8208]:
  event=E2E_RESV_STATE_CREATED, current state=ESTABLISHED
* Jan 25 18:40:03.465: RSVP-AGG-3175: 10.3.3.3->10.4.4.4_46[A][4AB8208]:
  event=E2E_RESV_STATE_ADMITTED, current state=ESTABLISHED
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show debugging</code></td>
<td>Displays active debug output.</td>
</tr>
</tbody>
</table>
debug ip rsvp authentication

To display debugging output related to Resource Reservation Protocol (RSVP) authentication, use the debug ip rsvp authentication command in privileged EXEC mode. To disable debugging output, use the no form of this command.

**debug ip rsvp authentication**

**no debug ip rsvp authentication**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

After you enable RSVP authentication, RSVP logs system error events whenever an authentication check fails. These events are logged instead of just being displayed when debugging is enabled because they may indicate potential security attacks. The events are generated when:

- RSVP receives a message that does not contain the correct cryptographic signature. This could be due to misconfiguration of the authentication key or algorithm on one or more RSVP neighbors, but it may also indicate an (unsuccessful) attack.
- RSVP receives a message with the correct cryptographic signature, but with a duplicate authentication sequence number. This may indicate an (unsuccessful) message replay attack.
- RSVP receives a message with the correct cryptographic signature, but with an authentication sequence number that is outside the receive window. This could be due to a reordered burst of valid RSVP messages, but it may also indicate an (unsuccessful) message replay attack.
- Failed challenges result from timeouts or bad challenge responses.

**Examples**

The following example shows output from the debug ip rsvp authentication command in which the authentication type (digest) and the sequence number have been validated:

```
Router# debug ip rsvp authentication
RSVP authentication debugging is on
Router# show debugging
*Jan 30 08:10:46.335:RSVP_AUTH:Resv integrity digest from 192.168.101.2 valid
*Jan 30 08:10:46.335:RSVP_AUTH:Resv integrity sequence number 13971113505298841601 from 192.168.101.2 valid
*Jan 30 08:10:46.335:RSVP_AUTH:Resv from 192.168.101.2 passed all authentication checks
```
Cisco routers using RSVP authentication on Cisco IOS software ideally should have clocks that can be accurately restored to the correct time when the routers boot. This capability is available on certain Cisco routers that have clocks with battery backup. For those platforms that do not have battery backup, consider configuring the router to keep its clock synchronized with a Network Time Protocol (NTP) time server. Otherwise, if two adjacent routers have been operating with RSVP authentication enabled and one of them reboots such that its clock goes backward in time, it is possible (but unlikely) the router that did not reboot will log RSVP authentication sequence number errors.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip rsvp authentication</td>
<td>Activates RSVP cryptographic authentication.</td>
</tr>
<tr>
<td>show debugging</td>
<td>Displays active debug output.</td>
</tr>
</tbody>
</table>
**debug ip rsvp detail**

To display detailed information about Resource Reservation Protocol (RSVP)-enabled and Subnetwork Bandwidth Manager (SBM) message processing, use the `debug ip rsvp detail` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip rsvp detail
no debug ip rsvp detail
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(23)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(23)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the detailed debug information about RSVP and SBM that is available when you enable debug mode through the `debug ip rsvp detail` command:

```
Router# debug ip rsvp detail
RSVP debugging is on
router2#u
*Dec 31 16:44:29.651: RSVP: send I_AM_DSBM message from 145.2.2.150
*Dec 31 16:44:29.651: RSVP: IP to 224.0.0.17 length=88 checksum=43AF (Ethernet2)
ttl:254 reserved:0 length:88
*Dec 31 16:44:29.651: DSBM_IP_ADDR type 1 length 8 : 91020296
*Dec 31 16:44:29.651: HOP_L2 type 1 length 12: 00E01ECE
*Dec 31 16:44:29.651: SBM_PRIORITY type 1 length 8 : 00000064
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ip rsvp</code></td>
<td>Displays information about SBM message processing, the DSBM election process, and RSVP message processing.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>debug ip rsvp detail sbm</td>
<td>Displays detailed information about the contents of SMB messages only, and SBM and DSBM state transitions.</td>
</tr>
<tr>
<td>ip rsvp dsbm-candidate</td>
<td>Configures an interface as a DSBM candidate.</td>
</tr>
<tr>
<td>show ip rsvp sbm</td>
<td>Displays information about SBM configured for a specific RSVP-enabled interface or all RSVP-enabled interfaces on the router.</td>
</tr>
</tbody>
</table>
debug ip rsvp dump-messages

⚠️  Caution

Use this command with a small number of tunnels or Resource Reservation Protocol (RSVP) reservations. Too much data can overload the console.

To display debugging messages for all RSVP events, use the `debug ip rsvp dump-messages` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip rsvp dump-messages [{hex | path | resv | sbm | signalling}]
no debug ip rsvp dump-messages
```

**Syntax Description**

- **hex**: (Optional) Hex dump of packet contents.
- **path**: (Optional) Contents of Path messages.
- **resv**: (Optional) Contents of Resv messages.
- **sbm**: (Optional) Contents of SBM messages.
- **signalling**: (Optional) Contents of all signaling (Path and Resv) messages.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(24)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(24)S.</td>
</tr>
</tbody>
</table>

**Examples**

The following command shows how to enable debugging for RSVP events:

```
Router# debug ip rsvp dump-messages
RSVP message dump debugging is on
```

In the following display, notice that a Path message is transmitted and an ACK_DESIRED flag is set for ID: 0x26 Epoch: 0x76798A. In response, a Resv message is sent and an acknowledgment (ACK) is issued for ID: 0x26 Epoch: 0x76798A indicating the RSVP state is established on the neighboring router:

```
00:37:15: RSVP: version:1 flags:0000 type:PROXY_PATH cksum:0000 ttl:255 reserved:0 length:212
00:37:15: SESSION type 7 length 16:
00:37:15: Destination 140.75.1.1, TunnelId 100, Source 140.20.1.1, Protocol 0, Flags 0000
00:37:15: HOP type 1 length 12:
00:37:15: Neighbor 140.20.1.1, LIH 0x80000000
```
00:37:15: TIME_VALUES type 1 length 8:
00:37:15: Refresh period is 30000 msecs
00:37:15: SENDER_TEMPLATE type 7 length 12:
00:37:15: Source 140.20.1.1, tunnel_id 9
00:37:15: SENDER_TSPEC type 2 length 36:
00:37:15: version=0, length in words=7
00:37:15: Token bucket fragment (service_id=1, length=6 words
00:37:15: parameter id=127, flags=0, parameter length=5
00:37:15: average rate=1250 bytes/sec, burst depth=1000 bytes
00:37:15: peak rate =-1250 bytes/sec
00:37:15: min unit=0 bytes, max pkt size=4294967295 bytes
00:37:15: ADSPEC type 2 length 48:
00:37:15: version=0 length in words=10
00:37:15: General Parameters break bit=0 service length=8
00:37:15: IS Hops:0
00:37:15: Minimum Path Bandwidth (bytes/sec):2147483647
00:37:15: Path Latency (microseconds):0
00:37:15: Path MTU:-1
00:37:15: Controlled Load Service break bit=0 service length=0
00:37:15: LABEL_REQUEST type 1 length 8:
00:37:15: Layer 3 protocol ID:2048
00:37:15: EXPLICIT_ROUTE type 1 length 36:
00:37:15: (1) Strict IPv4 Prefix, 8 bytes, 140.20.1.1/32
00:37:15: (2) Strict IPv4 Prefix, 8 bytes, 140.4.4.2/32
00:37:15: (3) Strict IPv4 Prefix, 8 bytes, 140.70.1.1/32
00:37:15: (4) Strict IPv4 Prefix, 8 bytes, 140.70.1.2/32
00:37:15: SESSION_ATTRIBUTE type 7 length 28:
00:37:15: Session name:tagsw4500-21_t100
00:37:15: Setup priority?:7, reservation priority?:
00:37:15: Status:May-Reroute
00:37:15: RSVP:version:1 flags:0001 type:Path cksum:D61E ttl:255 reserved:0 length:216
00:37:15: MESSAGE_ID type 1 length 12:
00:37:15: ID:0x26 Epoch:0x76798A
00:37:15: Flags:ACK_DESIRED
00:37:15: SESSION type 7 length 16:
00:37:15: Destination 140.75.1.1, TunnelId 100, Source 140.20.1.1, Protocol 0, Flags 0000
00:37:15: HOP type 1 length 12:
00:37:15: Neighbor 140.4.4.1, LIH 0x10000401
00:37:15: TIME_VALUES type 1 length 8:
00:37:15: Refresh period is 30000 msecs
00:37:15: EXPLICIT_ROUTE type 1 length 28:
00:37:15: IPv4 Prefix, 8 bytes, 140.4.4.2/32
00:37:15: (2) Strict IPv4 Prefix, 8 bytes, 140.70.1.1/32
00:37:15: (3) Strict IPv4 Prefix, 8 bytes, 140.70.1.2/32
00:37:15: LABEL_REQUEST type 1 length 8:
00:37:15: Layer 3 protocol ID:2048
00:37:15: SESSION_ATTRIBUTE type 7 length 28:
00:37:15: Session name:tagsw4500-21_t100
00:37:15: Setup priority?:7, reservation priority?:
00:37:15: Status:May-Reroute
00:37:15: SENDER_TEMPLATE type 7 length 12:
00:37:15: Source 140.20.1.1, tunnel_id 9
00:37:15: SENDER_TSPEC type 2 length 36:
00:37:15: version=0, length in words=7
00:37:15: Token bucket fragment (service_id=1, length=6 words
00:37:15: parameter id=127, flags=0, parameter length=5
00:37:15: average rate=1250 bytes/sec, burst depth=1000 bytes
00:37:15: peak rate =-1250 bytes/sec
00:37:15: min unit=0 bytes, max pkt size=4294967295 bytes
00:37:15: ADSPEC type 2 length 48:
00:37:15: version=0 length in words=10
00:37:15: General Parameters break bit=0 service length=8
00:37:15: IS Hops:1
00:37:15: Minimum Path Bandwidth (bytes/sec):1250000
00:37:15: Path Latency (microseconds):0
00:37:15: Path MTU:1500
00:37:15: Controlled Load Service  break bit=0  service length=0
00:37:15: RSVP:version:1 flags:0001 type:Resv cksum:DADF ttl:255 reserved:0 length:132
00:37:15: MESSAGE_ID_ACK type 1 length 12:
00:37:15: Type:ACK
00:37:15: ID:0x26 Epoch:0x76798A
00:37:15: Flags:None
00:37:15: MESSAGE_ID type 1 length 12:
00:37:15: ID:0x43 Epoch:0xE1A1B7
00:37:15: Flags:ACK_DESIRED
00:37:15: SESSION type 7 length 16:
00:37:15: Destination 140.75.1.1, TunnelId 100, Source 140.20.1.1, Protocol 0, Flags 0000
00:37:15: RSVP:version:1 flags:0001 type:Ack cksum:34F5 ttl:255 reserved:0 length:20
00:37:15: MESSAGE_ID_ACK type 1 length 12:
00:37:15: Type:ACK
00:37:15: ID:0x43 Epoch:0xE1A1B7
00:37:15: Flags:None
00:37:15: HOP type 1 length 12:
00:37:15: Neighbor 140.4.4.2, LIH 0x10000401
00:37:15: TIME_VALUES type 1 length 8 :
00:37:15: Refresh period is 30000 msecs
00:37:15: STYLE type 1 length 8 :
00:37:15: Shared-Explicit (SE)
00:37:15: FLOWSPEC type 2 length 36:
00:37:15: version = 0 length in words = 7
00:37:15: service id = 5, service length = 6
00:37:15: tspec parameter id = 127, flags = 0, length = 5
00:37:15: average rate = 1250 bytes/sec, burst depth = 1000 bytes
00:37:15: peak rate = 1250 bytes/sec
00:37:15: min unit = 0 bytes, max pkt size = 0 bytes
00:37:15: FILTER_SPEC type 7 length 12:
00:37:15: Source 140.20.1.1, tunnel_id 9
00:37:15: LABEL type 1 length 8 :
00:37:15: Labels:16
00:37:15: HOP type 1 length 12:
00:37:15: Neighbor 140.4.4.2, LIH 0x10000401
00:37:15: TIME_VALUES type 1 length 8 :
00:37:15: Refresh period is 30000 msecs
00:37:15: STYLE type 1 length 8 :
00:37:15: Shared-Explicit (SE)
00:37:15: FLOWSPEC type 2 length 36:
00:37:15: version = 0 length in words = 7
00:37:15: service id = 5, service length = 6
00:37:15: tspec parameter id = 127, flags = 0, length = 5
00:37:15: average rate = 1250 bytes/sec, burst depth = 1000 bytes
00:37:15: peak rate = 1250 bytes/sec
00:37:15: min unit = 0 bytes, max pkt size = 0 bytes
00:37:15: FILTER_SPEC type 7 length 12:
00:37:15: Source 140.20.1.1, tunnel_id 9
00:37:15: LABEL type 1 length 8 :
00:37:15: Labels:16
00:37:15: %LINK-3-UPDOWN:Interface Tunnel100, changed state to up
00:37:18:%LINEPROTO-5-UPDOWN:Line protocol on Interface Tunnel100, changed state to up

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip rsvp signalling refresh reduction</td>
<td>Enables refresh reduction.</td>
</tr>
<tr>
<td>show debug</td>
<td>Displays active debug output.</td>
</tr>
</tbody>
</table>
**debug ip rsvp errors**

To display informational debugging messages and messages about irregular events, use the `debug ip rsvp errors` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip rsvp errors
no debug ip rsvp errors
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(29)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(29)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ip rsvp errors` command to display informational messages and messages about irregular events such as an incomplete setup or breakdown of an RSVP session. Informational messages do not necessarily indicate problems. It is useful to use this command if something has gone wrong, but you do not know what.

If you enter a different debug command, such as `debug ip rsvp signalling`, all the signalling errors and the normal signalling events are displayed. You do not have to also enter the `debug ip rsvp errors` command.

If there are many active RSVP sessions, enter the following configuration command to activate ACL filtering so that you will view only relevant debugging messages.

```
Router(config)# access-list
    number
    permit
    udp
    src_ip
    src_port
    dst_ip
    dst_port
```

Where

- `number` -- Access list number, from 100 to 199
- `src_ip` -- The tunnel headend
- `src_port` -- The link-state packet (LSP) ID
- `dst_ip` -- The tunnel tailend
- `dst_port` -- The tunnel ID, where the tunnel ID is the tunnel interface number
Then enter the following command to turn on ACL filtering:

```bash
Router# debug ip rsvp filter
```

In the following example, debugging is allowed only when the session is initiated from 192.168.1.4 toward 192.168.1.8, for Tunnel8 on the headend.

```
Note
This ACL will capture both PATH and RESV messages for the session from 192.168.1.4 to 192.168.1.8, but not any tunnels originating from 1.8 going to 1.4. You can also specify the LSP ID, but that is less useful because it changes all the time, and the combination of the head, tail, and tunnel ID is generally enough to limit the output to what you want.
```

```bash
Router(config)# access-list 101 permit udp host 192.168.1.4 host 192.168.1.8 eq 8
Router# debug ip rsvp filter
```

### Examples

The following is sample output from the `debug ip rsvp errors` command:

```bash
Router# debug ip rsvp errors

*May 21 08:54:31.918: RSVP: 5.1.1.1_68->7.1.1.1_3[5.1.1.1]: Problem parsing PATH message: MISFORMATTED object (13) C-Type (2)
```
**debug ip rsvp hello**

To verify that a Hello instance has been created, that a Hello instance has been deleted, or that communication with a neighbor has been lost, use the `debug ip rsvp hello` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip rsvp hello [client] [detail] [messages] [stats]
o no debug ip rsvp hello [client] [detail] [messages] [stats]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>client</th>
<th>(Optional) Indicates whether clients are enabled or disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>detail</td>
<td>(Optional) Indicates whether detailed output is enabled or disabled.</td>
</tr>
<tr>
<td></td>
<td>messages</td>
<td>(Optional) Indicates whether messages are enabled or disabled.</td>
</tr>
<tr>
<td></td>
<td>stats</td>
<td>(Optional) Indicates whether statistics are enabled or disabled.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging activity for the Hello instance or communication with a neighbor does not occur.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(22)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)SXD1</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXD1.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you enter the `debug ip rsvp hello` command, Resource Reservation Protocol (RSVP) signaling messages are shown, but RSVP hello messages are excluded because of the large number of hello messages that are sent.

**Examples**

Following is sample output from the `debug ip rsvp hello` command. The first portion of the output is for serial interface 2/0 when Hello is created.

```
Router# debug ip rsvp hello
00:22:03: RSVP-HELLO: rsvp_hello_inst_init: Initializing ACTIVE hello inst 10.0.0.2->10.0.0.3
00:22:03: RSVP-HELLO: rsvp_hello_create_instance_from_psb: Next hop Se2/0 is adjacent
00:22:03: RSVP-HELLO: rsvp_hello_create_instance_from_psb: Create hello instance for 10.0.0.2->10.0.0.3 on Se2/0 (psb=61BC5F60)
00:22:03: RSVP-HELLO: rsvp_hello_find_instance: psb_cnt=2 for hello inst 10.0.0.2->10.0.0.3
00:22:03: RSVP-HELLO: rsvp_hello_incoming_message: Neighbor 10.0.0.3 state changed to UP
00:22:05: %LINK-3-UPDOWN: Interface Tunnel1, changed state to up
00:22:06: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
Router(config-if)#
```
Router(config-if)# **shut**

The following output shows that Hello has been deleted:

00:25:19: RSVP-HELLO: rsvp_hello_path_delete: psb for hello inst 10.0.0.2->10.0.0.3 exited READY state (psb_cnt=1)
00:25:19: RSVP-HELLO: rsvp_hello_path_delete: psb for hello inst 10.0.0.2->10.0.0.3 exited READY state (psb_cnt=0)
00:25:19: RSVP-HELLO: rsvp_hello_path_delete: Last psb deleted, hello inst for 10.0.0.2->10.0.0.3 ACTIVE->PASSIVE
00:25:19: RSVP-HELLO: rsvp_hello_path_delete: psb for hello inst 10.0.0.2->10.0.0.3 exited READY state (psb_cnt=0)
00:25:19: RSVP-HELLO: rsvp_hello_path_delete: Last psb deleted, hello inst for 10.0.0.2->10.0.0.3 ACTIVE->PASSIVE
00:25:21: %LINK-5-CHANGED: Interface Tunnel1, changed state to administratively down
00:25:22: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
00:05:51: RSVP-HELLO: Communication lost with 10.0.0.2
00:05:51: RSVP-HELLO: rsvp_hello_communication_lost: Neighbor 10.0.0.2 was reset (src_inst)

Following is sample output from the **debug ip rsvp hello stats** command:

Router(config)# debug **ip rsvp hello stats**
Router#
00:32:28: RSVP-HELLO: rsvp_hello_stats_init: Hello stats is being configured

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip rsvp signalling hello (configuration)</strong></td>
<td>Enables Hello globally on the router.</td>
<td></td>
</tr>
<tr>
<td><strong>ip rsvp signalling hello dscp</strong></td>
<td>Sets the DSCP value that is in the IP header of the Hello message sent out from an interface.</td>
<td></td>
</tr>
<tr>
<td><strong>ip rsvp signalling hello (interface)</strong></td>
<td>Enables Hello on an interface where you need Fast Reroute protection.</td>
<td></td>
</tr>
<tr>
<td><strong>ip rsvp signalling hello refresh interval</strong></td>
<td>Configures the Hello request interval.</td>
<td></td>
</tr>
<tr>
<td><strong>ip rsvp signalling hello refresh misses</strong></td>
<td>Specifies how many Hello acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down.</td>
<td></td>
</tr>
<tr>
<td><strong>ip rsvp signalling hello statistics</strong></td>
<td>Enables Hello statistics on the router.</td>
<td></td>
</tr>
</tbody>
</table>
debug ip rsvp high-availability

To display debugging output for Resource Reservation Protocol traffic engineering (RSVP-TE) high availability (HA) activities that improve the accessibility of network resources, use the **debug ip rsvp high-availability** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip rsvp high-availability {all | database | errors | events | fsm | issu | messages}
no debug ip rsvp high-availability {all | database | errors | events | fsm | issu | messages}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>all</strong></td>
<td>Displays debugging output for all RSVP-TE HA categories except for the dumping of messages.</td>
</tr>
<tr>
<td><strong>database</strong></td>
<td>Displays information about read and write operations to and from the checkpointed database during the RSVP-TE HA activities.</td>
</tr>
<tr>
<td><strong>errors</strong></td>
<td>Displays errors encountered by RSVP-TE during HA activities.</td>
</tr>
</tbody>
</table>
| **events** | Displays significant RSVP-TE stateful switchover (SSO) events during RSVP-TE HA activities, such as:  
  - RSVP-TE process events  
  - RSVP-TE Route Processor (RP) state (active, standby, and recovery) changes  
  - Recovery period beginning and end  
  - Redundant Facility (RF) events handled by RSVP-TE |
| **fsm**  | Displays significant events for the RSVP-TE checkpointed database finite state machine (fsm) during the RSVP-TE HA activities. |
| **issu** | Displays information about RSVP-TE In-Service Software Upgrade (ISSU) activity. |
| **messages** | Displays information about Checkpointing Facility (CF) messages sent by RSVP-TE between the active RP and the standby RP. |

### Command Default

Debugging is not enabled.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>Support for ISSU was added.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command displays information about RSVP-TE activities, before and after SSO, that improve the availability of network resources and services.
The following example is sample output from the `debug ip rsvp high-availability all` command, which turns on debugging for IP RSVP-TE HA events, messages, database, errors, fsm, and ISSU:

```
Router# debug ip rsvp high-availability all
RSVP HA all debugging is on
Router# show debug  ---- This command displays the debugging that is enabled.
IP RSVP HA debugging is on for:
   events  
   messages 
   database  
   errors    
   fsm       
   issu

This sample debugging output is displayed as an SSO recovery begins on the standby router in the process of the standby router becoming active.

The prefix in the debug output is composed of label switched path (LSP) 5-tuples in the following format: 10.0.0.3_61->10.0.0.9_10[10.0.0.3]. The 10.0.0.3 represents the source address, the 61 represents the LSP ID, the 10.0.0.9 represents the tunnel destination (tunnel tail), the 10 represents the tunnel ID, and the [10.0.0.3] represents the extended tunnel ID.

```

*May 12 19:46:14.267: RSVP-HA: session 65.39.97.4_18698[0.0.0.0]:rsvp_ha_read_lsp_head_info: Read LSP Head info: tun_id: 10
*May 12 19:46:14.267: RSVP-HA: session 10.0.0.1_10[0.0.0.0]: rsvp_ha_db_entry_find: lsp_head
*May 12 19:46:14.267: RSVP-HA: session 10.221.123.48_10[0.0.0.0]: rsvp_ha_db_entry_find: lsp_head entry found
*May 12 19:46:14.267: RSVP-HA: session 10.0.0.9_10[0.0.0.0]: rsvp_ha_db_entry_find: lsp_head entry not found
*May 12 19:46:14.267: RSVP-HA: session 10.0.0.9_10[0.0.0.0]: rsvp_ha_db_wavl_entry_insert: Inserted entry into lsp_head Write DB, Send_Pending tree
*May 12 19:46:14.267: RSVP-HA: session 10.0.0.9_10[0.0.0.0]: rsvp_ha_fsm_wr_event_add_entry: add lsp_head entry to Write DB
*May 12 19:46:14.267: RSVP-HA: session 10.0.0.9_10[0.0.0.0]: rsvp_ha_write_generic_info: Writing lsp info
```

Cisco IOS Debug Command Reference - Commands I through L
Created lsp entry
*May 12 19:46:20.807: RSVP-HA:10.0.0.3_61->10.0.0.9_10[10.0.0.3]:
  rsvp_ha_set_entry_state: None -> Send-Pending
*May 12 19:46:20.807: RSVP-HA: 10.0.0.3_61->10.0.0.9_10[10.0.0.3]:
  rsvp_ha_db_wavl_entry_insert: Inserted entry into lsp Write DB, Send_Pending tree
*May 12 19:46:20.807: RSVP-HA: 10.0.0.3_61->10.0.0.9_10[10.0.0.3]:
  rsvp_ha_fsm_wr_event_add_entry: add lsp entry to Write DB
*May 12 19:46:20.807: RSVP-HA: session 10.27.90.140_10[0.0.0.0]:
  rsvp_ha_db_entry_find: lsp_head entry found
*May 12 19:46:20.807: RSVP-HA: session 10.0.0.9_10[0.0.0.0]: rsvp_ha_db_wavl_entry_remove:
  Removed entry from lsp_head Read DB, Checkpointed tree
*May 12 19:46:20.807: RSVP-HA: session 10.0.0.9_10[0.0.0.0]: rsvp_ha_db_entry_free: Freeing
  lsp_head entry
*May 12 19:46:20.807: RSVP-HA: session 10.0.0.9_10[0.0.0.0]:rsvp_ha_set_entry_state:
  Checkpointed -> None
.
.
.

The following example shows how to turn debugging off for this command:

Router# no debug ip rsvp high-availability all
RSVP HA all debugging is off

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>debug ip rsvp sso</strong></td>
<td>Displays debugging output for RSVP signalling when the graceful restart feature is configured.</td>
</tr>
<tr>
<td><strong>debug mpls traffic-eng ha sso</strong></td>
<td>Displays debugging output for MPLS traffic engineering HA activities during the graceful switchover from an active RP to a redundant standby RP.</td>
</tr>
</tbody>
</table>
debug ip rsvp p2mp

To display status messages for Resource Reservation Protocol (RSVP) point-to-multipoint (P2MP) events, use the **debug ip rsvp p2mp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```bash
debug ip rsvp p2mp
no debug ip rsvp p2mp
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRE</td>
<td>This command was introduced. For P2MP traffic engineering tunnels, the output displays the status of the sublabel switched paths (sub-LSPs).</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the P2MP tunnel is not up, issue this command and the **debug ip rsvp signalling** command and examine the output to determine if there is a problem with the configuration.

Use this command with a small number of tunnels or RSVP reservations or use the RSVP debug message filter to limit the amount of data. Too much data can overload the CPU.

**Examples**

The following example shows status messages as a P2MP sub-LSP is signaled:

```bash
Router# debug ip rsvp p2mp
RSVP p2mp debugging is on
IP RSVP debugging is on for:
  p2mp
Router (config)# interface tunnel100
Router (config-if)# no shutdown
06:56:21: RSVP: 10.1.0.1_134[Src/1]->10.2.0.1_100[Src] {13}: First Sub-LSP, accept Path.
06:56:21: RSVP: 10.1.0.1_134[Src/2]->10.3.0.1_100[Src] {13}: Sibling Sub-LSP received with consistent signalling attributes, accept Path
06:56:21: RSVP: 10.1.0.1_134[Src/3]->10.4.0.1_100[Src] {13}: Sibling Sub-LSP received with consistent signalling attributes, accept Path
06:56:22: RSVP: 10.1.0.1_134[Src/1]->10.2.0.1_100[Src] {13}: First Sub-LSP, accept Resv.
06:56:22: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1100, changed state to up
06:56:22: RSVP: 10.1.0.1_134[Src/3]->10.4.0.1_100[Src] {13}: Sibling Sub-LSP received with consistent signalling attributes, accept Resv
06:56:22: RSVP: 10.1.0.1_134[Src/2]->10.3.0.1_100[Src] {13}: Sibling Sub-LSP received with consistent signalling attributes, accept Resv
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip rsvp signalling</td>
<td>Displays RSVP signalling (PATH and RESV) messages.</td>
</tr>
<tr>
<td>show ip rsvp reservation</td>
<td>Displays RSVP PATH-related receiver information currently in the database.</td>
</tr>
<tr>
<td>show ip rsvp sender</td>
<td>Displays RSVP RESV-related receiver information currently in the database.</td>
</tr>
</tbody>
</table>
### debug ip rsvp policy

To display debugging messages for Resource Reservation Protocol (RSVP) policy processing, use the `debug ip rsvp policy` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging for RSVP policy processing is not enabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(23)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(23)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You might find it useful to enable the `debug cops` command when you are using the `debug ip rsvp policy` command. Together, these commands generate a complete record of the policy process.

**Examples**

The following example uses only the `debug ip rsvp policy` command:

```
Router-1# debug ip rsvp policy
RSVP_POLICY debugging is on
02:02:14:RSVP-POLICY:Creating outbound policy IDB entry for Ethernet2/0 (61E6AB38)
02:02:14:RSVP-COPS:COPS query for Path message, 10.31.0.1_44->10.33.0.1_44
02:02:14:RSVP-POLICY:Building incoming Path context
02:02:14:RSVP-POLICY:Building outgoing Path context on Ethernet2/0
02:02:14:RSVP-POLICY:Build REQ message of 216 bytes
02:02:14:RSVP-POLICY:Message sent to PDP
02:02:14:RSVP-COPS:COPS engine called us with reason 2, handle 6202A658
02:02:14:RSVP-COPS:Received decision message
02:02:14:RSVP-POLICY:Accept incoming message
02:02:14:RSVP-POLICY:Send outgoing message to Ethernet2/0
02:02:14:RSVP-POLICY:Replacement policy object for path-in context
02:02:14:RSVP-POLICY:Replacement TSPEC object for path-in context
02:02:14:RSVP-COPS:COPS report for Path message, 10.31.0.1_44->10.33.0.1_44
02:02:14:RSVP-POLICY:Report sent to PDP
02:02:14:RSVP-COPS:COPS report for Path message, 10.31.0.1_44->10.33.0.1_44
```

The following example uses both the `debug ip rsvp policy` and the `debug cops` commands:

```
Router-1# debug ip rsvp policy
RSVP_POLICY debugging is on
Router-1# debug cops
```
COPS debugging is on
02:15:14:RSVP-POLICY:Creating outbound policy IDB entry for Ethernet2/0 (61E6AB38)
02:15:14:RSVP-COPS:COPS query for Path message, 10.31.0.1_44->10.33.0.1_44
02:15:14:RSVP-POLICY:Building incoming Path context
02:15:14:RSVP-POLICY:Building outgoing Path context on Ethernet2/0
02:15:14:RSVP-POLICY:Build REQ message of 216 bytes
02:15:14:COPS:** SENDING MESSAGE **
COPS HEADER:Version 1, Flags 0, Opcode 1 (REQ), Client-type:1, Length:216
HANDLE (1/1) object. Length:8. 00 00 22 01
CONTEXT (2/1) object. Length:8. R-type:5, M-type:1
IN_IF (3/1) object. Length:12. Address:10.1.2.1, If_index:4
OUT_IF (4/1) object. Length:12. Address:10.33.0.1, If_index:3
CLIENT SI (9/1) object. Length:168. CSI data:
02:15:14: SESSION type 1 length 12:
02:15:14: Destination 10.33.0.1, Protocol_Id 17, Don't Police, DstPort 44
02:15:14: HOP type 1 length 12: 0A010201
02:15:14: TIME_VALUES type 1 length 8: 00007530
02:15:14: SENDER_TEMPLATE type 1 length 12:
02:15:14: Source 10.31.0.1, udp_source_port 44
02:15:14: SENDER_TSPEC type 2 length 36:
02:15:14: version=0, length in words=7
02:15:14: Token bucket fragment (service_id=1, length=6 words
02:15:14: parameter id=127, flags=0, parameter length=5
02:15:14: average rate=1250 bytes/sec, burst depth=10000 bytes
02:15:14: peak rate =1250000 bytes/sec
02:15:14: min unit=0 bytes, max unit=1514 bytes
02:15:14: ADSPEC type 2 length 84:
02:15:14: version=0 length in words=19
02:15:14: General Parameters break bit=0 service length=8
02:15:14: IS Hops:1
02:15:14: Minimum Path Bandwidth (bytes/sec):1250000
02:15:14: Path Latency (microseconds):0
02:15:14: Path MTU:1500
02:15:14: Guaranteed Service break bit=0 service length=8
02:15:14: Path Delay (microseconds):192000
02:15:14: Path Jitter (microseconds):1200
02:15:14: Path delay since shaping (microseconds):192000
02:15:14: Path Jitter since shaping (microseconds):1200
02:15:14: Controlled Load Service break bit=0 service length=0
02:15:14: COPS:Sent 216 bytes on socket,
02:15:14: RSVP-POLICY:Message sent to PDP
02:15:14: COPS:Received decision message
02:15:14: RSVP-POLICY:Received decision for Path message
02:15:14: RSVP-POLICY:Accept incoming message
02:15:14: RSVP-POLICY:Send outgoing message to Ethernet2/0
02:15:14:COPS:Sent 216 bytes on socket,
02:15:14:RSVP-POLICY:Message sent to PDP
02:15:14:COPS:Message event!
02:15:14:COPS:State of TCP is 4
02:15:14: COPS:Read block of 96 bytes, num-104 (len-104)
02:15:14:COPS:** RECEIVED MESSAGE **
COPS HEADER:Version 1, Flags 1, Opcode 2 (DEC), Client-type:1, Length:104
HANDLE (1/1) object. Length:8. 00 00 22 01
CONTEXT (2/1) object. Length:8. R-type:1, M-type:1
DECISION (6/1) object. Length:8. COMMAND cmd:1, flags:0
DECISION (6/3) object. Length:56. REPLACEMENT 00 10 0E 01 61 60 6A 6B 6C 00 24 0C 02 00
00 00 07 01 00 00 06 7F 00 00 05 44 9C 40 00 46 1C 40 00 49 98
96 10 00 00 00 08 00 00 01 C8
CONTEXT (2/1) object. Length:8. R-type:4, M-type:1
DECISION (6/1) object. Length:8. COMMAND cmd:1, flags:0
02:15:14:Notifying client (callback code 2)
02:15:14:RSVP-COPS:COPS engine called us with reason 2, handle 6202A104
02:15:14:RSVP-COPS:Received decision message
02:15:14:RSVP-POLICY:Received decision for Path message
02:15:14:RSVP-POLICY:Accept incoming message
02:15:14:RSVP-POLICY:Send outgoing message to Ethernet2/0
02:15:14:RSVP-POLICY:Replacement policy object for path-in context
02:15:14:RSVP-POLICY: Replacement TSPEC object for path-in context
02:15:14:RSVP-COPS: COPS report for Path message, 10.31.0.1_44->10.33.0.1_44
02:15:14:COPS: ** SENDING MESSAGE **
   COPS HEADER: Version 1, Flags 1, Opcode 3 (RPT), Client-type: 1, Length: 24
   HANDLE (1/1) object. Length: 8. 00 00 22 01
   REPORT (12/1) object. Length: 8. REPORT type COMMIT (1)
02:15:14:COPS: Sent 24 bytes on socket,
02:15:14:RSVP-POLICY: Report sent to PDP
02:15:14:Timer for connection entry is zero
02:15:14:RSVP-COPS: COPS report for Path message, 10.31.0.1_44->10.33.0.1_44

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug cops</td>
<td>Displays debugging messages for COPS processing.</td>
</tr>
</tbody>
</table>
debug ip rsvp rate-limit

To display debugging messages for Resource Reservation Protocol (RSVP) rate-limiting events, use the `debug ip rsvp rate-limit` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
default ip rsvp rate-limit
no debug ip rsvp rate-limit
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(24)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(24)S.</td>
</tr>
</tbody>
</table>

**Examples**

The following command shows how to enable debugging for RSVP rate-limiting and message manager events:

```
Router# debug ip rsvp rate-limit
RSVP rate-limit debugging is on
Router# debug ip rsvp msg-mgr
RSVP msg-mgr debugging is on
```

In the following display, RSVP process information including messages, timers, neighbors IP addresses, and message IDs, appear:

```
01:00:19:RSVP-RATE-LIMIT:rsvp_msg_pacing_send_message
01:00:19:RSVP-MSG-MGR (140.4.4.2):Starting timer msg-pacing interval 20
01:00:19:RSVP-MSG-MGR (140.4.4.2):Enqueue element 27000405 of type 3 on msg-pacing TAIL
01:00:19:RSVP-RATE-LIMIT:rsvp_msg_pacing_timer - timer expired
01:00:19:RSVP-MSG-MGR (140.4.4.2):Dequeueing element 27000405 of type 3 from msg-pacing
01:00:19:RSVP-RATE-LIMIT:rsvp_msg_pacing_send_qe:sending psb (qe 27000405)
01:00:21:%LINK-3-UPDOWN:Interface Tunnel100, changed state to up
01:00:22:%LINEPROTO-5-UPDOWN:Line protocol on Interface Tunnel100, changed state to up
01:01:03:RSVP-RATE-LIMIT:rsvp_msg_pacing_send_message
01:01:03:RSVP-MSG-MGR (140.4.4.2):Starting timer msg-pacing interval 20
01:01:03:RSVP-MSG-MGR (140.4.4.2):Enqueue element 27000405 of type 3 on msg-pacing TAIL
01:01:03:RSVP-RATE-LIMIT:rsvp_msg_pacing_timer - timer expired
01:01:03:RSVP-MSG-MGR (140.4.4.2):Dequeueing element 27000405 of type 3 from msg-pacing
01:01:03:RSVP-RATE-LIMIT:rsvp_msg_pacing_send_qe:sending psb (qe 27000405)
01:01:42:RSVP-RATE-LIMIT:rsvp_msg_pacing_send_message
01:01:42:RSVP-MSG-MGR (140.4.4.2):Starting timer msg-pacing interval 20
01:01:42:RSVP-MSG-MGR (140.4.4.2):Enqueue element 27000405 of type 3 on msg-pacing TAIL
01:01:42:RSVP-RATE-LIMIT:rsvp_msg_pacing_timer - timer expired
01:01:42:RSVP-MSG-MGR (140.4.4.2):Dequeueing element 27000405 of type 3 from msg-pacing
01:01:42:RSVP-RATE-LIMIT:rsvp_msg_pacing_send_qe:sending psb (qe 27000405)
```
01:02:09:RSVP-RATE-LIMIT:rsvp_msg_pacing_send_message
01:02:09:RSVP-MSG-MGR (140.4.4.2):Starting timer msg-pacing interval 20
01:02:09:RSVP-MSG-MGR (140.4.4.2):Enqueue element 27000405 of type 3 on msg-pacing TAIL
01:02:09:RSVP-RATE-LIMIT:rsvp_msg_pacing_timer - timer expired
01:02:09:RSVP-MSG-MGR (140.4.4.2):Dequeueing element 27000405 of type 3 from msg-pacing
01:02:09:RSVP-RATE-LIMIT:rsvp_msg_pacing_send_qe:sending psb (qe 27000405)

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip rsvp signalling rate-limit</td>
<td>Controls the transmission rate for RSVP messages sent to a neighboring router during a specified interval.</td>
</tr>
<tr>
<td>show debug</td>
<td>Displays active debug output.</td>
</tr>
</tbody>
</table>
debug ip rsvp reliable-msg

To display debugging messages for Resource Reservation Protocol (RSVP) reliable messages events, use the `debug ip rsvp reliable-msg` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
deploy ip rsvp reliable-msg
no debug ip rsvp reliable-msg
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(24)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(24)S.</td>
</tr>
</tbody>
</table>

**Examples**

The following command shows how to enable debugging for RSVP reliable messages events:

```
Router# debug ip rsvp reliable-msg
RSVP reliable-msg debugging is on
```

In the following display, message IDs, acknowledgments (ACKs), and message processes including retransmissions, appear:

```
01:07:37:RSVP-RMSG:Inserted msg id(0x46, 0x48000403) on local msgid db
01:07:37:RSVP-RMSG:rsvp_rmsg_process_acks, Handle:000C1701 neighbor:140.4.4.2
01:07:37:RSVP-RMSG:max_ids:1 q_sz:1 msg_sz:1500 ids_len:1432 num_objs:0 obj_len:0
nbr:140.4.4.2
01:07:39:%LINK-3-UPDOWN:Interface Tunnel100, changed state to up
01:07:40:%LINEPROTO-5-UPDOWN:Line protocol on Interface Tunnel100, changed state to up
01:08:07:RSVP-RMSG:rsvp_rmsg_process_acks, Handle:000C1701 neighbor:140.4.4.2
01:08:07:RSVP-RMSG:max_ids:1 q_sz:1 msg_sz:1500 ids_len:1432 num_objs:0 obj_len:0
nbr:140.4.4.2
01:08:37:RSVP-RMSG:max_ids:1 q_sz:1 msg_sz:1500 ids_len:1424 num_objs:1 obj_len:8
nbr:140.4.4.2
01:08:37:RSVP-RMSG:rsvp_rmsg_process_immediate_tmb, Handle:2D000404 neighbor:140.4.4.2
01:08:37:RSVP-RMSG:Inserted msg id(0x47, 0x2D000404) on local msgid db
01:08:37:RSVP-RMSG:current queue:immed next_queue:rxmt-1 (qe 2D000404s)
01:08:37:RSVP-RMSG:rsvp_rmsg_process_acks, Handle:000C1701 neighbor:140.4.4.2
01:08:37:RSVP-RMSG:max_ids:1 q_sz:1 msg_sz:1500 ids_len:1432 num_objs:0 obj_len:0
nbr:140.4.4.2
01:08:37:RSVP-RMSG:rsvp_rmsg_process_immediate_tmb, Handle:2E000404 neighbor:140.4.4.2
01:08:37:RSVP-RMSG:Inserted msg id(0x48, 0x2E000404) on local msgid db
01:08:37:RSVP-RMSG:current queue:immed next_queue:rxmt-1 (qe 2E000404s)
```
01:09:07:RSVP-RMSG:rsvp_rmsg_process_acks, Handle:000C1701 neighbor:140.4.4.2
01:09:07:RSVP-RMSG:max_ids:1 q_sz:1 mag_sz:1500 ids_len:1432 num_objs:0 obj_len:0
nbr:140.4.4.2
01:09:08:RSVP-RMSG:rsvp_rmsg_process_rxmt_tmb, Handle:2E000404 neighbor:140.4.4.2
01:09:08:RSVP-RMSG:An ack was received for tmb 2E000404 on neighbor 140.4.4.2
01:09:37:RSVP-RMSG:max_ids:1 q_sz:1 mag_sz:1500 ids_len:1424 num_objs:1 obj_len:8
nbr:140.4.4.2
01:09:37:RSVP-RMSG:rsvp_rmsg_process_acks, Handle:000C1701 neighbor:140.4.4.2
01:09:37:RSVP-RMSG:max_ids:1 q_sz:1 mag_sz:1500 ids_len:1432 num_objs:0 obj_len:0
nbr:140.4.4.2
01:09:38:RSVP-RMSG:rsvp_rmsg_process_rxmt_tmb, Handle:2F000404 neighbor:140.4.4.2
01:09:38:RSVP-RMSG:An ack was received for tmb 2F000404 on neighbor 140.4.4.2

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip rsvp signalling refresh reduction</td>
<td>Enables refresh reduction.</td>
</tr>
<tr>
<td>show debug</td>
<td>Displays active debug output.</td>
</tr>
</tbody>
</table>
debug ip rsvp sbm

To display detailed information about Subnetwork Bandwidth Manager (SBM) messages only, and SBM and Designated Subnetwork Bandwidth Manager (DSBM) state transitions, use the `debug ip rsvp sbm` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip rsvp sbm
no debug ip rsvp sbm
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ip rsvp sbm` command provides information about messages received, minimal detail about the content of these messages, and information about state transitions.

**Examples**

The following example shows the detailed debug information about SBM and the SBM and DSBM state transitions that is available when you enable debug mode through the `debug ip rsvp sbm` command:

```
Router# debug ip rsvp sbm
RSVP debugging is on
router2#
*Dec 31 16:45:34.659: RSVP: send I_AM_DSBM message from 145.2.2.150
*Dec 31 16:45:34.659: RSVP: IP to 224.0.0.17 length=88 checksum=9385 (Ethernet2)
*Dec 31 16:45:34.659: RSVP: version:1 flags:0000 type:I_AM_DSBM cksum:9385
  ttl:254 reserved:0 length:88
  DSBM_IP_ADDR type 1 length 8 : 91020296
  HOP_L2 type 1 length 12: 00E01ECE
  : 0F760000
  DSBM_PRIORITY type 1 length 8 : 0029B064
  DSBM_TIMERS type 1 length 8 : 00000F05
  SBM_INFO type 1 length 44: 00000000
  : 00240C02 00000007
  : 01000006 7F000005
  : 00000000 00000000
  : 00000000 00000000
  : 00000000
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip rsvp</td>
<td>Displays information about SBM message processing, the DSBM election process, and RSVP message processing.</td>
</tr>
<tr>
<td>debug ip rsvp authentication</td>
<td>Displays detailed information about RSVP and SBM.</td>
</tr>
<tr>
<td>ip rsvp dsbm-candidate</td>
<td>Configures an interface as a DSBM candidate.</td>
</tr>
</tbody>
</table>
debug ip rsvp sso

To display debugging output for Resource Reservation Protocol (RSVP) signaling when the graceful restart feature is configured, use the `debug ip rsvp sso` command in privileged EXEC mode. To disable debugging, use the `no` form of this command.

```
debup ip rsvp sso
no debug ip rsvp sso
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays debugging output from RSVP signaling during and after the Route Processor (RP) stateful switchover when system control and routing protocol execution is transferred from the active RP to the redundant standby RP. The SSO process occurs when the active router becomes unavailable, so that no interruption of network services occurs. The command displays information about the activities that RSVP performs when you configure a graceful restart, such as:

- Writing checkpointing information into the write database when a new traffic engineering (TE) label switched path (LSP) is signaled on the active RP
- Recovering the LSP checkpointed information from the read database after SSO
- Displaying information about LSPs not recovered

**Examples**

The following is sample output from the `debug ip rsvp sso` command that was displayed during a successful SSO on the standby router as it became active:

```
Router# debug ip rsvp sso
RSVP sso debugging is on
Router#
```

**Note**

The prefix in the debug output is composed of LSP 5-tuples in the following format: `10.0.0.3_61->10.0.0.9_10[10.0.0.3]`. The 10.0.0.3 represents the source address, the 61 represents the LSP ID, the 10.0.0.9 represents the tunnel destination (tunnel tail), the 10 represents the tunnel ID, and the [10.0.0.3] represents the extended tunnel ID.
The following example shows how to turn debugging off for this command:

```
Router# no debug ip rsvp sso
RSVP sso debugging is off
```
**debug ip rsvp summary-refresh**

To display debugging messages for Resource Reservation Protocol (RSVP) summary-refresh messages events, use the `debug ip rsvp summary-refresh` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(24)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(24)S.</td>
</tr>
</tbody>
</table>

**Examples**

The following command shows how to enable debugging for RSVP summary-refresh messages events:

```
Router# debug ip rsvp summary-refresh
RSVP summary-refresh debugging is on
```

In the following output, the IP addresses, the interfaces, the types of RSVP messages (Path and Resv), message IDs, and epoch identifiers (for routers) for which RSVP summary-refresh events occur are shown:

```
01:11:00:RSVP-SREFRESH:Incoming message from nbr 140.4.4.2 with epoch:0xE1A1B7 msgid:0x84 on Ethernet1
01:11:00:RSVP-SREFRESH 140.20.1.1_18->140.75.1.1_100[140.20.1.1]:Created msgid 0x84 for nbr 140.4.4.2
01:11:02:%LINK-3-UPDOWN:Interface Tunnel100, changed state to up
01:11:03:%LINEPROTO-5-UPDOWN:Line protocol on Interface Tunnel100, changed state to up
01:11:30:RSVP-SREFRESH:140.20.1.1_18->140.75.1.1_100[140.20.1.1]:Path, ID:0x4C :Start using Srefresh to 140.4.4.2
01:11:31:RSVP-SREFRESH:Incoming message from nbr 140.4.4.2 with epoch:0xE1A1B7 msgid:0x84 on Ethernet1
01:11:31:RSVP-SREFRESH:State exists for nbr:140.4.4.2 epoch:0xE1A1B7 msgid:0x84 on Ethernet1
01:12:00:RSVP-SREFRESH:Preparing to Send Srefresh(es) to 140.4.4.2, 1 IDs Total
01:12:00:RSVP-SREFRESH:Sending 1 IDs in this Srefresh
01:12:00:RSVP-SREFRESH:140.20.1.1_18->140.75.1.1_100[140.20.1.1]:Path, ID:0x4C
01:12:01:RSVP-SREFRESH:Preparing to Send Srefresh(es) to 140.4.4.2 with epoch:0xE1A1B7 msgid:0x86 on Ethernet1
01:12:01:RSVP-SREFRESH:Rec'd 1 IDs in Srefresh from nbr 140.4.4.2 (on Ethernet1), epoch:0xE1A1B7 msgid:0x86
01:12:01:RSVP-SREFRESH:140.20.1.1_18->140.75.1.1_100[140.20.1.1]:Resv, ID:0x84
01:12:30:RSVP-SREFRESH:Preparing to Send Srefresh(es) to 140.4.4.2, 1 IDs Total
01:12:30:RSVP-SREFRESH:Sending 1 IDs in this Srefresh
```
01:12:30:RSVP-SREFRESH:140.20.1.1_18->140.75.1.1_100[140.20.1.1]:Path, ID:0x4C
01:12:31:RSVP-SREFRESH:Incoming message from nbr 140.4.4.2 with epoch:0xE1A1B7 msgid:0x88 on Ethernet1
01:12:31:RSVP-SREFRESH:Rec'd 1 IDs in Srefresh from 140.4.4.2 (on Ethernet1), epoch:0xE1A1B7 msgid:0x88
01:12:31:RSVP-SREFRESH:Preparing to Send Srefresh(es) to 140.4.4.2, 1 IDs Total
01:13:00:RSVP-SREFRESH:Sending 1 IDs in this Srefresh
01:13:00:RSVP-SREFRESH:140.20.1.1_18->140.75.1.1_100[140.20.1.1]:Resv, ID:0x84
01:13:01:RSVP-SREFRESH:Incoming message from nbr 140.4.4.2 with epoch:0xE1A1B7 msgid:0x8A on Ethernet1
01:13:01:RSVP-SREFRESH:Rec'd 1 IDs in Srefresh from 140.4.4.2 (on Ethernet1), epoch:0xE1A1B7 msgid:0x8A
01:13:01:RSVP-SREFRESH:140.20.1.1_18->140.75.1.1_100[140.20.1.1]:Resv, ID:0x84

In the preceding output, notice the message IDs that correspond to Path or Resv state being refreshed. Because the entire message does not have to be transmitted, there is less data and network performance is improved.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip rsvp signalling refresh reduction</code></td>
<td>Enables refresh reduction.</td>
</tr>
<tr>
<td><code>show debug</code></td>
<td>Displays active debug output.</td>
</tr>
</tbody>
</table>
**debug ip rsvp traffic-control**

To display debugging messages for compression-related events, use the `debug ip rsvp traffic-control` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

**debug ip rsvp traffic-control**
**no debug ip rsvp traffic-control**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was modified. The command output was modified to include</td>
</tr>
<tr>
<td></td>
<td>compression-related events.</td>
</tr>
<tr>
<td>12.0(24)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(24)S.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(18)SXF2</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXF2.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 2.6 This command was integrated into Cisco IOS XE Release 2.6.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ip rsvp traffic-control` command to troubleshoot compression-related problems.

**Examples**

The following example from the `debug ip rsvp traffic-control` command shows that compression was successfully predicted:

```
Router# debug ip rsvp traffic-control
RSVP debugging is on
Router# show debugging
00:44:49: RSVP-TC: Attempting to install QoS for rsb 62CC66F0
00:44:49: RSVP-TC: Adding new tcsb 02000406 for rsb 62CC66F0
00:44:49: RSVP-TC: Assigning WFQ QoS (on FR VC 101) to tcsb 02000406
00:44:49: RSVP-TC: Predicted compression for TCSB 2000406:
00:44:49: RSVP-TC: method = rtp 00:44:49: RSVP-TC: context ID = 2
00:44:49: RSVP-TC: factor = 82 percent 00:44:49: RSVP-TC: bytes-saved = 36 bytes
00:44:49: RSVP-TC: Bandwidth check: requested bw=65600 old bw=0
00:44:49: RSVP-TC: RSVP bandwidth is available
00:44:49: RSVP-TC: Consulting policy for tcsb 02000406
00:44:49: RSVP-TC: Policy granted QoS for tcsb 02000406
00:44:49: RSVP-TC: Requesting QoS for tcsb 02000406
00:44:49: RSVP-TC: ( r = 8200 bytes/s M = 164 bytes )
00:44:49: RSVP-TC: b = 328 bytes m = 164 bytes )
```
The following example from the `debug ip rsvp traffic-control` command shows that compression was unsuccessfully predicted because no compression context IDs were available:

```
Router# debug ip rsvp traffic-control
RSVP debugging is on
Router# show debugging
00:10:16:RSVP-TC:Attempting to install QoS for rsb 62CED62C
00:10:16:RSVP-TC:Adding new tcsb 01000421 for rsb 62CED62C
00:10:16:RSVP-TC:Assigning WFQ QoS (on FR VC 101) to tcsb 01000421
00:10:16:RSVP-TC:sender's flow is not rtp compressible for TCSB 1000421
00:10:16: reason: no contexts available
00:10:16:RSVP-TC:sender's flow is not udp compressible for TCSB 1000421
00:10:16: reason: no contexts available
00:10:16:RSVP-TC:Bandwidth check:requested bw=80000 old bw=0
00:10:16:RSVP-TC:RSVP bandwidth is available
00:10:16:RSVP-TC:Consulting policy for tcsb 01000421
00:10:16:RSVP-TC:Policy granted QoS for tcsb 01000421
00:10:16:RSVP-TC:Requesting QoS for tcsb 01000421
00:10:16:RSVP-TC: ( r = 10000 bytes/s M = 200 bytes
00:10:16:RSVP-TC: b = 400 bytes m = 200 bytes )
00:10:16:RSVP-TC: p = 10000 bytes/s Service Level = priority
00:10:16:RSVP-WFQ:Update for tcsb 01000421 on FR PVC dli 101 on Se3/0
00:10:16:RSVP-WFQ:Admitted 80 kbps of bandwidth
00:10:16:RSVP-WFQ:Allocated PRIORITY queue 24
00:10:16:RSVP-TC:Allocation succeeded for tcsb 01000421
```
**debug ip rsvp wfq**

To display debugging messages for the weighted fair queue (WFQ), use the `debug ip rsvp wfq` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
depicomp ip rsvp wfq
no debug ip rsvp wfq
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(3)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(24)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(24)S.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(18)SXF2</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXF2.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.6</td>
<td>This command was integrated into Cisco IOS XE Release 2.6.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip rsvp wfq` command:

```
Router# debug ip rsvp wfq
RSVP debugging is on
Router# show debugging
IP RSVP debugging is on
IP RSVP debugging (Traffic Control events) is on
IP RSVP debugging (WFQ events) is on
Router#
03:03:23:RSVP-TC:Attempting to install QoS for rsb 6268A538
03:03:23:RSVP-TC:Adding new tcsb 00001A01 for rsb 6268A538
03:03:23:RSVP-TC:Assigning WFQ QoS to tcsb 00001A01
03:03:23:RSVP-TC:Consulting policy for tcsb 00001A01
03:03:23:RSVP-TC:Policy granted QoS for tcsb 00001A01
03:03:23:RSVP-TC:Requesting QoS for tcsb 00001A01
03:03:23:RSVP-TC: ( x = 12500 bytes/s M = 1514 bytes )
03:03:23:RSVP-TC: p = 12500 bytes/s Service Level = non-priority
03:03:23:RSVP-WFQ:Requesting a RESERVED queue on Et0/1 for tcsb 00001A01
03:03:23:RSVP-WFQ:Queue 265 allocated for tcsb 00001A01
03:03:23:RSVP-TC:Allocation succeeded for tcsb 00001A01
Router# no debug ip rsvp wfq
RSVP debugging is off
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show debugging</td>
<td>Displays active debugging output.</td>
</tr>
</tbody>
</table>
debug ip rtp header-compression through debug ipv6 icmp

• debug ip rtp header-compression through debug ipv6 icmp, on page 324
debug ip rtp header-compression through debug ipv6 icmp

debug ip rtp header-compression

To display events specific to Real-Time Transport Protocol (RTP) header compression, use the debug ip rtp header-compression command in privileged EXEC mode. To disable debugging output, use the no form of this command.

```
debug ip rtp header-compression
no debug ip rtp header-compression
```

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Examples

The following is sample output from the debug ip rtp header-compression command:

```
Router# debug ip rtp header-compression
RHC BRIO: rcv compressed rtp packet
RHC BRIO: context0: expected sequence 0, received sequence 0
RHC BRIO: rcv compressed rtp packet
RHC BRIO: context0: expected sequence 1, received sequence 1
RHC BRIO: rcv compressed rtp packet
RHC BRIO: context0: expected sequence 2, received sequence 2
RHC BRIO: rcv compressed rtp packet
RHC BRIO: context0: expected sequence 3, received sequence 3
```

The table below describes the significant fields shown in the display.

**Table 51: debug ip rtp header-compression Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>context0</td>
<td>Compression state for a connection 0.</td>
</tr>
<tr>
<td>expected sequence</td>
<td>RTP header compression link sequence (expected).</td>
</tr>
<tr>
<td>received sequence</td>
<td>RTP header compression link sequence (actually received).</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip rtp packets</td>
<td>Displays a detailed dump of packets specific to RTP header compression.</td>
</tr>
</tbody>
</table>

debug ip rtp packets

To display a detailed dump of packets specific to Real-Time Transport Protocol (RTP) header compression, use the debug ip rtp packets command in privileged EXEC mode. To disable debugging output, use the no form of this command.
debug ip rtp packets
no debug ip rtp packets

Syntax Description
This command has no arguments or keywords.

Command Modes
Privileged EXEC

Examples
The following is sample output from the debug ip rtp packets command:

Router# debug ip rtp packets
RTP packet dump:
  IP: source: 171.68.8.10, destination: 224.2.197.169, id: 0x249B, ttl: 9,
      TOS: 0 prot: 17,
  UDP: source port: 1034, destination port: 27404, checksum: 0xB429,len: 152
  RTP: version: 2, padding: 0, extension: 0, marker: 0,
       payload: 3, ssr 2369713968,
       sequence: 2468, timestamp: 85187180, csrc count: 0

The table below describes the significant fields shown in the display.

Table 52: debug ip rtp packets Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>IP identification.</td>
</tr>
<tr>
<td>ttl</td>
<td>IP time to live (TTL).</td>
</tr>
<tr>
<td>len</td>
<td>Total UDP length.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip rtp header-compression</td>
<td>Displays events specific to RTP header compression.</td>
</tr>
</tbody>
</table>

debug ip scp

To troubleshoot secure copy (SCP) authentication problems, use the debug ip scp command in privileged EXEC mode. To disable debugging output, use the no form of this command.

depag ip scp
no debug ip scp

Syntax Description
This command has no arguments or keywords.

Command Modes
Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
This command was integrated into Cisco IOS Release 12.0(21)S.
This command was integrated into Cisco IOS Release 12.2(22)S.
This command was integrated into Cisco IOS Release 12.2(25)S.
This command was integrated into Cisco IOS Release 12.2(18)SXD.

Examples

The following example is output from the `debug ip scp` command. In this example, a copy of the file scptest.cfg from a UNIX host running configuration of the router was successful.

```
Router# debug ip scp
4d06h:SCP:[22 -> 10.11.29.252:1018] send <OK>
4d06h:SCP:[22 <- 10.11.29.252:1018] recv C0644 20 scptest.cfg
4d06h:SCP:[22 -> 10.11.29.252:1018] send <OK>
4d06h:SCP:[22 <- 10.11.29.252:1018] recv 20 bytes
4d06h:SCP:[22 <- 10.11.29.252:1018] recv <OK>
4d06h:SCP:[22 -> 10.11.29.252:1018] send <OK>
4d06h:SCP:[22 <- 10.11.29.252:1018] recv <EOF>
```

The following example is also output from the `debug ip scp` command, but in this example, the user has privilege 0 and is therefore denied:

```
Router# debug ip scp
4d06h:SCP:[22 -> 10.11.29.252:1018] send Privilege denied.
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip scp server enable</td>
<td>Enables SCP server-side functionality.</td>
</tr>
</tbody>
</table>

**debug ip sctp api**

To provide diagnostic information about Stream Control Transmission Protocol (SCTP) application programming interfaces (APIs), use the `debug ip sctp api` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
depth ip sctp api
no debug ip sctp api
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

In a live system, the debugging messages for performance, state, signal, and warnings are the most useful. These show any association or destination address failures and can be used to monitor the stability of any established associations.

**Caution**

The `debug ip sctp api` command should not be used in a live system that has any significant amount of traffic running because it can generate a lot of traffic, which can cause associations to fail.

**Examples**

The following example shows SCTP calls to the API that are being executed and the parameters associated with these calls:

```
Router# debug ip sctp api
*Mar 1 00:31:14.211: SCTP: sctp_send: Assoc ID: 1
*Mar 1 00:31:14.211: SCTP: stream num: 10
*Mar 1 00:31:14.211: SCTP: datalen: 100
*Mar 1 00:31:14.211: SCTP: context: 1
*Mar 1 00:31:14.211: SCTP: lifetime: 0
*Mar 1 00:31:14.211: SCTP: unordered flag: FALSE
*Mar 1 00:31:14.211: SCTP: bundle flag: TRUE
*Mar 1 00:31:14.211: SCTP: sctp_send successful return
*Mar 1 00:31:14.211: SCTP: sctp_receive: Assoc ID: 1
*Mar 1 00:31:14.211: SCTP: sctp_receive successful return
*Mar 1 00:31:14.211: SCTP: Process Send Request
*Mar 1 00:31:14.951: SCTP: max data len: 100
*Mar 1 00:31:14.951: SCTP: sctp_receive: Assoc ID: 0
*Mar 1 00:31:14.951: SCTP: sctp_receive successful return
```

The table below describes the significant fields shown in the display.

**Table 53: debug ip sctp api Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assoc ID</td>
<td>Association identifier.</td>
</tr>
<tr>
<td>stream num</td>
<td>SCTP stream number.</td>
</tr>
<tr>
<td>bptr, dptr</td>
<td>Address of the buffer that contains the data, and address of the start of the data.</td>
</tr>
<tr>
<td>datalen</td>
<td>Length of the data that the application is sending (the datagram).</td>
</tr>
<tr>
<td>context</td>
<td>A value that is meaningful to the application. Returned with the datagram if the datagram ever needs to be retrieved.</td>
</tr>
<tr>
<td>lifetime</td>
<td>Not used.</td>
</tr>
<tr>
<td>unordered flag</td>
<td>Specifies that the datagram should be sent as unordered data.</td>
</tr>
<tr>
<td>bundle flag</td>
<td>Indicates whether the application wants the datagram to be delayed slightly, trying to bundle it with other data being sent.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
max data len | Maximum length of data that can be received—the size of the receive buffer.

### Related Commands

| Command | Description |
--- | ---|
| clear ip sctp statistics | Empties the buffer that holds SCTP statistics. |
| debug ip sctp congestion | Shows a list of all current SCTP associations. |
| show ip sctp association parameters | Shows the parameters configured for the association defined by the association identifier. |
| show ip sctp association statistics | Shows the current statistics for the association defined by the association identifier. |
| show ip sctp errors | Shows error counts logged by SCTP. |
| show ip sctp instances | Shows all currently defined SCTP instances. |
| show ip sctp statistics | Shows overall statistics counts for SCTP. |
| show iua as | Shows information about the current condition of an application server. |
| show iua asp | Shows information about the current condition of an application server process. |

## debug ip sctp congestion

To provide diagnostic information about Stream Control Transmission Protocol (SCTP) congestion parameters, use the `debug ip sctp congestion` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip sctp congestion
no debug ip sctp congestion
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

In a live system, the debugging messages for performance, state, signal, and warnings are the most useful. These show any association or destination address failures and can be used to monitor the stability of any established associations.

Debug commands other than those for performance, state, signal, and warnings can generate a great deal of output and therefore can cause associations to fail. These commands should be used only in test environments or when there are very low amounts of traffic.

Examples

The following example shows parameters used to calculate SCTP congestion:

Router# debug ip sctp congestion
SCTP: Assoc 0: Slow start 10.6.0.4, cwnd 3000
SCTP: Assoc 0: Data chunks rcvd, local rwnd 7800
SCTP: Assoc 0: Free chunks, local rwnd 9000
SCTP: Assoc 0: Data chunks rcvd, local rwnd 8200
SCTP: Assoc 0: Free chunks, local rwnd 9000
SCTP: Assoc 0: Data chunks rcvd, local rwnd 7800
SCTP: Assoc 0: Data chunks rcvd, local rwnd 7000
SCTP: Assoc 0: Add Sack, local a_rwnd 8200
SCTP: Assoc 0: Free chunks, local rwnd 9000
SCTP: Assoc 0: Bundle for 10.5.0.4, rem rwnd 14000, cwnd 19500, outstand 0
SCTP: Assoc 0: Bundled 12 chunks, remote rwnd 12800, outstanding 1200
SCTP: Assoc 0: Bundling data, next chunk datalen (100) > remaining mtu size
SCTP: Assoc 0: Bundle for 10.5.0.4, rem rwnd 12800, cwnd 19500, outstanding 1200
SCTP: Assoc 0: Bundled 12 chunks, remote rwnd 11600, outstanding 2400
SCTP: Assoc 0: Bundling data, next chunk datalen (100) > remaining mtu size
SCTP: Assoc 0: Bundle for 10.5.0.4, rem rwnd 11600, cwnd 19500, outstanding 2400
SCTP: Assoc 0: Bundled 12 chunks, remote rwnd 10400, outstanding 3600
SCTP: Assoc 0: Bundling data, next chunk datalen (100) > remaining mtu size
SCTP: Assoc 0: Bundle for 10.5.0.4, rem rwnd 10400, cwnd 19500, outstanding 3600
SCTP: Assoc 0: Bundled 4 chunks, remote rwnd 10000, outstanding 4000
SCTP: Assoc 0: No additional chunks waiting.
SCTP: Assoc 0: Data chunks rcvd, local rwnd 7800
SCTP: Assoc 0: Data chunks rcvd, local rwnd 7000
SCTP: Assoc 0: Add Sack, local a_rwnd 7000
SCTP: Assoc 0: Chunk A22F3B45 ack'd, dest 10.5.0.4, outstanding 3900
SCTP: Assoc 0: Chunk A22F3B46 ack'd, dest 10.5.0.4, outstanding 3800
SCTP: Assoc 0: Chunk A22F3B47 ack'd, dest 10.5.0.4, outstanding 3700
SCTP: Assoc 0: Chunk A22F3B48 ack'd, dest 10.5.0.4, outstanding 3600
SCTP: Assoc 0: Chunk A22F3B49 ack'd, dest 10.5.0.4, outstanding 3500
SCTP: Assoc 0: Chunk A22F3B4A ack'd, dest 10.5.0.4, outstanding 3400
SCTP: Assoc 0: Chunk A22F3B4B ack'd, dest 10.5.0.4, outstanding 3300
SCTP: Assoc 0: Chunk A22F3B4C ack'd, dest 10.5.0.4, outstanding 3200
SCTP: Assoc 0: Chunk A22F3B4D ack'd, dest 10.5.0.4, outstanding 3100
SCTP: Assoc 0: Chunk A22F3B4E ack'd, dest 10.5.0.4, outstanding 3000
SCTP: Assoc 0: Chunk A22F3B4F ack'd, dest 10.5.0.4, outstanding 2900
SCTP: Assoc 0: Chunk A22F3B50 ack'd, dest 10.5.0.4, outstanding 2800
SCTP: Assoc 0: Chunk A22F3B51 ack'd, dest 10.5.0.4, outstanding 2700
SCTP: Assoc 0: Chunk A22F3B52 ack'd, dest 10.5.0.4, outstanding 2600
SCTP: Assoc 0: Chunk A22F3B53 ack'd, dest 10.5.0.4, outstanding 2500
SCTP: Assoc 0: Chunk A22F3B54 ack'd, dest 10.5.0.4, outstanding 2400
SCTP: Assoc 0: Chunk A22F3B55 ack'd, dest 10.5.0.4, outstanding 2300
SCTP: Assoc 0: Chunk A22F3B56 ack'd, dest 10.5.0.4, outstanding 2200

The table below describes the significant fields shown in the display.
### Table 54: debug ip sctp congestion Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cwnd</td>
<td>Congestion window values for destination address.</td>
</tr>
<tr>
<td>rwnd, a_rwnd</td>
<td>Receiver window values as defined in RFC 2960.</td>
</tr>
<tr>
<td>outstanding</td>
<td>Number of bytes outstanding.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip sctp statistics</td>
<td>Empties the buffer that holds SCTP statistics.</td>
</tr>
<tr>
<td>show ip sctp association parameters</td>
<td>Shows the parameters configured for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp association statistics</td>
<td>Shows the current statistics for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp errors</td>
<td>Shows error counts logged by SCTP.</td>
</tr>
<tr>
<td>show ip sctp instances</td>
<td>Shows all currently defined SCTP instances.</td>
</tr>
<tr>
<td>show ip sctp statistics</td>
<td>Shows overall statistics counts for SCTP.</td>
</tr>
<tr>
<td>show iua as</td>
<td>Shows information about the current condition of an application server.</td>
</tr>
<tr>
<td>show iua asp</td>
<td>Shows information about the current condition of an application server process.</td>
</tr>
</tbody>
</table>

### debug ip sctp init

To show datagrams and other information related to the initializing of new Stream Control Transmission Protocol (SCTP) associations, use the `debug ip sctp init` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip sctp init
no debug ip sctp init
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

---

**Related Commands**

- clear ip sctp statistics
- show ip sctp association parameters
- show ip sctp association statistics
- show ip sctp errors
- show ip sctp instances
- show ip sctp statistics
- show iua as
- show iua asp
Modification

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

Usage Guidelines

All initialization chunks are shown, including the INIT, INIT_ACK, COOKIE_ECHO, and COOKIE_ACK chunks. This debug command can be used to see the chunks associated with any initialization sequence but does not display data chunks sent once the association is established. Therefore, it is safe to use in a live system that has traffic flowing when you have trouble with associations failing and being reestablished.

Examples

The following example shows initialization chunks for SCTP associations:

```
Router# debug ip sctp init
*Mar 1 00:53:07.279: SCTP Test: Attempting to open assoc to remote port 8787...assoc ID is 0
*Mar 1 00:53:07.279: SCTP: Process Assoc Request
*Mar 1 00:53:07.279: SCTP: Assoc 0: dest addr list:
*Mar 1 00:53:07.279: SCTP:     addr 10.5.0.4
*Mar 1 00:53:07.279: SCTP:     addr 10.6.0.4
*Mar 1 00:53:07.279:
*Mar 1 00:53:13.279: SCTP: Assoc 0: Send Init
*Mar 1 00:53:13.279: SCTP:     INIT_CHUNK, len 42
*Mar 1 00:53:13.279: SCTP:     Initiate Tag: B4A10C4D, Initial TSN: B4A10C4D, rwnd 9000
*Mar 1 00:53:13.279: SCTP: Streams Inbound: 13, Outbound: 13
*Mar 1 00:53:13.279: SCTP:     IP Addr: 10.1.0.2
*Mar 1 00:53:13.279: SCTP:     IP Addr: 10.2.0.2
*Mar 1 00:53:13.279: SCTP: Supported addr types: 5
*Mar 1 00:53:13.307: SCTP: Process Init
*Mar 1 00:53:13.307: SCTP:     INIT_CHUNK, len 42
*Mar 1 00:53:13.307: SCTP:     Initiate Tag: 3C2D8327, Initial TSN: 3C2D8327, rwnd 18000
*Mar 1 00:53:13.307: SCTP:     IP Addr: 10.5.0.4
*Mar 1 00:53:13.307: SCTP:     IP Addr: 10.6.0.4
*Mar 1 00:53:13.307: SCTP: Supported addr types: 5
*Mar 1 00:53:13.307: SCTP: Assoc 0: Send InitAck
*Mar 1 00:53:13.307: SCTP:     INIT_ACK_CHUNK, len 124
*Mar 1 00:53:13.307: SCTP:     Responder cookie len 88
*Mar 1 00:53:13.307: SCTP:     IP Addr: 10.1.0.2
*Mar 1 00:53:13.307: SCTP:     IP Addr: 10.2.0.2
*Mar 1 00:53:13.311: SCTP: Assoc 0: Process Cookie
*Mar 1 00:53:13.311: SCTP:     COOKIE_ECHO_CHUNK, len 88
*Mar 1 00:53:13.311: SCTP: Assoc 0: dest addr list:
*Mar 1 00:53:13.311: SCTP:     addr 10.5.0.4
*Mar 1 00:53:13.311: SCTP:     addr 10.6.0.4
*Mar 1 00:53:13.311:
*Mar 1 00:53:13.311: SCTP: Instance 0 dest addr list:
*Mar 1 00:53:13.311: SCTP:     addr 10.5.0.4
*Mar 1 00:53:13.311: SCTP:     addr 10.6.0.4
*Mar 1 00:53:13.311:
*Mar 1 00:53:13.311: SCTP: Assoc 0: Send CookieAck
*Mar 1 00:53:13.311: SCTP: COOKIE_ACK_CHUNK
```

The table below describes the significant fields shown in the display.
### Table 55: `debug ip sctp init Field Descriptions`

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation Tag</td>
<td>Initiation chunk identifier.</td>
</tr>
<tr>
<td>Initial TSN</td>
<td>Initial transmission sequence number.</td>
</tr>
<tr>
<td>rwnd</td>
<td>Receiver window values.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear ip sctp statistics</code></td>
<td>Empties the buffer that holds SCTP statistics.</td>
</tr>
<tr>
<td><code>debug ip sctp congestion</code></td>
<td>Shows a list of all current SCTP associations.</td>
</tr>
<tr>
<td><code>show ip sctp association parameters</code></td>
<td>Shows the parameters configured for the association defined by the association identifier.</td>
</tr>
<tr>
<td><code>show ip sctp association statistics</code></td>
<td>Shows the current statistics for the association defined by the association identifier.</td>
</tr>
<tr>
<td><code>show ip sctp errors</code></td>
<td>Shows error counts logged by SCTP.</td>
</tr>
<tr>
<td><code>show ip sctp instances</code></td>
<td>Shows all currently defined SCTP instances.</td>
</tr>
<tr>
<td><code>show ip sctp statistics</code></td>
<td>Shows overall statistics counts for SCTP.</td>
</tr>
<tr>
<td><code>show iua as</code></td>
<td>Shows information about the current condition of an application server.</td>
</tr>
<tr>
<td><code>show iua asp</code></td>
<td>Shows information about the current condition of an application server process.</td>
</tr>
</tbody>
</table>

### `debug ip sctp multihome`

To show the source and destination of datagrams in order to monitor the use of the multihome addresses for Stream Control Transmission Protocol (SCTP), use the `debug ip sctp multihome` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
display ip sctp multihome
no display ip sctp multihome
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

More than one IP address parameter can be included in an initialization (INIT) chunk when the INIT sender is multihomed. Datagrams should be sent to the primary destination addresses unless the network is experiencing problems, in which case the datagrams should be sent to secondary addresses.

Caution

The `debug ip sctp multihome` command generates one debug line for each datagram sent or received. It should be used with extreme caution in a live network.

Examples

The following example shows source and destination for multihomed addresses:

```
Router# debug ip sctp multihome
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 1404
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 476
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 28
SCTP: Assoc 0: Send Data to dest 10.5.0.4
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 1404
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 1404
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 1404
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 476
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 28
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 28
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 1404
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 1404
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 28
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 1404
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 476
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 28
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 28
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 1404
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 28
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 1404
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 476
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 28
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 28
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 1404
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 476
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>s</td>
<td>Source address and port.</td>
</tr>
<tr>
<td>d</td>
<td>Destination address and port.</td>
</tr>
</tbody>
</table>
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip sctp statistics</td>
<td>Empties the buffer that holds SCTP statistics.</td>
</tr>
<tr>
<td>debug ip sctp congestion</td>
<td>Shows a list of all current SCTP associations.</td>
</tr>
<tr>
<td>show ip sctp association parameters</td>
<td>Shows the parameters configured for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp association statistics</td>
<td>Shows the current statistics for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp errors</td>
<td>Shows error counts logged by SCTP.</td>
</tr>
<tr>
<td>show ip sctp instances</td>
<td>Shows all currently defined SCTP instances.</td>
</tr>
<tr>
<td>show ip sctp statistics</td>
<td>Shows overall statistics counts for SCTP.</td>
</tr>
<tr>
<td>show iua as</td>
<td>Shows information about the current condition of an application server.</td>
</tr>
<tr>
<td>show iua asp</td>
<td>Shows information about the current condition of an application server process.</td>
</tr>
</tbody>
</table>

**debug ip sctp performance**

To display the average number of Stream Control Transmission Protocol (SCTP) chunks and datagrams being sent and received per second, use the `debug ip sctp performance` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
depug ip sctp performance
no debug ip sctp performance
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

In a live system, the debugging messages for performance, state, signal, and warnings are the most useful. These show any association or destination address failures and can be used to monitor the stability of any established associations.

Once enabled, the `debug ip sctp performance` command displays the average number of chunks and datagrams being sent and received per second once every 10 seconds. Note that the averages are cumulative since the last time the statistics were cleared using the `clear ip sctp statistics` command and may not accurately reflect the number of datagrams and chunks currently being sent and received at that particular moment.
The following example shows a low rate of traffic:

Router# debug ip sctp performance

SCTP Sent: SCTP Dgrams 5, Chunks 28, Data Chunks 29, ULP Dgrams 29
SCTP Rcvd: SCTP Dgrams 7, Chunks 28, Data Chunks 29, ULP Dgrams 29
Chunks Discarded: 0, Retransmitted 0
SCTP Sent: SCTP Dgrams 6, Chunks 29, Data Chunks 30, ULP Dgrams 30
SCTP Rcvd: SCTP Dgrams 7, Chunks 29, Data Chunks 30, ULP Dgrams 30
Chunks Discarded: 0, Retransmitted 0

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCTP Dgrams</td>
<td>Datagram sent to or received from the network.</td>
</tr>
<tr>
<td>Chunks</td>
<td>Includes data chunks and control chunks sent or received.</td>
</tr>
<tr>
<td>Data Chunks</td>
<td>Data chunks sent or received.</td>
</tr>
<tr>
<td>ULP Dgrams</td>
<td>Upper-layer protocol (ULP) datagrams, which are datagrams sent to or received from the ULP or application.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip sctp statistics</td>
<td>Empties the buffer that holds SCTP statistics.</td>
</tr>
<tr>
<td>debug ip sctp congestion</td>
<td>Shows a list of all current SCTP associations.</td>
</tr>
<tr>
<td>show ip sctp association parameters</td>
<td>Shows the parameters configured for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp association statistics</td>
<td>Shows the current statistics for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp errors</td>
<td>Shows error counts logged by SCTP.</td>
</tr>
<tr>
<td>show ip sctp instances</td>
<td>Shows all currently defined SCTP instances.</td>
</tr>
<tr>
<td>show ip sctp statistics</td>
<td>Shows overall statistics counts for SCTP.</td>
</tr>
<tr>
<td>show iua as</td>
<td>Shows information about the current condition of an application server.</td>
</tr>
<tr>
<td>show iua asp</td>
<td>Shows information about the current condition of an application server process.</td>
</tr>
</tbody>
</table>
debug ip sctp rcvchunks

To provide diagnostic information about chunks received with Stream Control Transmission Protocol (SCTP), use the `debug ip sctp rcvchunks` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
degen ip sctp rcvchunks
no debug ip sctp rcvchunks
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
No default behavior or values

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `debug ip sctp rcvchunks` command shows the following information about received chunks:

- Whether the chunk is for a new datagram or is part of a datagram that is being reassembled
- Whether the datagram is complete after receiving this chunk
- If the datagram is complete, whether the datagram is in sequence within the specified stream and can be delivered to the upper-layer protocol (ULP)
- The selective acknowledgments (SACKs) that are returned to the remote SCTP peer
- The cumulative transmission sequence number (Cum TSN) that was acknowledged and the number of fragments included
- Whether the datagram is received by the ULP

⚠️ **Caution**
The `debug ip sctp rcvchunks` command generates multiple debug lines for each chunk received. It should be used with extreme caution in a live network.

**Examples**
In the following example, a segmented datagram is received in two chunks for stream 0 and sequence number 0. The length of the first chunk is 1452 bytes, and the second is 1 byte. The first chunk indicates that it is for a new datagram, but the second chunk indicates that it is part of an existing datagram that is already being reassembled. When the first chunk is processed, it is noted to be in sequence, but is not complete and so cannot be delivered yet. When the second chunk is received, the datagram is both in sequence and complete. The application receives the datagram, and a SACK is shown to acknowledge that both chunks were received with no missing chunks indicated (that is, with no fragments).

```
Router# debug ip sctp rcvchunks
SCTP: Assoc 0: New chunk (0/0/1452/2C33D822) for new dgram (0)
```
The table below describes the significant fields shown in the display.

Table 58: debug ip sctp recvchunks Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/0/1452/2C33D822</td>
<td>Stream number / datagram sequence number / chunk length, in bytes / chunk transmission sequence number.</td>
</tr>
<tr>
<td>Sack Chunk</td>
<td>Selective acknowledgment chunk.</td>
</tr>
<tr>
<td>ApplRecv</td>
<td>Application has received the chunk.</td>
</tr>
<tr>
<td>CumTSN</td>
<td>Cumulative transmission sequence number that is being acknowledged.</td>
</tr>
<tr>
<td>numFrgags</td>
<td>Number of fragments, or missing chunks.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip sctp statistics</td>
<td>Empties the buffer that holds SCTP statistics.</td>
</tr>
<tr>
<td>debug ip sctp congestion</td>
<td>Shows a list of all current SCTP associations.</td>
</tr>
<tr>
<td>show ip sctp association parameters</td>
<td>Shows the parameters configured for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp association statistics</td>
<td>Shows the current statistics for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp errors</td>
<td>Shows error counts logged by SCTP.</td>
</tr>
<tr>
<td>show ip sctp instances</td>
<td>Shows all currently defined SCTP instances.</td>
</tr>
<tr>
<td>show ip sctp statistics</td>
<td>Shows overall statistics counts for SCTP.</td>
</tr>
<tr>
<td>show iua as</td>
<td>Shows information about the current condition of an application server.</td>
</tr>
<tr>
<td>show iua asp</td>
<td>Shows information about the current condition of an application server process.</td>
</tr>
</tbody>
</table>

**debug ip sctp rto**

To show adjustments that are made to the retransmission timeout (RTO) value when using Stream Control Transmission Protocol (SCTP), use the **debug ip sctp rto** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.
debug ip scpt rto
no debug ip scpt rto

Syntax Description
This command has no arguments or keywords.

Command Default
No default behavior or values

Command Modes
Privileged EXEC

Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 12.2(4)T | This command was introduced.

Usage Guidelines
The debug ip scpt rto command shows adjustments that are made to the retransmission timeout value (shown as retrans in the command output) because of either retransmission of data chunks or unacknowledged heartbeats.

Caution
The debug ip scpt rto command can generate a great deal of output. It should be used with extreme caution in a live network.

Examples
In the following example, there is only one destination address available. Each time the chunk needs to be retransmitted, the RTO value is doubled.

Router# debug ip scpt rto
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 942BAC55
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 2000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 942BAC55
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 4000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 942BAC55
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 8000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 942BAC55
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 16000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 942BAC55
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 32000 ms

Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip scpt statistics</td>
<td>Empties the buffer that holds SCTP statistics.</td>
</tr>
<tr>
<td>debug ip scpt congestion</td>
<td>Shows a list of all current SCTP associations.</td>
</tr>
<tr>
<td>show ip scpt association parameters</td>
<td>Shows the parameters configured for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip scpt association statistics</td>
<td>Shows the current statistics for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip scpt errors</td>
<td>Shows error counts logged by SCTP.</td>
</tr>
</tbody>
</table>
### debug ip sctp segments

To show short diagnostics for every datagram that is sent or received with Stream Control Transmission Protocol (SCTP), use the `debug ip sctp segments` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 12.2(4)T | This command was introduced.

**Usage Guidelines**

The `debug ip sctp segments` command provides the short form of the output about datagrams. For the verbose form, use the `debug ip sctp segments v` command.

**Caution**

The `debug ip sctp segments` command generates several lines of output for each datagram sent or received. It should be used with extreme caution in a live network.

**Examples**

The following output shows an example in which an association is established, a few heartbeats are sent, the remote endpoint fails, and the association is restarted.

```
Router# debug ip sctp segments
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 56
SCTP: INIT_CHUNK, Tag: 3C72A02A, TSN: 3C72A02A
SCTP: Recv: Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 56
SCTP: INIT_CHUNK, Tag: 13E5AD6C, TSN: 13E5AD6C
SCTP: Sent: Assoc NULL: s=10.1.0.2 8787, d=10.5.0.4 8787, len 136
SCTP: INIT_ACK_CHUNK, Tag: 3C72A02A, TSN: 3C72A02A
SCTP: Recv: Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 100
```
SCTP: COOKIE_ECHO_CHUNK, len 88
SCTP: Sent: Assoc NULL: s=10.1.0.2 8787, d=10.5.0.4 8787, len 16
SCTP: COOKIE_ACK_CHUNK
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 52
SCTP: HEARTBEAT_CHUNK
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 52
SCTP: HEARTBEAT_CHUNK
SCTP: Recv: Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 56
SCTP: INIT_CHUNK, Tag: 4F2D8235, TSN: 4F2D8235
SCTP: Sent: Assoc NULL: s=10.1.0.2 8787, d=10.5.0.4 8787, len 136
SCTP: INIT_ACK_CHUNK, Tag: 7DD7E424, TSN: 7DD7E424
SCTP: Recv: Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 100
SCTP: COOKIE_ECHO_CHUNK, len 88
SCTP: Sent: Assoc NULL: s=10.1.0.2 8787, d=10.5.0.4 8787, len 16
SCTP: COOKIE_ACK_CHUNK
SCTP: Recv: Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 144
SCTP: SACK_CHUNK, TSN ack: 7DD7E423, rwnd 18000, num frags 0
SCTP: DATA_CHUNK, 4/0/100/4F2D8235
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 28
SCTP: SACK_CHUNK, TSN ack: 4F2D8235, rwnd 8900, num frags 0
SCTP: DATA_CHUNK, 4/0/100/7DD7E424
SCTP: Recv: Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 28
SCTP: SACK_CHUNK, TSN ack: 7DD7E424, rwnd 17900, num frags 0
SCTP: Recv: Assoc 0: s=10.6.0.4 8787, d=10.2.0.2 8787, len 44
SCTP: HEARTBEAT_CHUNK
SCTP: Sent: Assoc 0: s=10.2.0.2 8787, d=10.6.0.4 8787, len 44
SCTP: HEARTBEAT_ACK_CHUNK
SCTP: Recv: Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 128
SCTP: DATA_CHUNK, 7/0/100/4F2D8236
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 144
SCTP: SACK_CHUNK, TSN ack: 4F2D8236, rwnd 9000, num frags 0
SCTP: DATA_CHUNK, 7/0/100/7DD7E425
SCTP: Recv: Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 28
SCTP: SACK_CHUNK, TSN ack: 7DD7E424, rwnd 18000, num frags 0
SCTP: Recv: Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 28
SCTP: SACK_CHUNK, TSN ack: 7DD7E425, rwnd 17900, num frags 0
SCTP: Recv: Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 128
SCTP: DATA_CHUNK, 4/1/100/4F2D8237

The table below describes the significant fields shown in the display.

Table 59: debug ip sctp segments Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>s</td>
<td>Source address and port.</td>
</tr>
<tr>
<td>d</td>
<td>Destination address and port.</td>
</tr>
<tr>
<td>len</td>
<td>Length of chunk, in bytes.</td>
</tr>
<tr>
<td>Tag</td>
<td>The identifier for an initialization chunk.</td>
</tr>
<tr>
<td>TSN</td>
<td>Transmission sequence number.</td>
</tr>
<tr>
<td>rwnd</td>
<td>Receiver window value.</td>
</tr>
<tr>
<td>num frags</td>
<td>Number of fragments received.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
---|---
7 / 0 / 100 / 4F2D8236 | (Data chunks) Stream number / datagram sequence number / chunk length, in bytes / chunk transmission sequence number.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip sctp statistics</td>
<td>Empties the buffer that holds SCTP statistics.</td>
</tr>
<tr>
<td>debug ip sctp congestion</td>
<td>Shows a list of all current SCTP associations.</td>
</tr>
<tr>
<td>debug ip sctp segmentv</td>
<td>Shows every datagram that is sent or received and the chunks that are contained in each. This is the verbose form of the output, and it shows detailed information for each chunk type.</td>
</tr>
<tr>
<td>show ip sctp association parameters</td>
<td>Shows the parameters configured for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp association statistics</td>
<td>Shows the current statistics for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp errors</td>
<td>Shows error counts logged by SCTP.</td>
</tr>
<tr>
<td>show ip sctp instances</td>
<td>Shows all currently defined SCTP instances.</td>
</tr>
<tr>
<td>show ip sctp statistics</td>
<td>Shows overall statistics counts for SCTP.</td>
</tr>
<tr>
<td>show iua as</td>
<td>Shows information about the current condition of an application server.</td>
</tr>
<tr>
<td>show iua asp</td>
<td>Shows information about the current condition of an application server process.</td>
</tr>
</tbody>
</table>

**debug ip sctp segmentv**

To show verbose diagnostics for every datagram that is sent or received with Stream Control Transmission Protocol (SCTP), use the `debug ip sctp segmentv` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip sctp segmentv
no debug ip sctp segmentv
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ip sctp segmentv` command provides the verbose form of the output for datagrams. For the simple form, use the `debug ip sctp segments` command.

⚠️ **Caution**

The `debug ip sctp segmentv` command generates multiple lines of output for each datagram sent and received. It should be used with extreme caution in a live network.

**Examples**

The following output shows an example in which an association is established, a few heartbeats are sent, the remote endpoint fails, and the association is restarted:

```
Router# debug ip sctp segmentv
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 56, ver tag 0
SCTP:    INIT_CHUNK, len 42
SCTP:    Initiate Tag: B131ED6A, Initial TSN: B131ED6A, rwnd 9000
SCTP:    Streams Inbound: 13, Outbound: 13
SCTP:    IP Addr: 10.1.0.2
SCTP:    IP Addr: 10.2.0.2
SCTP:    Supported addr types: 5
SCTP: Recv: Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 56, ver tag 0
SCTP:    INIT_CHUNK, len 42
SCTP:    Streams Inbound: 13, Outbound: 13
SCTP:    IP Addr: 10.5.0.4
SCTP:    IP Addr: 10.6.0.4
SCTP:    Supported addr types: 5
SCTP: Sent: Assoc NULL: s=10.1.0.2 8787, d=10.5.0.4 8787, len 136, ver tag 5516B2F3
SCTP:    INIT_ACK_CHUNK, len 124
SCTP:    Initiate Tag: B131ED6A, Initial TSN: B131ED6A, rwnd 9000
SCTP:    Streams Inbound: 13, Outbound: 13
SCTP:    Responder cookie len 88
SCTP:    IP Addr: 10.1.0.2
SCTP:    IP Addr: 10.2.0.2
SCTP: Recv: Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 100, ver tag B131ED6A
SCTP:    COOKIE_ECHO_CHUNK, len 88
SCTP:    Streams Inbound: 13, Outbound: 13
SCTP:    Supported addr types: 5
SCTP: Sent: Assoc NULL: s=10.1.0.2 8787, d=10.5.0.4 8787, len 16, ver tag 5516B2F3
SCTP:    COOKIE_ACK_CHUNK
SCTP: Recv: Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 144, ver tag B131ED6A
SCTP:    SACK CHUNK, len 16
SCTP:    TSN ack: (0xB131ED69)
SCTP:    Rcv win credit: 18000
SCTP:    Num frags: 0
SCTP:    DATA CHUNK, flags 3, chunkLen 116
SCTP:    DATA CHUNK, 0/0/100/5516B2F3
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 28, ver tag 5516B2F3
SCTP:    SACK CHUNK, len 16
SCTP:    TSN ack: (0x5516B2F3)
SCTP:    Rcv win credit: 8900
SCTP:    Num frags: 0
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 128, ver tag 5516B2F3
SCTP:    DATA CHUNK, flags 3, chunkLen 116
SCTP:    DATA CHUNK, 0/0/100/B131ED6A
SCTP: Recv: Assoc 0: s=10.6.0.4 8787, d=10.2.0.2 8787, len 44, ver tag B131ED6A
SCTP:    HEARTBEAT_CHUNK
SCTP: Sent: Assoc 0: s=10.2.0.2 8787, d=10.6.0.4 8787, len 44, ver tag 5516B2F3
```
The table below describes the significant fields shown in the display.

Table 60: debug ip sctp segmentv Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>s</td>
<td>Source address and port.</td>
</tr>
<tr>
<td>d</td>
<td>Destination address and port.</td>
</tr>
<tr>
<td>len</td>
<td>Length of chunk, in bytes.</td>
</tr>
<tr>
<td>ver tag</td>
<td>Verification identifier.</td>
</tr>
<tr>
<td>Tag</td>
<td>The identifier for an initialization chunk.</td>
</tr>
<tr>
<td>TSN</td>
<td>Transmission sequence number.</td>
</tr>
<tr>
<td>rwnd</td>
<td>Receive window value.</td>
</tr>
<tr>
<td>Rcv win credit</td>
<td>Receive window value. Same as rwnd.</td>
</tr>
<tr>
<td>Num frags</td>
<td>Number of fragments received.</td>
</tr>
<tr>
<td>0/0/100/5516B2F3</td>
<td>(Data chunks) Stream number / datagram sequence number / chunk length, in bytes / chunk transmission sequence number.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip sctp statistics</td>
<td>Empties the buffer that holds SCTP statistics.</td>
</tr>
<tr>
<td>debug ip sctp congestion</td>
<td>Shows a list of all current SCTP associations.</td>
</tr>
<tr>
<td>debug ip sctp segments</td>
<td>Shows short diagnostics for every datagram that is sent or received with SCTP.</td>
</tr>
<tr>
<td>show ip sctp association parameters</td>
<td>Shows the parameters configured for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp association statistics</td>
<td>Shows the current statistics for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp errors</td>
<td>Shows error counts logged by SCTP.</td>
</tr>
<tr>
<td>show ip sctp instances</td>
<td>Shows all currently defined SCTP instances.</td>
</tr>
<tr>
<td>show ip sctp statistics</td>
<td>Shows overall statistics counts for SCTP.</td>
</tr>
<tr>
<td>show iua as</td>
<td>Shows information about the current condition of an application server.</td>
</tr>
</tbody>
</table>
debug ip sctp signal

To show signals that are sent from Stream Control Transmission Protocol (SCTP) to the application or upper-layer protocol (ULP), use the `debug ip sctp signal` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ip sctp signal` command can be used to see if the current associations are stable or not. Because it generates output only on state transitions, it is safe to use in a live environment. It still should be used with caution, however, depending on the number of associations being handled by the system and the stability of the network.

The `debug ip sctp state` command is often used at the same time as the `debug ip sctp signal` command. Using the two commands together gives good insight into the stability of associations.

**Examples**

In the following example, a new association is requested and established. The peer then restarts the association and notes that the association failed and is being reestablished. The local peer then indicates that the association has failed because it has tried to retransmit the specified chunk more than the maximum number of times without success. As a result, the association fails (because of communication loss) and is terminated. The ULP requests that the association be attempted again, and this attempt succeeds. A shutdown is then received from the remote peer, and the local peer enters the shutdown acknowledge sent state, which is followed by the association being terminated. Again, another association attempt is made and succeeds.

```
Router# debug ip sctp signal
Router# debug ip sctp state
<new assoc attempt>
00:20:08: SCTP: Assoc 0: state CLOSED -> COOKIE_WAIT
00:20:15: SCTP: Assoc 0: state COOKIE_WAIT -> ESTABLISHED
00:20:15: SCTP: Assoc 0: Sent ASSOC_UP signal for CONFIGD_ASSOC
00:21:03: SCTP: Assoc 0: Restart rcvd from peer
00:21:03: SCTP: Assoc 0: Sent ASSOC_RESTART signal
00:21:04: SCTP: Assoc 0: chunk 62EA7F40 retransmitted more than max times, failing assoc
```
00:21:04: SCTP: Assoc 0: Sent ASSOC_FAILED signal, reason: SCTP_COMM_LOST
00:21:04: SCTP: Assoc 0: Sent ASSOC_TERMINATE signal
00:21:04: SCTP: Assoc 0: state ESTABLISHED -> CLOSED
<new assoc attempt>
00:21:04: SCTP: Assoc 0: state CLOSED -> COOKIE_WAIT
00:21:04: SCTP: Assoc 0: state COOKIE_WAIT -> COOKIE_ECHOED
00:21:04: SCTP: Assoc 0: state COOKIE_ECHOED -> ESTABLISHED
00:21:04: SCTP: Assoc 0: Sent ASSOC_UP signal for CONFIGD_ASSOC
00:21:04: SCTP: Assoc 0: state TERMINATE_PENDING signal
00:21:04: SCTP: Assoc 0: state ESTABLISHED -> SHUTDOWN_ACKSENT
00:21:04: SCTP: Assoc 0: Sent ASSOC_TERMINATE signal
00:21:04: SCTP: Assoc 0: state SHUTDOWN_ACKSENT -> CLOSED
<new assoc attempt>
00:21:04: SCTP: Assoc 0: state CLOSED -> COOKIE_WAIT
00:21:04: SCTP: Assoc 0: state COOKIE_WAIT -> COOKIE_ECHOED
00:21:04: SCTP: Assoc 0: state COOKIE_ECHOED -> ESTABLISHED
00:21:04: SCTP: Assoc 0: Sent ASSOC_UP signal for CONFIGD_ASSOC

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip sctp statistics</td>
<td>Empties the buffer that holds SCTP statistics.</td>
</tr>
<tr>
<td>debug ip sctp congestion</td>
<td>Shows a list of all current SCTP associations.</td>
</tr>
<tr>
<td>debug ip sctp state</td>
<td>Shows SCTP state transitions.</td>
</tr>
<tr>
<td>show ip sctp association parameters</td>
<td>Shows the parameters configured for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp association statistics</td>
<td>Shows the current statistics for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp errors</td>
<td>Shows error counts logged by SCTP.</td>
</tr>
<tr>
<td>show ip sctp instances</td>
<td>Shows all currently defined SCTP instances.</td>
</tr>
<tr>
<td>show ip sctp statistics</td>
<td>Shows overall statistics counts for SCTP.</td>
</tr>
<tr>
<td>show iua as</td>
<td>Shows information about the current condition of an application server.</td>
</tr>
<tr>
<td>show iua asp</td>
<td>Shows information about the current condition of an application server process.</td>
</tr>
</tbody>
</table>

### debug ip sctp sndchunks

To show information about chunks that are being sent to remote Stream Control Transmission Protocol (SCTP) peers, use the `debug ip sctp sndchunks` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

**debug ip sctp sndchunks**

**no debug ip sctp sndchunks**

### Syntax Description

This command has no arguments or keywords.
The `debug ip sctp sndchunks` command provides the following information:

- Application send requests from the local SCTP peer
- Chunks being bundled and sent to the remote peer
- Processing of the selective acknowledgments (SACKs) from the remote peer, indicating which chunks were successfully received
- Chunks that are marked for retransmission

The `debug ip sctp sndchunks` command generates large amounts of data if there is any significant amount of traffic flowing. It should be used with extreme caution in live networks.

The following example shows output for the `debug ip sctp sndchunks` command for a case in which data chunks are being sent, with some of them marked for retransmission:

```
Router# debug ip sctp sndchunks
SCTP: Assoc 0: ApplSend, chunk: 0/10412/100/A23134F8 to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 5/10443/100/A23134F9 to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 5/10448/100/A231355C to 10.5.0.4
SCTP: Assoc 0: Set oldest chunk for dest 10.5.0.4 to TSN A23134F8
SCTP: Assoc 0: Bundling data, added 0/10412/100/A23134F8, outstanding 100
SCTP: Assoc 0: Bundling data, added 5/10443/100/A23134F9, outstanding 200
SCTP: Assoc 0: Bundling data, added 4/10545/100/A23134FA, outstanding 300
SCTP: Assoc 0: Bundling data, added 10/10371/100/A23134FB, outstanding 400
SCTP: Assoc 0: Bundling data, added 11/10382/100/A23134FC, outstanding 500
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A231350F, numFrags=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A2313510
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A2313527, numFrags=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A2313528
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A231353F, numFrags=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A2313540
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A2313557, numFrags=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A2313558
SCTP: Assoc 0: ApplSend, chunk: 10/10385/100/A23135BE to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 8/10230/100/A23135BF to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 5/10459/100/A23135C0 to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 4/10558/100/A23135C1 to 10.5.0.4
SCTP: Assoc 0: Set oldest chunk for dest 10.5.0.4 to TSN A231355C
SCTP: Assoc 0: Bundling data, added 5/10449/100/A231355D, outstanding 100
SCTP: Assoc 0: Bundling data, added 3/10490/100/A231355E, outstanding 200
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A23135A4, numFrags=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A23135A5
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A23135BC, numFrags=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A23135BD
```
The table below describes the significant fields shown in the display.

**Table 61: debug ip sctp sndchunks Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 / 10412 / 100 / A23134F8</td>
<td>Stream number / datagram sequence number / chunk length, in bytes / chunk transmission sequence number.</td>
</tr>
<tr>
<td>outstanding</td>
<td>Number of bytes outstanding to the specified destination address.</td>
</tr>
<tr>
<td>CumTSN</td>
<td>Cumulative transmission sequence number (TSN).</td>
</tr>
<tr>
<td>numFrags</td>
<td>Number of fragments sent.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip sctp statistics</td>
<td>Empties the buffer that holds SCTP statistics.</td>
</tr>
<tr>
<td>debug ip sctp congestion</td>
<td>Shows a list of all current SCTP associations.</td>
</tr>
<tr>
<td>show ip sctp association parameters</td>
<td>Shows the parameters configured for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp association statistics</td>
<td>Shows the current statistics for the association defined by the association identifier.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>show ip sctp errors</td>
<td>Shows error counts logged by SCTP.</td>
</tr>
<tr>
<td>show ip sctp instances</td>
<td>Shows all currently defined SCTP instances.</td>
</tr>
<tr>
<td>show ip sctp statistics</td>
<td>Shows overall statistics counts for SCTP.</td>
</tr>
<tr>
<td>show iua as</td>
<td>Shows information about the current condition of an application server.</td>
</tr>
<tr>
<td>show iua asp</td>
<td>Shows information about the current condition of an application server process.</td>
</tr>
</tbody>
</table>

**debug ip sctp state**

To show state transitions in the Stream Control Transmission Protocol (SCTP), use the `debug ip sctp state` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
download ip sctp state
no debug ip sctp state
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
No default behavior or values

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ip sctp state` command can be used to see if the current associations are stable or not. Because it generates output only on state transitions, it is safe to use in a live environment. It still should be used with caution, however, depending on the number of associations being handled by the system and the stability of the network.

The `debug ip sctp state` command is often used at the same time as the `debug ip sctp signal` command. Using the two commands together gives good insight into the stability of associations.

**Examples**

In the following example, a new association is requested and established. The peer then restarts the association and notes that the association failed and is being reestablished. The local peer then indicates that the association has failed because it has tried to retransmit the specified chunk more than the maximum number of times without success. As a result, the association fails (because of communication loss) and is terminated. The upper-layer protocol (ULP) requests that the association be attempted again, and this attempt succeeds. A shutdown is then received from the remote peer, and the local peer enters the shutdown acknowledge sent state, which is followed by the association being terminated. Again, another association attempt is made and succeeds.
Router# debug ip sctp signal
Router# debug ip sctp state

00:20:08: SCTP: Assoc 0: state CLOSED -> COOKIE_WAIT
00:20:15: SCTP: Assoc 0: state COOKIE_WAIT -> ESTABLISHED
00:21:03: SCTP: Assoc 0: Sent ASSOC_UP signal for CONFIGD_ASSOC
00:21:03: SCTP: Assoc 0: Restart rcvd from peer
00:21:03: SCTP: Assoc 0: Sent ASSOC_RESTART signal
00:21:04: SCTP: Assoc 0: chunk 62EA7F40 retransmitted more than max times, failing assoc
00:21:04: SCTP: Assoc 0: Sent ASSOC_FAILED signal, reason: SCTP_COMM_LOST
00:21:04: SCTP: Assoc 0: Sent ASSOC_TERMINATE signal
00:21:04: SCTP: Assoc 0: state ESTABLISHED -> CLOSED

<new assoc attempt>
00:21:04: SCTP: Assoc 0: state CLOSED -> COOKIE_WAIT
00:21:04: SCTP: Assoc 0: state COOKIE_WAIT -> COOKIE_ECHOED
00:21:04: SCTP: Assoc 0: state COOKIE_ECHOED -> ESTABLISHED
00:21:04: SCTP: Assoc 0: Sent ASSOC_UP signal for CONFIGD_ASSOC
00:21:04: SCTP: Assoc 0: Sent TERMINATE_PENDING signal
00:21:04: SCTP: Assoc 0: state ESTABLISHED -> SHUTDOWN_ACKSENT
00:21:04: SCTP: Assoc 0: Sent ASSOC_TERMINATE signal
00:21:04: SCTP: Assoc 0: state SHUTDOWN_ACKSENT -> CLOSED

<new assoc attempt>
00:21:04: SCTP: Assoc 0: state CLOSED -> COOKIE_WAIT
00:21:04: SCTP: Assoc 0: state COOKIE_WAIT -> COOKIE_ECHOED
00:21:04: SCTP: Assoc 0: state COOKIE_ECHOED -> ESTABLISHED
00:21:04: SCTP: Assoc 0: Sent ASSOC_UP signal for CONFIGD_ASSOC

The table below describes the significant fields shown in the display.

Table 62: debug ip sctp state Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLOSED -&gt; COOKIE_WAIT</td>
<td>SCTP endpoint sends initialization chunk and moves to the COOKIE_WAIT state to wait for acknowledgment and a state cookie from the remote endpoint.</td>
</tr>
<tr>
<td>COOKIE_WAIT -&gt; COOKIE_ECHOED</td>
<td>SCTP endpoint returns the state cookie to the remote endpoint and enters COOKIE_ECHOED state.</td>
</tr>
<tr>
<td>COOKIE_ECHOED -&gt; ESTABLISHED</td>
<td>SCTP endpoint enters ESTABLISHED state after receiving acknowledgment that the state cookie has been received by the remote endpoint.</td>
</tr>
<tr>
<td>ESTABLISHED -&gt; SHUTDOWN_ACKSENT</td>
<td>SCTP endpoint enters SHUTDOWN_ACKSENT state after receiving a shutdown message and sending a shutdown acknowledgment to the remote endpoint.</td>
</tr>
<tr>
<td>SHUTDOWN_ACKSENT -&gt; CLOSED</td>
<td>SCTP endpoint enters CLOSED state.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip sctp statistics</td>
<td>Empties the buffer that holds SCTP statistics.</td>
</tr>
<tr>
<td>debug ip sctp congestion</td>
<td>Shows a list of all current SCTP associations.</td>
</tr>
<tr>
<td>debug ip sctp signal</td>
<td>Shows signals that are sent from SCTP to the application or ULP.</td>
</tr>
</tbody>
</table>
**debug ip sctp timer**

To provide information about Stream Control Transmission Protocol (SCTP) timers that are started, stopped, and triggering, use the **debug ip sctp timer** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip sctp timer
no debug ip sctp timer
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Many SCTP timers should not be restarted after they have been started once. For these timers, the first call succeeds in starting the timer, and subsequent calls do nothing until the timer either expires or is stopped. For example, the retransmission timer is started when the first chunk is sent, but then is not started again for subsequent chunks when there is outstanding data.

**Caution**

The **debug ip sctp timer** command generates a significant amount of output. It should be used with extreme caution in a live network.
The following example shows the starting and stopping of various SCTP timers:

```
Router# debug ip sctp timer
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Timer BUNDLE triggered
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timers already started, not restarting
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUMSACK</td>
<td>Cumulative selective acknowledgment.</td>
</tr>
<tr>
<td>RETRANS</td>
<td>Retransmission.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip sctp statistics</td>
<td>Empties the buffer that holds SCTP statistics.</td>
</tr>
<tr>
<td>debug ip sctp congestion</td>
<td>Shows a list of all current SCTP associations.</td>
</tr>
<tr>
<td>show ip sctp association parameters</td>
<td>Shows the parameters configured for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp association statistics</td>
<td>Shows the current statistics for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp errors</td>
<td>Shows error counts logged by SCTP.</td>
</tr>
</tbody>
</table>
### debug ip sctp warnings

To display diagnostic information about unusual situations in Stream Control Transmission Protocol (SCTP), use the `debug ip sctp warnings` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

In a live system, the debugging messages for performance, state, signal, and warnings are the most useful. They show any association or destination address failures and can be used to monitor the stability of established associations.

The `debug ip sctp warnings` command displays information on any unusual situation that is encountered. These situations may or may not indicate problems, depending on the particulars of the situation.

**Examples**

The following example shows some events and conditions that are flagged as warnings:

```
Router# debug ip sctp warnings
SCTP: Assoc 0: No cookie in InitAck, discarding
SCTP: Assoc 0: Incoming INIT_ACK: inbound streams reqd 15, allowed 13
SCTP: Assoc 0: Incoming INIT_ACK request: outbound streams req'd 13, allowed 1
SCTP: Assoc 0: Remote verification tag in init ack is zero, discarding
SCTP: Remote verification tag in init is zero, discarding
SCTP: Assoc 0: Rwnd less than min allowed (1500) in incoming INITACK, rcvd 0
SCTP: Assoc 0: Rwnd less than min allowed (1500) in incoming INITACK, rcvd 1499
SCTP: Rwnd in INIT too small (0), discarding
SCTP: Rwnd in INIT too small (1499), discarding
SCTP: Unknown INIT param 16537 (0x4099), length 8
```
SCTP: Assoc 0: Unknown INITACK param 153 (0x99), length 8
SCTP: Assoc 0: No cookie in InitAck, discarding
SCTP: Assoc 0: No cookie in InitAck, discarding
SCTP: Processing INIT, invalid param len 0, discarding...
SCTP: Assoc 0: Processing INITACK, invalid param len 0, discarding...

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip sctp statistics</td>
<td>Empties the buffer that holds SCTP statistics.</td>
</tr>
<tr>
<td>debug ip sctp congestion</td>
<td>Shows a list of all current SCTP associations.</td>
</tr>
<tr>
<td>show ip sctp association parameters</td>
<td>Shows the parameters configured for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp association statistics</td>
<td>Shows the current statistics for the association defined by the association identifier.</td>
</tr>
<tr>
<td>show ip sctp errors</td>
<td>Shows error counts logged by SCTP.</td>
</tr>
<tr>
<td>show ip sctp instances</td>
<td>Shows all currently defined SCTP instances.</td>
</tr>
<tr>
<td>show ip sctp statistics</td>
<td>Shows overall statistics counts for SCTP.</td>
</tr>
<tr>
<td>show iua as</td>
<td>Shows information about the current condition of an application server.</td>
</tr>
<tr>
<td>show iua asp</td>
<td>Shows information about the current condition of an application server process.</td>
</tr>
</tbody>
</table>

### debug ip sd

To display all session directory (SD) announcements received, use the `debug ip sd` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip sd
no debug ip sd
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

This command shows session directory announcements for multicast IP. Use it to observe multicast activity.

**Examples**

The following is sample output from the `debug ip sd` command:

```
Router# debug ip sd
SD: Announcement from 172.16.58.81 on Serial0.1, 146 bytes
s=cisco: CBONE Audio
i=cisco internal-only audio conference
o=dino@dino-ss20.cisco.com
```
The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD</td>
<td>Session directory event.</td>
</tr>
<tr>
<td>Announcement from</td>
<td>Address sending the SD announcement.</td>
</tr>
<tr>
<td>on Serial0.1</td>
<td>Interface receiving the announcement.</td>
</tr>
<tr>
<td>146 bytes</td>
<td>Size of the announcement event.</td>
</tr>
<tr>
<td>s=</td>
<td>Session name being advertised.</td>
</tr>
<tr>
<td>i=</td>
<td>Information providing a descriptive name for the session.</td>
</tr>
<tr>
<td>o=</td>
<td>Origin of the session, either an IP address or a name.</td>
</tr>
<tr>
<td>c=</td>
<td>Connect description showing address and number of hops.</td>
</tr>
<tr>
<td>m=</td>
<td>Media description that includes media type, port number, and ID.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip dvmrp</td>
<td>Displays information on DVMRP packets received and sent.</td>
</tr>
<tr>
<td>debug ip igmp</td>
<td>Displays IGMP packets received and sent, and IGMP host-related events.</td>
</tr>
<tr>
<td>debug ip mbgp dampening</td>
<td>Logs route flap dampening activity related to MBGP.</td>
</tr>
<tr>
<td>debug ip mrouting</td>
<td>Displays changes to the IP multicast routing table.</td>
</tr>
<tr>
<td>debug ip pim</td>
<td>Displays PIM packets received and sent, and PIM-related events.</td>
</tr>
</tbody>
</table>

**debug ip sdee**

To enable debugging messages for Security Device Event Exchange (SDEE) notification events, use the `debug ip sdee` command in privileged EXEC mode. To disable SDEE debugging messages, use the `no` form of this command.

```
debug ip sdee [alerts] [detail] [messages] [requests] [subscriptions]
no debug ip sdee [alerts] [detail] [messages] [requests] [subscriptions]
```
### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alerts</td>
<td>Displays new alerts that are reported to SDEE from IPS.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays detailed SDEE messages.</td>
</tr>
<tr>
<td>messages</td>
<td>Displays error and status messages that are reported to SDEE from IPS.</td>
</tr>
<tr>
<td>requests</td>
<td>Displays SDEE client requests.</td>
</tr>
<tr>
<td>subscriptions</td>
<td>Displays SDEE client subscription requests.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample SDEE debug output. In this example, you can see which messages correspond to SDEE alerts, requests, and subscriptions.

```
Router# debug ip sdee alerts requests subscriptions
5d00h:SDEE:got request from client at 10.0.0.2
5d00h:SDEE:reported 13 events for client at 10.0.0.2
5d00h:SDEE:GET request for client 10.0.0.2 subscription IDS1720:0
5d00h:SDEE:reported 50 events for client 10.0.0.2 subscription IDS1720:0
5d00h: SDEE alert:sigid 2004 name ICMP Echo Req from 10.0.0.2 time 1021174067
5d00h: SDEE alert:sigid 2004 name ICMP Echo Req from 10.0.0.2 time 1021174071
5d00h: SDEE alert:sigid 2004 name ICMP Echo Req from 10.0.0.2 time 1021174072
5d00h:SDEE:missed events for IDS1720:0
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ips notify</td>
<td>Specifies the method of event notification.</td>
</tr>
<tr>
<td>ip sdee events</td>
<td>Sets the maximum number of SDEE events that can be stored in the event buffer.</td>
</tr>
<tr>
<td>ip sdee subscriptions</td>
<td>Sets the maximum number of SDEE subscriptions that can be open simultaneously.</td>
</tr>
</tbody>
</table>

### debug ip security

To display IP security option processing, use the `debug ip security` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
default ip security
no debug ip security
```
Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Usage Guidelines

The **debug ip security** command displays information for both basic and extended IP security options. For interfaces where **ip security** is configured, each IP packet processed for that interface results in debugging output regardless of whether the packet contains IP security options. IP packets processed for other interfaces that also contain IP security information also trigger debugging output. Some additional IP security debugging information is also controlled by the **debug ip packet** command in privileged EXEC mode.

Caution

Because the **debug ip security** command generates a substantial amount of output for every IP packet processed, use it only when traffic on the IP network is low, so other activity on the system is not adversely affected.

Examples

The following is sample output from the **debug ip security** command:

```
Router# debug ip security
IP Security: src 172.24.72.52 dst 172.24.72.53, number of BSO 1
  idb: NULL
  pak: insert (0xFF) 0x0
IP Security: BSO postroute: SECINSERT changed to secret (0x5A) 0x10
IP Security: src 172.24.72.53 dst 172.24.72.52, number of BSO 1
  idb: secret (0x6) 0x10 to secret (0x6) 0x10, no implicit def secret (0x6) 0x10
  pak: secret (0x5A) 0x10
IP Security: checking BSO 0x10 against [0x10 0x10]
IP Security: classified BSO as secret (0x5A) 0x10
```

The table below describes significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number of BSO</td>
<td>Indicates the number of basic security options found in the packet.</td>
</tr>
<tr>
<td>idb</td>
<td>Provides information on the security configuration for the incoming interface.</td>
</tr>
<tr>
<td>pak</td>
<td>Provides information on the security classification of the incoming packet.</td>
</tr>
<tr>
<td>src</td>
<td>Indicates the source IP address.</td>
</tr>
<tr>
<td>dst</td>
<td>Indicates the destination IP address.</td>
</tr>
</tbody>
</table>

The following line indicates that the packet was locally generated, and it has been classified with the internally significant security level “insert” (0xff) and authority information of 0x0:

```
idb: NULL
pak: insert (0xff) 0x0
```

The following line indicates that the packet was received via an interface with dedicated IP security configured. Specifically, the interface is configured at security level “secret” and with authority
debug ip sla error

To enable debugging output of Cisco IOS IP Service Level Agreements (SLAs) operation run-time errors, use the `debug ip sla error` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip sla error [{operation-number | ep-api | event-publisher}]
no debug ip sla error [{operation-number | ep-api | event-publisher}]
```

**Syntax Description**

- `operation-number` (Optional) Identification number of the operation for which debugging output is to be enabled.
- `ep-api` (Optional) Enables IP SLAs Event Publisher application programming interface (API) debug messages.
- `event-publisher` (Optional) Enables IP SLAs Event Publisher debug messages.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(4)T</td>
<td>This command was introduced. This command replaces the <code>debug ip sla monitor error</code> command.</td>
</tr>
<tr>
<td>12.0(32)SY</td>
<td>This command was integrated into Cisco IOS Release 12.0(32)SY.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the <code>debug rtr error</code> command.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the <code>debug ip sla monitor error</code> command.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the <code>debug ip sla monitor error</code> command.</td>
</tr>
<tr>
<td>12.4(22)T</td>
<td>This command was modified. The <code>ep-api</code> and <code>event-publisher</code> keywords were added.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was modified. The <code>ep-api</code> and <code>event-publisher</code> keywords were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ip sla error operation-number` command displays run-time errors. When an operation number other than 0 is specified, all run-time errors for that operation are displayed when the operation is active. When the operation number is 0, all run-time errors relating to the IP SLAs scheduler process are displayed. When

Information of 0x0. The packet itself was classified at level “secret” (0x5a) and authority information of 0x10.

idb: secret (0x6) 0x10 to secret (0x6) 0x10, no implicit
def secret (0x6) 0x10
pak: secret (0x5a) 0x10
no operation number is specified, all run-time errors for all active operations configured on the router are displayed.

**Note**

Use the `debug ip sla error` command before using the `debug ip sla trace` command because the `debug ip sla error` command generates a lesser amount of debugging output.

The `debug ip sla error` command is supported in IPv4 networks. This command can also be used to enable debugging output for an IP SLAs operation that supports IPv6 addresses.

**Examples**

The following is sample output from the `debug ip sla error` command. The output indicates failure because the target is not there or because the responder is not enabled on the target.

```
Router# debug ip sla error
```

```
May 5 05:00:35.483: control message failure:1
May 5 05:01:35.003: control message failure:1
May 5 05:02:34.527: control message failure:1
May 5 05:03:34.039: control message failure:1
May 5 05:04:33.563: control message failure:1
May 5 05:05:33.099: control message failure:1
May 5 05:06:32.596: control message failure:1
May 5 05:07:32.119: control message failure:1
May 5 05:08:31.643: control message failure:1
May 5 05:09:31.167: control message failure:1
May 5 05:10:30.683: control message failure:1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ip sla trace</code></td>
<td>Traces the execution of an IP SLAs operation.</td>
</tr>
</tbody>
</table>

**debug ip sla ethernet-monitor**

To enable debugging output for a Cisco IOS IP Service Level Agreements (SLAs) Ethernet operation, use the `debug ip sla ethernet-monitor` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
dump ip sla ethernet-monitor [operation-number]
dump no ip sla ethernet-monitor [operation-number]
```

**Syntax Description**

| `operation-number` | (Optional) Number of the Ethernet operation for which the debugging output will be displayed. |

**Command Default**

Debugging activity for a Cisco IOS IP SLAs Ethernet operation does not occur.

**Command Modes**

Privileged EXEC (#)
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRB</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `debug ip sla ethernet-monitor` command:

```plaintext
Router# debug ip sla ethernet-monitor
00:00:15: IP SLAs Auto Ethernet(0):vlan = 2, domain = DOMAIN_OPERATOR_L3_1, mpid = 6322 from CFM
00:00:15: IP SLAs Auto Ethernet(0):saaHandleEventFromCFM::Received Event from CFM
00:00:15: IP SLAs Auto Ethernet(0):Event::ECFM_SAA_EV_MEP_ADD
00:00:15: IP SLAs Auto Ethernet(0):1 auto-probes found for domain = DOMAIN_OPERATOR_L3_1 and vlan = 2
00:00:15: IP SLAs Auto Ethernet(0):autoProbe probe_id = 1
00:00:15: IP SLAs Auto Ethernet(0):0 Probes already running in auto-probe = 1
00:00:15: IP SLAs Auto Ethernet(1):starting probe with freq = 20 sec
00:00:15: IP SLAs Auto Ethernet(1):starting probe 100001
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip sla</code></td>
<td>Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.</td>
</tr>
<tr>
<td><code>ip sla ethernet-monitor</code></td>
<td>Begins configuration for an IP SLAs auto Ethernet operation and enters IP SLA Ethernet monitor configuration mode.</td>
</tr>
</tbody>
</table>

### debug ip sla monitor error

**Note**

Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the `debug ip sla monitor error` command is replaced by the `debug ip sla error` command. See the `debug ip sla error` command for more information.

To enable debugging output of Cisco IOS IP Service Level Agreements (SLAs) operation run-time errors, use the `debug ip sla monitor error` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip sla monitor error [operation-number]
no debug ip sla monitor error [operation-number]
```

### Syntax Description

| `operation-number` (Optional) Identification number of the operation for which debugging output is to be enabled. |
### Command Modes

**Privileged EXEC**

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced. This command replaces the <code>debug rtr error</code> command.</td>
</tr>
<tr>
<td>12.4(4)T</td>
<td>This command was replaced by the <code>debug ip sla error</code> command.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was replaced by the <code>debug ip sla error</code> command.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was replaced by the <code>debug ip sla error</code> command.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `debug ip sla monitor error` command displays run-time errors. When an operation number other than 0 is specified, all run-time errors for that operation are displayed when the operation is active. When the operation number is 0, all run-time errors relating to the IP SLAs scheduler process are displayed. When no operation number is specified, all run-time errors for all active operations configured on the router are displayed.

#### Note

Use the `debug ip sla monitor error` command before using the `debug ip sla monitor trace` command because the `debug ip sla monitor error` command generates a lesser amount of debugging output.

### Examples

The following is sample output from the `debug ip sla monitor error` command. The output indicates failure because the target is not there or because the responder is not enabled on the target. All debugging output for IP SLAs (including the output from the `debug ip sla monitor trace` command) has the format shown in the table below.

```
Router# debug ip sla monitor error
May 5 05:00:35.483: control message failure:1
May 5 05:01:35.003: control message failure:1
May 5 05:02:34.527: control message failure:1
May 5 05:03:34.039: control message failure:1
May 5 05:04:33.563: control message failure:1
May 5 05:05:33.099: control message failure:1
May 5 05:06:32.596: control message failure:1
May 5 05:07:32.119: control message failure:1
May 5 05:08:31.643: control message failure:1
May 5 05:09:31.167: control message failure:1
May 5 05:10:30.683: control message failure:1
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP SLA Monitor 1</td>
<td>Number of the operation generating the message.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error Return Code</td>
<td>Message identifier indicating the error type (or error itself).</td>
</tr>
<tr>
<td>LU0 IP SLA Monitor Probe 1</td>
<td>Name of the process generating the message.</td>
</tr>
<tr>
<td>in echoTarget on call luReceive LuApiReturnCode of InvalidHandle - invalid host name or API handle</td>
<td>Supplemental messages that pertain to the message identifier.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip sla monitor trace</td>
<td>Traces the execution of an IP SLAs operation.</td>
</tr>
</tbody>
</table>

### debug ip sla monitor mpls-lsp-monitor

#### Note
Effective with Cisco IOS Release 12.2(33)SB, the debug ip sla monitor mpls-lsp-monitor command is replaced by the debug ip sla mpls-lsp-monitor command. See the debug ip sla mpls-lsp-monitor command for more information.

To enable debugging output for the IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor, use the debug ip sla monitor mpls-lsp-monitor command in privileged EXEC mode. To disable debugging output, use the no form of this command.

```
debug ip sla monitor mpls-lsp-monitor [operation-number]
no debug ip sla monitor mpls-lsp-monitor [operation-number]
```

#### Syntax Description

| operation-number | (Optional) Number of the LSP Health Monitor operation for which the debugging output will be displayed. |

#### Command Default
Debugging is disabled.

#### Command Modes
Privileged EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SB2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was replaced by the debug ip sla mpls-lsp-monitor command.</td>
</tr>
</tbody>
</table>

#### Examples
The following is sample output from the debug ip sla monitor mpls-lsp-monitor command:
Router# debug ip sla monitor mpls-lsp-monitor
IP SLA Monitor MPLSLM debugging for all entries is on
*Aug 19 19:59: IP SLA Monitor MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLA Monitor MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLA Monitor MPLSLM(1):Adding vrf red into tree entry 10.10.10.8
*Aug 19 19:59: IP SLA Monitor MPLSLM(1):Adding ProbeID 100005 to tree entry 10.10.10.8 (1)
*Aug 19 19:59: IP SLA Monitor MPLSLM(1):Adding vrf blue into tree entry 10.10.10.8
*Aug 19 19:59: IP SLA Monitor MPLSLM(1):Duplicate in AddQ 10.10.10.8
*Aug 19 19:59: IP SLA Monitor MPLSLM(1):Adding vrf green into tree entry 10.10.10.8
*Aug 19 19:59: IP SLA Monitor MPLSLM(1):Duplicate in AddQ 10.10.10.8
*Aug 19 19:59: IP SLA Monitor MPLSLM(1):Added Probe(s) 100005 will be scheduled after 26 secs over schedule period 60

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto ip sla mpls-lsp-monitor</td>
<td>Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.</td>
</tr>
</tbody>
</table>

**debug ip sla trace**

To trace the execution of a Cisco IOS IP Service Level Agreements (SLAs) operation, use the `debug ip sla trace` command in privileged EXEC mode. To disable trace debugging output, use the `no` form of this command.

```
debug ip sla trace [{operation-number | ep-api | event-publisher}]
no debug ip sla trace [{operation-number | ep-api | event-publisher}]
```

**Syntax Description**

- `operation-number` *(Optional)* Identification number of the operation for which debugging output is to be enabled.
- `ep-api` *(Optional)* Enables IP SLAs Event Publisher API debugging output.
- `event-publisher` *(Optional)* Enables IP SLAs Event Publisher debugging output.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(4)T</td>
<td>This command was introduced. This command replaces the <code>debug ip sla monitor trace</code> command.</td>
</tr>
<tr>
<td>12.0(32)SY</td>
<td>This command was integrated into Cisco IOS Release 12.0(32)SY.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the <code>debug rtr trace</code> command.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the <code>debug ip sla monitor trace</code> command.</td>
</tr>
</tbody>
</table>
This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the debug ip sla monitor trace command.

This command was modified. The ap-api and event-publisher keywords were added.

This command was modified. The ep-api and event-publisher keywords were added.

### Usage Guidelines

The `debug ip sla trace operation-number` command traces the execution of an IP SLAs operation. When an operation number other than 0 is specified, execution for that operation is traced. When the operation number is 0, the IP SLAs scheduler process is traced. When no operation number is specified, all active operations are traced.

The `debug ip sla trace` command also enables the `debug ip sla error` command for the specified operation. However, the `no debug ip sla trace` command does not disable the `debug ip sla error` command. You must manually disable the command by using the `no debug ip sla error` command.

All debugging output (including `debug ip sla error` command output) has the format shown in the `debug ip sla trace` command output example.

### Note

The `debug ip sla trace` command can generate a large number of debug messages. First use the `debug ip sla error` command, and then use the `debug ip sla trace` on a per-operation basis.

### Examples

The following is sample output from the `debug ip sla trace` command. In this example, an operation is traced through a single operation attempt: the setup of a connection to the target, and the attempt at an echo to calculate UDP packet response time.

```
Router# debug ip sla trace
May 5 05:25:08.584: rtt hash insert :3.0.0.3 3383
May 5 05:25:08.588: source=3.0.0.3(3383) dest-ip=5.0.0.1(9)
May 5 05:25:08.588: sending control msg:
May 5 05:25:08.588: Ver:1 ID:51 Len:52
May 5 05:25:08.592: cmd:command:RTT_CMD_UDP_PORT_ENABLE, ip:5.0.0.1, port:9, duration:5000
May 5 05:25:08.607: receiving reply
May 5 05:25:08.607: Ver:1 ID:51 Len:8
May 5 05:25:08.623: local delta:8
May 5 05:25:08.627: delta from responder:1
May 5 05:25:08.627: received <16> bytes and responseTime = 3 (ms)
May 5 05:25:08.631: rtt hash remove:3.0.0.3 3383
IP SLA Monitor 1:Starting An Echo Operation
- IP SLA Monitor Probe 1
May 5 05:26:08.104: rtt hash insert :3.0.0.3 2974
May 5 05:26:08.104: source=3.0.0.3(2974) dest-ip=5.0.0.1(9)
May 5 05:26:08.108: sending control msg:
May 5 05:26:08.108: Ver:1 ID:52 Len:52
May 5 05:26:08.112: cmd:command:RTT_CMD_UDP_PORT_ENABLE, ip:5.0.0.1, port:9, duration:5000
May 5 05:26:08.127: receiving reply
May 5 05:26:08.127: Ver:1 ID:52 Len:8
May 5 05:26:08.143: local delta:8
May 5 05:26:08.143: delta from responder:1
May 5 05:26:08.143: received <16> bytes and responseTime = 3 (ms)
```

Cisco IOS Debug Command Reference - Commands I through L
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip sla error</td>
<td>Enables debugging output of IP SLAs operation run-time errors.</td>
</tr>
</tbody>
</table>

**debug ip sla mpls-lsp-monitor**

Note: Effective with Cisco IOS Release 15.1(1)S, the `debug ip sla mpls-lsp-monitor` command was replaced by the `debug ip sla trace mpls-lsp-monitor` command. See the `debug ip sla trace mpls-lsp-monitor` command for more information.

To enable debugging output for the IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor, use the `debug ip sla mpls-lsp-monitor` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip sla mpls-lsp-monitor [operation-number]
no debug ip sla mpls-lsp-monitor [operation-number]
```

**Syntax Description**

| operation-number | (Optional) Number of the LSP Health Monitor operation for which the debugging output will be displayed. |

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(32)SY</td>
<td>This command was integrated into Cisco IOS Release 12.0(32)SY.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the <code>debug rtr mpls-lsp-monitor</code> command.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the <code>debug ip sla monitor mpls-lsp-monitor</code> command.</td>
</tr>
<tr>
<td>15.1(1)S</td>
<td>This command was replaced by the <code>debug ip sla trace mpls-lsp-monitor</code> command.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ip sla mpls-lsp-monitor` command:

```
Router# debug ip sla mpls-lsp-monitor
IP SLAs MPLSLM debugging for all entries is on
*Aug 19 19:59: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding vrf red into tree entry 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding Probe 100005
```
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding ProbeID 100005 to tree entry 10.10.10.8 (1)
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding vrf blue into tree entry 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Duplicate in AddQ 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding vrf green into tree entry 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Duplicate in AddQ 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Added Probe(s) 100005 will be scheduled after 26 secs over
schedule period 60

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip sla trace mpls-lsp-monitor</td>
<td>Traces the execution of an IP SLAs LSP Health Monitor operation.</td>
<td></td>
</tr>
</tbody>
</table>

**debug ip sla trace**

To trace the execution of a Cisco IOS IP Service Level Agreements (SLAs) operation, use the `debug ip sla trace` command in privileged EXEC mode. To disable trace debugging output, use the `no` form of this command.

```plaintext
debug ip sla trace [{operation-number | ep-api | event-publisher}]
no debug ip sla trace [{operation-number | ep-api | event-publisher}]
```

**Syntax Description**

- `operation-number` (Optional) Identification number of the operation for which debugging output is to be enabled.
- `ep-api` (Optional) Enables IP SLAs Event Publisher API debugging output.
- `event-publisher` (Optional) Enables IP SLAs Event Publisher debugging output.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(4)T</td>
<td>This command was introduced. This command replaces the <code>debug ip sla monitor trace</code> command.</td>
</tr>
<tr>
<td>12.0(32)SY</td>
<td>This command was integrated into Cisco IOS Release 12.0(32)SY.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the <code>debug rtr trace</code> command.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the <code>debug ip sla monitor trace</code> command.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the <code>debug ip sla monitor trace</code> command.</td>
</tr>
<tr>
<td>12.4(22)T</td>
<td>This command was modified. The <code>ap-api</code> and <code>event-publisher</code> keywords were added.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was modified. The <code>ep-api</code> and <code>event-publisher</code> keywords were added.</td>
</tr>
</tbody>
</table>
Usage Guidelines

The `debug ip sla trace operation-number` command traces the execution of an IP SLAs operation. When an operation number other than 0 is specified, execution for that operation is traced. When the operation number is 0, the IP SLAs scheduler process is traced. When no operation number is specified, all active operations are traced.

The `debug ip sla trace` command also enables the `debug ip sla error` command for the specified operation. However, the `no debug ip sla trace` command does not disable the `debug ip sla error` command. You must manually disable the command by using the `no debug ip sla error` command.

All debugging output (including `debug ip sla error` command output) has the format shown in the `debug ip sla error` command output example.

Note

The `debug ip sla trace` command can generate a large number of debug messages. First use the `debug ip sla error` command, and then use the `debug ip sla trace` on a per-operation basis.

Examples

The following is sample output from the `debug ip sla trace` command. In this example, an operation is traced through a single operation attempt: the setup of a connection to the target, and the attempt at an echo to calculate UDP packet response time.

```
Router# debug ip sla trace
May 5 05:25:08.584: rtt hash insert :3.0.0.3 3383
May 5 05:25:08.584: source=3.0.0.3(3383) dest-ip=5.0.0.1(9)
May 5 05:25:08.588: sending control msg:
May 5 05:25:08.588: Ver:1 ID:51 Len:52
May 5 05:25:08.607: receiving reply
May 5 05:25:08.607: Ver:1 ID:51 Len:8
May 5 05:25:08.623: local delta:8
May 5 05:25:08.627: delta from responder:1
May 5 05:25:08.627: received <16> bytes and responseTime = 3 (ms)
May 5 05:25:08.631: rtt hash remove:3.0.0.3 3383 IP SLA Monitor 1:Starting An Echo Operation
- IP SLA Monitor Probe 1
May 5 05:26:08.104: rtt hash insert :3.0.0.3 2974
May 5 05:26:08.104: source=3.0.0.3(2974) dest-ip=5.0.0.1(9)
May 5 05:26:08.108: sending control msg:
May 5 05:26:08.108: Ver:1 ID:52 Len:52
May 5 05:26:08.127: receiving reply
May 5 05:26:08.127: Ver:1 ID:52 Len:8
May 5 05:26:08.143: local delta:8
May 5 05:26:08.147: delta from responder:1
May 5 05:26:08.147: received <16> bytes and responseTime = 3 (ms)
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip sla error</td>
<td>Enables debugging output of IP SLAs operation run-time errors.</td>
</tr>
</tbody>
</table>
**debug ip sla trace mpls-lsp-monitor**

To trace the execution of an IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation, use the `debug ip sla trace mpls-lsp-monitor` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
deploy ip sla trace mpls-lsp-monitor [operation-number]
no debug ip sla mpls-lsp-monitor
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>operation-number</th>
<th>(Optional) Number of the LSP Health Monitor operation for which the debugging output will be displayed. The range is 0 to 2147483647.</th>
</tr>
</thead>
</table>

**Command Default**

Trace debugging of IP SLAs LSP Health Monitor operations is disabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)S</td>
<td>This command was introduced. This command replaces the <code>debug ip sla mpls-lsp-monitor</code> command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For Cisco IP SLAs Engine 3.0 in Cisco IOS Release 15.1(1)S, this command replaces the `debug ip sla mpls-lsp-monitor` command.

To determine the IP SLAs engine version, IP SLAs Engine 2.0 or 3.0, running on your Cisco router, use the `show ip application` command in privileged EXEC mode, as shown in the following example:

```
Router# show ip sla application
IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III
```

The `debug ip sla trace mpls-lsp-monitor` command traces the execution of IP SLAs LSP Health Monitor operations. When an operation number other than 0 is specified, execution for that operation is traced. When the operation number is 0, the IP SLAs scheduler process is traced. When no operation number is specified, all active LSP Health Monitor operations are traced.

This command also enables the `debug ip sla error` command for the specified operation. However, the `no debug ip sla trace mpls-lsp-monitor` command does not disable the `debug ip sla error` command. You must manually disable the command by using the `no debug ip sla error` command.

The `debug ip sla trace mpls-lsp-monitor` command can generate a large number of debug messages. To help reduce the number of debug messages, first use the `debug ip sla error` command and then use the `debug ip sla trace mpls-lsp-monitor` command on a per-operation basis.

**Examples**

The following is sample output from the `debug ip sla trace mpls-lsp-monitor` command:

```
Router# debug ip sla trace mpls-lsp-monitor
IP SLA Monitor MPLSLM debugging for all entries is on
*Aug 19 19:59: IP SLA Monitor MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLA Monitor MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLA Monitor MPLSLM(1):Next hop 10.10.10.8 added in AddQ
```
**Aug 19 19:59:** IP SLA Monitor MPLSLM(1): Adding vrf red into tree entry 10.10.10.8

**Aug 19 19:59:** IP SLA Monitor MPLSLM(1): Adding Probe 100005

**Aug 19 19:59:** IP SLA Monitor MPLSLM(1): Adding ProbeID 100005 to tree entry 10.10.10.8 (1)

**Aug 19 19:59:** IP SLA Monitor MPLSLM(1): Adding vrf blue into tree entry 10.10.10.8

**Aug 19 19:59:** IP SLA Monitor MPLSLM(1): Adding vrf green into tree entry 10.10.10.8

**Aug 19 19:59:** IP SLA Monitor MPLSLM(1): Duplicate in AddQ 10.10.10.8

**Aug 19 19:59:** IP SLA Monitor MPLSLM(1): Added Probe(s) 100005 will be scheduled after 26 secs over schedule period 60

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>debug ip sla error</strong></td>
<td>Enables debugging output of Cisco IOS IP SLAs operation run-time errors.</td>
</tr>
<tr>
<td><strong>debug ip sla mpls-lsp-monitor</strong></td>
<td>Enables debugging output for Cisco IOS IP SLAs LSP Health Monitor operations in IP SLAs Engine 2.0.</td>
</tr>
<tr>
<td><strong>show ip application</strong></td>
<td>Displays global information about Cisco IOS IP SLAs.</td>
</tr>
</tbody>
</table>

**debug ip sla trace twamp**

To enable debugging output of Cisco IOS IP Service Level Agreements (SLAs) operation for Two-Way Active Measurement Protocol (TWAMP), use the `debug ip sla trace twamp` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip sla trace twamp {connection [source-ip ip-address] | control {reflector | server} | session [source-ip ip-address]}
no debug ip sla trace twamp {connection [source-ip ip-address] | control {reflector | server} | session [source-ip ip-address]}
```

**Syntax Description**

- **connection**
  - Displays communication messages between an IP SLAs TWAMP client and server.
- **source-ip ip-address**
  - (Optional) Debug IP Performance Metrics (IPPM) TWAMP connections for the specified source. Specify the source using the IP address of the client device.
- **control**
  - Displays communication messages between the IP SLAs TWAMP server and reflector.
- **reflector**
  - Displays communication messages sent by an IP SLAs TWAMP reflector to the TWAMP server.
- **server**
  - Displays communication messages sent by an IP SLAs TWAMP server to the TWAMP reflector.
- **session**
  - Displays communication messages between an IP SLAs TWAMP sender and reflector.
debug ip rtp header-compression through debug ipv6 icmp

display ip slb

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(52)SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the `debug ip sla trace twamp` command to display communication messages between the client and server during a TWAMP session.

**Note**

Use the `debug ip sla error twamp connection` command before using the `debug ip sla trace twamp connection` command because the `debug ip sla error twamp connection` command generates less debugging output.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip sla error twamp</td>
<td>Displays exceptions during communication between the IP SLAs TWAMP client and server.</td>
</tr>
</tbody>
</table>

debug ip slb

To display debugging messages for the Cisco IOS Server Load Balancing (SLB) feature, use the `debug ip slb` command in user EXEC or privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
display ip slb \{all | asn [msid] | conns [acl-number] | dfp | firewallfarm | fragments | gtp | icmp | kal-ap | natpool | probe | reals | replication | route | sessions \{[asn | gtp | ipmobile | radius\} \} | sticky gtp imsi \|vservers\} 
no display ip slb \{all | asn [msid] | conns [acl-number] | dfp | firewallfarm | fragments | gtp | icmp | kal-ap | natpool | probe | reals | replication | route | sessions \{[asn | gtp | ipmobile | radius\} \} | sticky gtp imsi \|vservers\} 
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all debugging messages for Cisco IOS SLB.</td>
</tr>
<tr>
<td>asn</td>
<td>Displays debugging messages related to Access Service Network (ASN) load balancing.</td>
</tr>
<tr>
<td>msid</td>
<td>(Optional) Displays debugging messages related to the ASN Mobile Station ID (MSID) sticky database.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **conns acl-number** | Displays debugging messages for all connections being handled by IOS SLB, including Wireless Session Protocol (WSP) events and states. The optional `acl-number` argument references an IP access control list (ACL). This argument limits the information displayed based on the client IP address, real server IP address, or virtual server IP address:  
  - For simple ACLs, IOS SLB checks the client IP address.  
  - For extended ACLs, IOS SLB checks the client real and virtual IP addresses.  
  For more information about ACLs, refer to the “Configuring IP Services” chapter of the *Cisco IOS IP Configuration Guide*, Release 12.2. |
| **dfp** | Displays debugging messages for Dynamic Feedback Protocol (DFP).  
  - To display debugging messages for the DFP agent subsystem, use the `debug ip dfp agent` command.  
  - To display debugging messages for the general packet radio service (GPRS) DFP weight calculation, use the `debug gprs dfp` command. |
| **firewallfarm** | Displays debugging messages related to firewall load balancing. |
| **fragments** | Displays debugging messages related to the IOS SLB fragment database. |
| **gtp** | Displays all GPRS Tunneling Protocol (GTP)-related packet handler, gateway GPRS support node (GGSN), serving GPRS support node (SGSN), and Network Service Access Point Identifier (NSAPI) debugging messages for IOS SLB. |
| **icmp** | Displays all Internet Control Message Protocol debugging messages for IOS SLB. |
| **kal-ap** | Displays all KeepAlive Application Protocol (KAL-AP) debugging messages for IOS SLB. |
| **natpool** | Displays debugging messages related to the IOS SLB client Network Address Translation (NAT) pool. |
| **probe** | Displays debugging messages related to probes. |
| **reals** | Displays debugging messages for all real servers defined to IOS SLB. |
| **replication** | Displays debugging messages related to IOS SLB stateful backup virtual server. |
| **route** | Displays debugging messages for all routing handled by the IOS SLB RADIUS framed-IP sticky database. |
### debug ip rtp header-compression through debug ipv6 icmp

### debug ip slb

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>User EXEC or privileged EXEC (#)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.0(7)XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.1(5)T</td>
<td>This command was integrated into Cisco IOS Release 12.1(5)T.</td>
</tr>
<tr>
<td></td>
<td>12.2</td>
<td>This command was integrated into Cisco IOS Release 12.2.</td>
</tr>
<tr>
<td></td>
<td>12.1(2)E</td>
<td>The natpool and replication keywords were added.</td>
</tr>
<tr>
<td></td>
<td>12.1(3a)E</td>
<td>The firewallfarm keyword was added.</td>
</tr>
<tr>
<td></td>
<td>12.1(7)E</td>
<td>The vservers keyword was added.</td>
</tr>
<tr>
<td></td>
<td>12.1(9)E</td>
<td>The sessions keyword was added.</td>
</tr>
<tr>
<td></td>
<td>12.1(11b)E</td>
<td>The route keyword, the acl-number argument, and the radius option on the sessions keyword were added.</td>
</tr>
<tr>
<td></td>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td></td>
<td>12.1(13)E3</td>
<td>The gtp keyword and the gtp option on the sessions keyword were added.</td>
</tr>
<tr>
<td></td>
<td>12.2(14)ZA2</td>
<td>The ipmobile keyword was added.</td>
</tr>
<tr>
<td></td>
<td>12.2(18)SXE</td>
<td>The sticky gtp imsi keywords were added.</td>
</tr>
<tr>
<td></td>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRC</td>
<td>The kal-ap keyword was added.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRC1</td>
<td>The asn keyword and the asnoption on the sessions keyword were added.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sessions [asn] gtp</td>
<td>Displays debugging messages for all sessions being handled by IOS SLB.</td>
</tr>
<tr>
<td>ipmobile</td>
<td>• The optional asn keyword enables users to limit the information displayed to only ASN sessions.</td>
</tr>
<tr>
<td>radius</td>
<td>• The optional gtp keyword enables users to limit the information displayed to only GTP sessions.</td>
</tr>
<tr>
<td></td>
<td>• The optional ipmobile keyword enables users to limit the information displayed to only Mobile IP sessions.</td>
</tr>
<tr>
<td></td>
<td>• The optional radius keyword enables users to limit the information displayed to only RADIUS sessions.</td>
</tr>
<tr>
<td>sticky gtp imsi</td>
<td>Displays all debugging messages related to the IOS SLB GTP International Mobile Subscriber ID (IMSI) sticky database.</td>
</tr>
<tr>
<td>vservers</td>
<td>Displays debugging messages for all virtual servers defined to IOS SLB.</td>
</tr>
</tbody>
</table>
**Modification**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRE</td>
<td>The <strong>msid</strong> option on the <strong>asn</strong> keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays debugging messages for IOS SLB.

See the following caution before using debug commands:

⚠️ **Caution**

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network flows and fewer users. Debugging during these periods reduces the effect these commands have on other users on the system.

**Examples**

The following example configures a debugging session to check all IP IOS SLB parameters:

```bash
Router# **debug ip slb all**
SLB All debugging is on
Router#
```

The following example stops all debugging:

```bash
Router# **no debug all**
All possible debugging has been turned off
Router#
```

The following example configures debugging to check IP IOS SLB replication used with stateful backup and displays the output from the send or transmit virtual server:

```bash
Router# **debug ip slb replication**
*Mar  2 08:02:38.019: SLB Replicate: (send) update vs: VS1 update_count 42
```

The following example shows Cisco IOS SLB DFP debug output:

```bash
Router# **debug ip slb dfp**
SLB DFP debugging is on
router#
022048 SLB DFP Queue to main queue - type 2 for Agent 161.44.2.3458229
022048 SLB DFP select_rc = -1  readset = 0
022048 SLB DFP  Sleeping...
022049 SLB DFP  readset = 0
022049 SLB DFP select_rc = -1  readset = 0
022049 SLB DFP Processing Q event for Agent 161.44.2.3458229 - OPEN
022049 SLB DFP Queue to conn_proc_q - type 2 for Agent 161.44.2.3458229
022049 SLB DFP  readset = 0
022049 SLB DFP Set SLB_DFP_SIDE_QUEUE
022049 SLB DFP Processing Conn Q event for Agent 161.44.2.3458229 - OPEN
022049 SLB DFP Open to Agent 161.44.2.3458229 succeeded, socket = 0
022049 SLB DFP Agent 161.44.2.3458229 start connect
022049 SLB DFP Connect to Agent 161.44.2.3458229 successful - socket 0
022049 SLB DFP Queue to main queue - type 6 for Agent 161.44.2.3458229
022049 SLB DFP Processing Conn Q unknown MAJOR 80
022049 SLB DFP Reset SLB_DFP_SIDE_QUEUE
022049 SLB DFP  select_rc = -1  readset = 0
022049 SLB DFP  Sleeping...
```
debug ip snat

To display information about IP packets translated by the IP stateful network address translation (SNAT) feature, use the **debug ip snat** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ip snat [detailed]**

**no debug ip snat [detailed]**

**Syntax Description**

| detailed | (Optional) Displays debug information in a detailed format. |

**Command Default**

Disabled

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
The **SNAT** feature allows two or more network address translators to function as a translation group. One member of the translation group handles traffic requiring translation of IP address information. It informs the backup translator of active flows as they occur. The backup translator can then use information from the active translator to prepare duplicate translation table entries enabling the backup translator to become the active translator in the event of a critical failure. Traffic continues to flow without interruption because the same network address translations are used and the state of those translations has been previously defined.

Because the **debug ip snat** command generates a significant amount of output, use it only when traffic on the IP network is low, so other activity on the system is not adversely affected.

The following is sample output from the **debug ip snat** command:

```
Router# debug ip snat detailed
2w6d:SNAT:Establish TCP peers for PRIMARY
2w6d:SNAT (Send):Enqueuing SYNC Message for Router-Id 100
2w6d:SNAT(write2net):192.168.123.2 <--> 192.168.123.3 send message
2w6d:SNAT(write2net):ver 2, id 100, opcode 1, len 68
2w6d:SNAT (Send):Enqueuing DUMP-REQUEST Message for Router-Id 100
2w6d:SNAT(write2net):192.168.123.2 <--> 192.168.123.3 send message
2w6d:SNAT(write2net):ver 2, id 100, opcode 6, len 68
2w6d:SNAT (readfromnet):Enqueuing SYNC Message msg to readQ
2w6d:SNAT (Receive):Processed SYNC Message from Router-Id:0 for Router-Id:200's entry/entries
2w6d:SNAT (readfromnet):Enqueuing DUMP-REQUEST Message msg to readQ
2w6d:SNAT (sense):Send SYNC message
2w6d:SNAT (Send):Enqueuing SYNC Message for Router-Id 100
2w6d:SNAT(write2net):192.168.123.2 <--> 192.168.123.3 send message
2w6d:SNAT(write2net):ver 2, id 100, opcode 1, len 68
2w6d:SNAT (readfromnet):Enqueuing SYNC Message msg to readQ
2w6d:SNAT (Receive):Processed SYNC Message from Router-Id:200 for Router-Id:200's
entry/entries
```

The table below describes the significant fields shown in the display.

**Table 67: debug ip snat Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNAT:</td>
<td>Indicates that the packet is being translated by the SNAT feature.</td>
</tr>
<tr>
<td>DUMP-REQUEST Message</td>
<td>Requests for entries after the SNAT router is active.</td>
</tr>
</tbody>
</table>

**debug ip socket**

To display all state change information for all sockets, use the **debug ip socket** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
depg ip socket
no debug ip socket
```

**Syntax Description**

This command has no arguments or keywords.
**Command Modes**

Privileged EXEC

**Usage Guidelines**

Use this command to collect information on the socket interface. To get more complete information on a socket/TCP port pair, use this command in conjunction with the `debug ip tcp transactions` command.

Because the socket debugging information is state-change oriented, you will not see the debugging message on a per-packet basis. However, if the connections normally have very short lives (few packet exchanges during the life cycle of a connection), then socket debugging could become expensive because of the state changes involved during connection setup and teardown.

**Examples**

The following is sample output from the `debug ip socket` output from a server process:

```
Router# debug ip socket
Added socket 0x60B86228 to process 40
SOCKET: set TCP property TCP_PID, socket 0x60B86228, TCB 0x60B85E38
Accepted new socket fd 1, TCB 0x60B85E38
Added socket 0x60B86798 to process 40
SOCKET: set TCP property TCP_PID, socket 0x60B86798, TCB 0x60B877C0
SOCKET: set TCP property TCP_BIT_NOTIFY, socket 0x60B86798, TCB 0x60B877C0
SOCKET: created new socket to TCP, fd 2, TCB 0x60B877C0
SOCKET: bound socket fd 2 to TCB 0x60B877C0
SOCKET: set TCP property TCP_WINDOW_SIZE, socket 0x60B86798, TCB 0x60B877C0
SOCKET: listen on socket fd 2, TCB 0x60B877C0
SOCKET: closing socket 0x60B86228, TCB 0x60B85E38
SOCKET: socket event process: socket 0x60B86228, TCB new state --> FINWAIT1
socket state: SS_DISCONNECTED SS_CANTSENDMORE SS_ISDISCONNECTING
SOCKET: Removed socket 0x60B86228 from process 40 socket list
```

The following is sample output from the `debug ip socket` command from a client process:

```
Router# debug ip socket
Added socket 0x60B70220 to process 2
SOCKET: set TCP property TCP_PID, socket 0x60B70220, TCB 0x60B6CFDC
SOCKET: set TCP property TCP_BIT_NOTIFY, socket 0x60B70220, TCB 0x60B6CFDC
SOCKET: created new socket to TCP, fd 0, TCB 0x60B6CFDC
SOCKET: socket event process: socket 0x60B70220, TCB new state --> SYNSENT
socket state: SS_CONNECTING
SOCKET: socket event process: socket 0x60B70220, TCB new state --> ESTAB
socket state: SS_CONNECTING
SOCKET: closing socket 0x60B70220, TCB 0x60B6CFDC
SOCKET: socket event process: socket 0x60B70220, TCB new state --> FINWAIT1
socket state: SS_DISCONNECTED SS_CANTSENDMORE SS_ISDISCONNECTING
SOCKET: Removed socket 0x60B70220 from process 2 socket list
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added socket 0x60B86228 process 40</td>
<td>New socket is opened for process 40.</td>
</tr>
<tr>
<td>SOCKET</td>
<td>Indicates that this is a SOCKET transaction.</td>
</tr>
<tr>
<td>set TCP property TCP_PID</td>
<td>Sets the process ID to the TCP associated with the socket.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>socket 0x60B86228, TCB 0x60B85E38</td>
<td>Address for the socket/TCP pair.</td>
</tr>
<tr>
<td>set TCP property TCP_BIT_NOTIFY</td>
<td>Sets the method for how the socket wants to be notified for an event.</td>
</tr>
<tr>
<td>created new socket to TCP, fd 2</td>
<td>Opened a new socket referenced by file descriptor 2 to TCP.</td>
</tr>
<tr>
<td>bound socket fd 2 to TCB</td>
<td>Bound the socket referenced by file descriptor 2 to TCP.</td>
</tr>
<tr>
<td>listen on socket fd 2</td>
<td>Indicates which file descriptor the application is listening to.</td>
</tr>
<tr>
<td>closing socket</td>
<td>Indicates that the socket is being closed.</td>
</tr>
<tr>
<td>socket event process</td>
<td>Processed a state change event occurred in the transport layer.</td>
</tr>
<tr>
<td>TCB new state --&gt; FINWAIT1</td>
<td>TCP state machine changed to FINWAIT1. (See the <code>debug ip tcp transaction</code> command for more information on TCP state machines.)</td>
</tr>
</tbody>
</table>
| socket state: SS_ISCONNECTED SS_CANTSENDMORE SS_ISDISCONNECTING | New SOCKET state flags after the transport event processing. This socket is still connected, but disconnecting is in progress, and it will not send more data to peer. Possible SOCKET state flags follow:  
- SS_NOFDREF  
  No file descriptor reference for this socket.  
- SS_ISCONNECTING  
  Socket connecting is in progress.  
- SS_ISBOUND  
  Socket is bound to TCP.  
- SS_ISCONNECTED  
  Socket is connected to peer.  
- SS_CANTSENDMORE  
  Can’t send more data to peer.  
- SS_CANTRCVMORE  
  Can’t receive more data from peer.  
- SS_ISDISCONNECTED  
  Socket is disconnected. Connection is fully closed. |
Connection is closed, and the socket is removed from the process socket list.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip tcp transactions</td>
<td>Displays information on significant TCP transactions such as state changes, retransmissions, and duplicate packets.</td>
</tr>
</tbody>
</table>

### debug ip ssh

To display debugging messages for Secure Shell (SSH), use the `debug ip ssh` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip ssh [detail | packet]
no debug ip ssh
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(Optional) Specifies SSH protocol, channel requests and information state changes.</td>
</tr>
<tr>
<td>packet</td>
<td>(Optional) Specifies information regarding the SSH packet.</td>
</tr>
</tbody>
</table>

#### Command Default

Debugging for SSH is not enabled.

#### Command Modes

Privileged EXEC (#)

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(1)T</td>
<td>This command was integrated into Cisco IOS Release 12.1T.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>The detail and packet keywords were added.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.4</td>
<td>This command was implemented on the Cisco ASR 1000 series routers.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

Use the `debug ip ssh` command to ensure normal operation of the SSH server.

#### Examples

The following example shows the SSH debugging output:

```
Router# debug ip ssh
00:53:46: SSH0: starting SSH control process
00:53:46: SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
00:53:46: SSH0: client version is - SSH-1.5-1.2.25
00:53:46: SSH0: SSH_SMSG_PUBLIC_KEY message sent
00:53:46: SSH0: SSH_CMSG_SESSION_KEY message received
00:53:47: SSH0: keys exchanged and encryption on
00:53:47: SSH0: authentication request for userid guest
```
The following example shows the SSH detail output:

```
Router# debug ip ssh detail
00:04:22: SSH0: starting SSH control process
00:04:22: SSH0: sent protocol version id SSH-1.99-Cisco-1.25
00:04:22: SSH0: protocol version id is - SSH-1.99-Cisco-1.25
00:04:22: SSH2 0: SSH2_MSG_KEXINIT sent
00:04:22: SSH2 0: SSH2_MSG_KEXINIT received
00:04:22: SSH2 0: expecting SSH2_MSG_KEXDH_INIT
00:04:22: SSH2 0: SSH2_MSG_KEXDH_INIT received
00:04:22: SSH2: kex_derive_keys complete
00:04:22: SSH2 0: SSH2_MSG_NEWKEYS sent
00:04:22: SSH2 0: waiting for SSH2_MSG_NEWKEYS
00:04:22: SSH2 0: SSH2_MSG_NEWKEYS received
00:04:24: SSH2 0: authentication successful for lab
00:04:24: SSH2 0: channel open request
00:04:24: SSH2 0: pty-req request
00:04:24: SSH2 0: setting TTY - requested: height 24, width 80; set: height 24, width 80
00:04:24: SSH2 0: shell request
00:04:24: SSH2 0: shell message received
00:04:24: SSH2 0: starting shell for vty
00:04:38: SSH0: Session terminated normally
```

The following example shows the SSH packet output:

```
Router# debug ip ssh packet
00:05:43: SSH2 0: send:packet of length 280 (length also includes padlen of 4)
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: input: total packet length of 280 bytes
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: input: padlength 4 bytes
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: input: total packet length of 144 bytes
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 136 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 136 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 16 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 136 bytes, maclen 0
00:05:43: SSH2 0: input: padlength 6 bytes
00:05:43: SSH2 0: signature length 143
00:05:43: SSH2 0: send:packet of length 448 (length also includes padlen of 7)
00:05:43: SSH2 0: send:packet of length 16 (length also includes padlen of 10)
00:05:43: SSH2 0: newkeys: mode 1
00:05:43: SSH2 0: ssh_receive: 16 bytes received
00:05:43: SSH2 0: input: total packet length of 16 bytes
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 8 bytes, maclen 0
00:05:43: SSH2 0: input: padlength 10 bytes
00:05:43: SSH2 0: newkeys: mode 0
00:05:43: SSH2 0: ssh_receive: 52 bytes received
00:05:43: SSH2 0: input: total packet length of 32 bytes
```
debug ip subscriber

To enable Intelligent Services Gateway (ISG) IP subscriber session debugging, use the `debug ip subscriber` command in privileged EXEC mode. To disable debugging, use the `no` form of this command.

```
ddebug ip subscriber {all | error | event | fsm | packet}
no debug ip subscriber {all | error | event | fsm | packet}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all debugging messages related to IP subscriber sessions.</td>
</tr>
<tr>
<td>error</td>
<td>Displays debugging messages about IP subscriber session errors.</td>
</tr>
<tr>
<td>event</td>
<td>Displays debugging messages about IP subscriber session events.</td>
</tr>
<tr>
<td>fsm</td>
<td>Displays debugging messages related to session state changes for IP subscriber sessions.</td>
</tr>
<tr>
<td>packet</td>
<td>Displays debugging messages related to IP subscriber session packets.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(31)SB2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.2</td>
<td>This command was integrated into Cisco IOS XE Release 2.2.</td>
</tr>
</tbody>
</table>

**Examples**

The following example show sample output for the `debug ip subscriber` command:

```
Router# debug ip subscriber packet
Packet debugs:
1d07h: IPSUB_DP: [Et0/0:I:CEF:0000.0000.0000.0002] Rx driver forwarded packet via les, return code = 0
1d07h: IPSUB_DP: [Et0/0:I:PROC:0000.0000.0000.0002] Packet classified, results = 0x18
1d07h: IPSUB_DP: [ms1:I:PROC:0000.0000.0000.0002] Rx driver forwarded the packet
1d07h: IPSUB_DP: [ms1:I:PROC:0000.0000.0000.0002] Packet classified, results = 0x42
1d07h: IPSUB_DP: [ms1:O:PROC:RED:50.0.0.3] Packet classified, results = 0x14
Router#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip subscriber</td>
<td>Displays information about ISG IP subscriber sessions.</td>
</tr>
</tbody>
</table>
**debug ip subscriber redundancy**

To enable Intelligent Service Gateway (ISG) IP subscriber session debugging on a Cisco 7600 router, use the `debug ip subscriber` command in privileged EXEC mode. To disable debugging, use the `no` form of this command.

```
debug ip subscriber redundancy
no debug ip subscriber redundancy
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRC</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows that the `debug ip subscriber redundancy` command is turned on:

```
Router# debug ip subscriber redundancy
IP subscriber redundancy debugging is on.
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip subscriber interface</td>
<td>Disconnects and removes all ISG IP subscriber sessions associated with a specific interface on a Cisco 7600 router.</td>
</tr>
<tr>
<td>clear ip subscriber slot</td>
<td>Disconnects and removes all ISG IP subscriber sessions associated with a specific hardware slot on a Cisco 7600 router.</td>
</tr>
<tr>
<td>show ip subscriber interface</td>
<td>Displays information about an ISG IP subscriber interface on a Cisco 7600 router.</td>
</tr>
<tr>
<td>show ip subscriber redundancy</td>
<td>Displays information about ISG IP subscriber sessions on a Cisco 7600 router.</td>
</tr>
<tr>
<td>show debugging</td>
<td>Displays information about the types of debugging that are enabled for your router.</td>
</tr>
</tbody>
</table>

**debug ip tcp congestion**

To display information about TCP congestion events, use the `debug ip tcp congestion` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip tcp congestion
no debug ip tcp congestion
```

**Syntax Description**

This command has no arguments or keywords.
Information from the New Reno congestion control algorithm is displayed.

Privileged EXEC (#)

This command was introduced.

The `debug ip tcp congestion` command can be used to debug a performance problem on a TCP/IP network that you have isolated above the data-link layer. It also displays information related to variation in TCP’s send window, congestion window, and congestion threshold window.

The following is sample output from the **debug ip tcp congestion** command:

```
Router# debug ip tcp congestion
*May 20 22:49:49.091: Setting New Reno as congestion control algorithm
*May 22 05:21:47.281: Advance cwnd by 12
*May 22 05:21:47.281: TCP85FD0C10: sndcwnd: 1472
*May 22 05:21:47.285: Advance cwnd by 3
*May 22 05:21:47.285: TCP85FD0C10: sndcwnd: 1475
*May 22 05:21:47.285: Advance cwnd by 3
*May 22 05:21:47.285: Advance cwnd by 9


For IOS TCP, New Reno is the default congestion control algorithm. However, an application can also use Binary Increase Congestion Control (BIC) as the congestion algorithm. The following is sample output from the **debug ip tcp congestion** command using the BIC congestion algorithm:

```
Router# debug ip tcp congestion
*May 22 05:21:42.281: Setting BIC as congestion control algorithm
*May 22 05:21:47.281: Advance cwnd by 12
*May 22 05:21:47.281: TCP85FD0C10: sndcwnd: 1472
*May 22 05:21:47.285: Advance cwnd by 3
*May 22 05:21:47.285: TCP85FD0C10: sndcwnd: 1475
*May 22 05:21:47.285: Advance cwnd by 3
*May 22 05:21:47.285: Advance cwnd by 9

The table below describes the significant fields shown in the display.

### Table 69: debug ip tcp congestion Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting New Reno as congestion control algorithm</td>
<td>TCP is using New Reno as the congestion control algorithm.</td>
</tr>
<tr>
<td>TCP85FD0C10</td>
<td>TCP’s control block identifier.</td>
</tr>
<tr>
<td>Advance cwnd</td>
<td>Increase in TCP’s congestion window.</td>
</tr>
<tr>
<td>sndcwnd</td>
<td>TCP’s send congestion window.</td>
</tr>
<tr>
<td>[New Reno]</td>
<td>Values reflected are those of TCP’s New Reno congestion control.</td>
</tr>
<tr>
<td>ssthresh:</td>
<td>TCP’s slow start threshold.</td>
</tr>
<tr>
<td>snd_mark</td>
<td>New value of one of New Reno’s parameters.</td>
</tr>
<tr>
<td>10.168.10.10:42416:</td>
<td>Local address and port number for the TCP connection.</td>
</tr>
<tr>
<td>10.168.30.11.49100:</td>
<td>Foreign address and port number for the TCP connection.</td>
</tr>
<tr>
<td>congestion window changes</td>
<td>Change in TCP’s send congestion window.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip tcp window-size</td>
<td>Alters the TCP window size.</td>
</tr>
</tbody>
</table>

### debug ip tcp driver

To display information on TCP driver events; for example, connections opening or closing, or packets being dropped because of full queues, use the **debug ip tcp driver** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
   debug ip tcp driver
   no debug ip tcp driver
```

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC

### Usage Guidelines

The TCP driver is the process that the router software uses to send packet data over a TCP connection. Remote source-route bridging (RSRB), serial tunneling (STUN), and X.25 switching currently use the TCP driver.
Using the **debug ip tcp driver** command together with the **debug ip tcp driver-pak** command provides the most verbose debugging output concerning TCP driver activity.

### Examples

The following is sample output from the **debug ip tcp driver** command:

```
Router# debug ip tcp driver
TCPDRV359CD8: Active open 172.21.80.26:0 --> 172.21.80.25:1996 OK, lport 36628
TCPDRV359CD8: enable tcp timeouts
```

The table below describes the significant fields shown in the display.

**Table 70: debug ip tcp driver Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCPDRV359CD8:</td>
<td>Unique identifier for this instance of TCP driver activity.</td>
</tr>
<tr>
<td>Active open 172.21.80.26</td>
<td>Indication that the router at IP address 172.21.80.26 has initiated a connection to another router.</td>
</tr>
<tr>
<td>:0</td>
<td>TCP port number the initiator of the connection uses to indicate that any port number can be used to set up a connection.</td>
</tr>
<tr>
<td>--&gt; 172.21.80.25</td>
<td>IP address of the remote router to which the connection has been initiated.</td>
</tr>
<tr>
<td>:1996</td>
<td>TCP port number that the initiator of the connection is requesting that the remote router use for the connection. (1996 is a private TCP port number reserved in this implementation for RSRB.)</td>
</tr>
<tr>
<td>OK,</td>
<td>Indication that the connection has been established. If the connection has not been established, this field and the following field do not appear in this line of output.</td>
</tr>
<tr>
<td>lport 36628</td>
<td>TCP port number that has actually been assigned for the initiator to use for this connection.</td>
</tr>
</tbody>
</table>

The following line indicates that the TCP driver user (RSRB, in this case) will allow TCP to drop the connection if excessive retransmissions occur:

```
TCPDRV359CD8: enable tcp timeouts
```

The following line indicates that the TCP driver user (in this case, RSRB) at IP address 172.21.80.26 (and using TCP port number 36628) is requesting that the connection to IP address 172.21.80.25 using TCP port number 1996 be aborted:

```
```

The following line indicates that this connection was in fact closed because of an abnormal termination:

```
```
**debug ip tcp driver-pak**

To display information on every operation that the TCP driver performs, use the `debug ip tcp driver-pak` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```plaintext
debug ip tcp driver-pak
no debug ip tcp driver-pak
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

This command turns on a verbose debugging by logging at least one debugging message for every packet sent or received on the TCP driver connection.

The TCP driver is the process that the router software uses to send packet data over a TCP connection. Remote source-rate bridging (RSRB), serial tunneling (STUN), and X.25 switching currently use the TCP driver.

To observe the context within which certain `debug ip tcp driver-pak` messages occur, turn on this command in conjunction with the `debug ip tcp driver` command.

**Caution**

Because the `debug ip tcp driver-pak` command generates so many messages, use it only on lightly loaded systems. This command not only places a substantial load on the system processor, it also may change the symptoms of any unexpected behavior that occurs.

**Examples**

The following is sample output from the `debug ip tcp driver-pak` command:

```plaintext
Router# debug ip tcp driver-pak
TCPDRV359CD8: send 2E8CD8 (len 26) queued
TCPDRV359CD8: output pak 2E8CD8 (len 26) (26)
TCPDRV359CD8: readf 42 bytes (Thresh 16)
TCPDRV359CD8: readf 26 bytes (Thresh 16)
TCPDRV359CD8: readf 10 bytes (Thresh 10)
TCPDRV359CD8: send 327E40 (len 4502) queued
TCPDRV359CD8: output pak 327E40 (len 4502) (4502)
```

The table below describes the significant fields shown in the display.

**Table 71: debug ip tcp driver-pak Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCPDRV359CD8</td>
<td>Unique identifier for this instance of TCP driver activity.</td>
</tr>
<tr>
<td>send</td>
<td>Indicates that this event involves the TCP driver sending data.</td>
</tr>
<tr>
<td>2E8CD8</td>
<td>Address in memory of the data the TCP driver is sending.</td>
</tr>
<tr>
<td>(len 26)</td>
<td>Length of the data (in bytes).</td>
</tr>
</tbody>
</table>
Indicates that the TCP driver user process (in this case, RSRB) has transferred the data to the TCP driver to send.

The following line indicates that the TCP driver has sent the data that it had received from the TCP driver user, as shown in the previous line of output. The last field in the line (26) indicates that the 26 bytes of data were sent out as a single unit.

TCPDRV359CD8: output pak 2E8CD8 (len 26) (26)

The following line indicates that the TCP driver has received 42 bytes of data from the remote IP address. The TCP driver user (in this case, remote source-route bridging) has established an input threshold of 16 bytes for this connection. (The input threshold instructs the TCP driver to transfer data to the TCP driver user only when at least 16 bytes are present.)

TCPDRV359CD8: readf 42 bytes (Thresh 16)

debug ip tcp ecn

To turn on debugging of the TCP Explicit Congestion Notification (ECN) capability, use the debug ip tcp ecn command in privileged EXEC mode. To turn off the debugging, use the no form of this command.

debug ip tcp ecn
no debug ip tcp ecn

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
</tbody>
</table>

Examples

The following example shows the messages that verify that the end hosts are connected and configured for ECN:

Router# debug ip tcp ecn
! TCP ECN debugging is on
! Router# telnet 10.1.25.31

Trying 10.1.25.31 ...
! 01:43:19: 10.1.25.35:11000 <--> 10.1.25.31:23 out ECN-setup SYN
Before a TCP connection can use ECN, a host sends an ECN-setup SYN (synchronization) packet to a remote end that contains an ECE and CWR bit set in the header. This indicates to the remote end that the sending TCP is ECN-capable, rather than an indication of congestion. The remote end sends an ECN-setup SYN-ACK (acknowledgment) packet to the sending host.

In the example above, the “out ECN-setup SYN” text means that a SYN packet with the ECE and CWR bit set was sent to the remote end. The “in non-ECN-setup SYN-ACK” text means that the remote end did not favorably acknowledge the ECN request and that therefore the session is ECN capable.

The following debug output shows that ECN capabilities are enabled at both ends. In response to the ECN-setup SYN, the other end favorably replied with an ECN-setup SYN-ACK message. This connection is now ECN capable for the rest of the session.

Router# telnet 10.10.10.10
Trying 10.10.10.10 ... Open
Password required, but none set
!
1d20h: 10.1.25.34:11003 <---> 10.1.25.35:23 out ECN-setup SYN
1d20h: 10.1.25.34:11003 <---> 10.1.25.35:23 in ECN-setup SYN-ACK

Use the show tcp tcb command to display the end-host connections.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip tcp ecn</td>
<td>Enables TCP ECN.</td>
</tr>
<tr>
<td>show tcp tcb</td>
<td>Displays the status of local and remote end hosts.</td>
</tr>
</tbody>
</table>

**Related Commands**

**debug ip tcp ha**

To display TCP high availability (HA) events or debugging information for TCP stack interactions between the active Route Processor (RP) and the standby RP, use the debug ip tcp ha command in privileged EXEC mode. To disable debugging output, use the no form of this command.

```
debug ip tcp ha {events | transactions} [detail]
no debug ip tcp ha {events | transactions} [detail]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>Displays TCP HA failures.</td>
</tr>
<tr>
<td>transactions</td>
<td>Displays failed TCP stack interactions between the active RP and standby RP.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed debugging information about successful TCP HA operations and useful informational messages or about successful TCP stack interactions between the active and standby RP.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(28)SB</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)S</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)S.</td>
</tr>
<tr>
<td>Cisco IOSXE 3.1S</td>
<td>This command was integrated into Cisco IOSXE Release 3.1S.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **debug ip tcp ha** command is used to display TCP stateful switchover (SSO) events or debugging information for TCP stack interactions between the active RP and the standby RP. This command is useful for troubleshooting SSO-aware TCP connections.

Use the **debug ip tcp ha** command with the **transactions** keyword to display failed TCP stack interactions between the active RP and standby RP. This form of the command displays failed TCP HA messages, RF redundancy-related client-application transactions, IPC client-application transactions, and In-Service Software Upgrade (ISSU) transactions.

Use the **debug ip tcp ha** command with the **transactions** and **detail** keywords to display successful TCP stack interactions between the active and standby RP. This form of the command displays successful TCP HA messages, RF redundancy-related client-application transactions, IPC client-application transactions, and ISSU transactions.

Use the **debug ip tcp ha** command with the **events** keyword to display TCP HA failures. This form of the command displays TCP HA failed encode or decode messages, system resources failures (such as memory allocation failures in the context of TCP HA), failed state changes, and failures that occur when SSO is enabled or disabled.

Use the **debug ip tcp ha** command with the **events** and **detail** keywords to display successful TCP HA operations and useful informational messages. This form of the command displays successful TCP encode or decode messages, state changes, and operations that occur when SSO is enabled or disabled.

### Examples

The following is sample output from the **debug ip tcp ha** command with the **transactions** and **detail** keywords. The following output shows packet flow from the active to the standby RP for an established TCP SSO connection:

*Feb 19 23:28:23.324: TCPHA: Sending pkt msg, conn_id = 396, seq no = 2959469308
*Feb 19 23:28:23.324: TCPHA: Sending pkt msg, conn_id = 41, seq no = 1270243395
*Feb 19 23:28:23.932: TCPHA: Sending pkt msg, conn_id = 42, seq no = 974255741
*Feb 19 23:28:23.932: TCPHA: Sending pkt msg, conn_id = 475, seq no = 3059612402
*Feb 19 23:28:24.544: TCPHA: Sending dummy pkt to standby; cid=109, size=19
*Feb 19 23:28:42.976: TCPHA: Recd IPC msg len 24, type 3
*Feb 19 23:28:42.976: TCPHA: Recd IPC msg len 24, type 3
*Feb 19 23:28:43.172: TCPHA: Recd IPC msg len 79, type

### debug ip tcp intercept

To display TCP intercept statistics, use the **debug ip tcp intercept** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ip tcp intercept**
no debug ip tcp intercept

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Examples

The following is sample output from the `debug ip tcp intercept` command:

Router# debug ip tcp intercept

A connection attempt arrives:

INTERCEPT: new connection (172.19.160.17:61774) -> (10.1.1.30:23)  

A second connection attempt arrives:

INTERCEPT: new connection (172.19.160.17:62030) -> (10.1.1.30:23)  

The router resends to both apparent clients:

INTERCEPT: retransmit 2 (172.19.160.17:61774) <- (10.1.1.30:23) SYNRCVD  
INTERCEPT: retransmit 2 (172.19.160.17:62030) <- (10.1.1.30:23) SYNRCVD

A third connection attempt arrives:

INTERCEPT: new connection (171.69.232.23:1048) -> (10.1.1.30:23)  
INTERCEPT: 171.69.232.23:1048 <- ACK+SYN (10.1.1.30:1048)

The router sends more retransmissions trying to establish connections with the apparent clients:

INTERCEPT: retransmit 4 (172.19.160.17:61774) <- (10.1.1.30:23) SYNRCVD  
INTERCEPT: retransmit 4 (172.19.160.17:62030) <- (10.1.1.30:23) SYNRCVD  
INTERCEPT: retransmit 2 (171.69.232.23:1048) <- (10.1.1.30:23) SYNRCVD

The router establishes the connection with the third client and resends to the server:

INTERCEPT: 1st half of connection is established (171.69.232.23:1048) -> (10.1.1.30:23)  
INTERCEPT: (171.69.232.23:1048) SYN -> 10.1.1.30:23  
INTERCEPT: retransmit 2 (171.69.232.23:1048) -> (10.1.1.30:23) SYNSENT

The server responds; the connection is established:

INTERCEPT: 2nd half of connection established (171.69.232.23:1048) -> (10.1.1.30:23)  
INTERCEPT: (171.69.232.23:1048) ACK -> 10.1.1.30:23

The router resends to the first two apparent clients, times out, and sends reset:

INTERCEPT: retransmit 8 (172.19.160.17:61774) <- (10.1.1.30:23) SYNRCVD  
INTERCEPT: retransmit 8 (172.19.160.17:62030) <- (10.1.1.30:23) SYNRCVD  
INTERCEPT: retransmit 16 (172.19.160.17:61774) <- (10.1.1.30:23) SYNRCVD  
INTERCEPT: retransmit 16 (172.19.160.17:62030) <- (10.1.1.30:23) SYNRCVD  
INTERCEPT: retransmitting too long (172.19.160.17:61774) -> (10.1.1.30:23) SYNRCD  
debug ip tcp packet

To enable debug messages for received and sent TCP packets, use the `debug ip tcp packet` command in privileged EXEC mode. To disable TCP packet debug messages, use the `no` form of this command.

```
debug ip tcp packet [{line-number | address ip-address | {aux | console | tty | vty} line-number | in | out | port port-number | slot/port | slot/subslot/port}]
no debug ip tcp packet [{line-number | address ip-address | {aux | console | tty | vty} line-number | in | out | port port-number | slot/port | slot/subslot/port}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>line-number</td>
<td>(Optional) Line number. Valid range is 0 to 710.</td>
</tr>
<tr>
<td>address ip-address</td>
<td>(Optional) Specifies the source or destination IP address.</td>
</tr>
<tr>
<td>aux line-number</td>
<td>(Optional) Specifies the auxiliary line.</td>
</tr>
<tr>
<td>console line-number</td>
<td>(Optional) Specifies the primary terminal line.</td>
</tr>
<tr>
<td>in</td>
<td>(Optional) Specifies the incoming segments.</td>
</tr>
<tr>
<td>out</td>
<td>(Optional) Specifies the outgoing segments.</td>
</tr>
<tr>
<td>port port-number</td>
<td>(Optional) Specifies the source or destination port number.</td>
</tr>
<tr>
<td>tty line-number</td>
<td>(Optional) Specifies the terminal controller.</td>
</tr>
<tr>
<td>vty line-number</td>
<td>(Optional) Specifies the virtual terminal.</td>
</tr>
<tr>
<td>slot / port</td>
<td>(Optional) Specifies the slot and port for modems. The slash mark is required.</td>
</tr>
<tr>
<td>slot / subslot / port</td>
<td>(Optional) Specifies the slot, subslot, and port for modems. The slash mark is required.</td>
</tr>
</tbody>
</table>

### Command Default

If no optional arguments or keywords are entered, this command displays all TCP packet debug messages.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `debug ip tcp packet` command:

```
Router# debug ip tcp packet
tcp0: I LISTEN 172.16.0.0:49620 172.16.0.1:80 seq 2116160325 OPTS 4 SYN WIN 1024
tcp0: O SYNRCVD 172.16.0.34:49620 172.16.0.1:80 seq 3992162775
```
debug ip tcp transactions

To display information on significant TCP transactions such as state changes, retransmissions, and duplicate packets, use the `debug ip tcp transactions` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

`debug ip tcp transactions`
`no debug ip tcp transactions`

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>The command output was enhanced to account for the following conditions: TCP entering Fast Recovery mode, duplicate acknowledgments being received during Fast Recovery mode, and partial acknowledgments being received.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is particularly useful for debugging a performance problem on a TCP/IP network that you have isolated above the data-link layer.

The `debug ip tcp transactions` command displays output for packets that the router sends and receives, but does not display output for packets that it forwards.

**Examples**

The following is sample output from the `debug ip tcp transactions` command:

```
Router# debug ip tcp transactions
TCP: sending SYN, seq 168108, ack 8865553
TCP0: Connection to 10.9.0.13:22530, advertising MSS 966
TCP0: state was LISTEN -> SYNRCVD [23 -> 10.9.0.13(22530)]
```
TCP0: state was SYNSENT -> SYNRCVD [23 -> 10.9.0.13(22530)]
TCP0: Connection to 10.9.0.13:22530, received MSS 956
TCP0: restart retransmission in 5996
TCP0: state was SYNRCVD -> ESTAB [23 -> 10.9.0.13(22530)]
TCP2: restart retransmission in 10689
TCP2: restart retransmission in 10633
TCP2: restart retransmission in 13384 -> 10.0.0.13(16151)]
TCP0: restart retransmission in 5996 [23 -> 10.0.0.13(16151)]

The following line from the `debug ip tcp transactions` command output shows that TCP has entered Fast Recovery mode:

```
fast re-transmit - sndcwnd - 512, snd_last - 33884268765
```

The following lines from the `debug ip tcp transactions` command output show that a duplicate acknowledgment is received when in Fast Recovery mode (first line) and a partial acknowledgment has been received (second line):

```
TCP0: ignoring second congestion in same window sndcwn - 512, snd_1st - 33884268765
TCP0: partial ACK received sndcwnd:338842495
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>Indicates that this is a TCP transaction.</td>
</tr>
<tr>
<td>sending SYN</td>
<td>Indicates that a synchronize packet is being sent.</td>
</tr>
<tr>
<td>seq 168108</td>
<td>Indicates the sequence number of the data being sent.</td>
</tr>
<tr>
<td>ack 88655553</td>
<td>Indicates the sequence number of the data being acknowledged.</td>
</tr>
<tr>
<td>TCP0</td>
<td>Indicates the TTY number (0, in this case) with which this TCP connection</td>
</tr>
<tr>
<td>Connection to</td>
<td>is associated.</td>
</tr>
<tr>
<td>10.9.0.13:22530</td>
<td>Indicates the remote address with which a connection has been established.</td>
</tr>
<tr>
<td>advertising MSS 966</td>
<td>Indicates the maximum segment size that this side of the TCP connection is</td>
</tr>
<tr>
<td></td>
<td>offering to the other side.</td>
</tr>
</tbody>
</table>
Indicates that the TCP state machine changed state from LISTEN to SYNRCVD. Possible TCP states that can follow are:

- CLOSED--Connection closed.
- CLOSEWAIT--Received a FIN segment.
- CLOSING--Received a FIN/ACK segment.
- ESTAB--Connection established.
- FINWAIT 1--Sent a FIN segment to start closing the connection.
- FINWAIT 2--Waiting for a FIN segment.
- LASTACK--Sent a FIN segment in response to a received FIN segment.
- LISTEN--Listening for a connection request.
- SYNRCVD--Received a SYN segment and responded.
- SYNSENT--Sent a SYN segment to start connection negotiation.
- TIMEWAIT--Waiting for the network to clear segments for this connection before the network no longer recognizes the connection as valid. This must occur before a new connection can be set up.

The elements within these brackets are as follows:

- The first field (23) indicates the local TCP port.
- The second field (10.9.0.13) indicates the destination IP address.
- The third field (22530) indicates the destination TCP port.

Indicates the number of milliseconds until the next retransmission takes place.

Indicates the size of the send congestion window.

Indicates the size of the last window.

### debug ip traffic-export events

To enable debugging messages for exported IP packet events, use the `debug ip traffic-export` command in privileged EXEC mode. To disable debugging messages, use the `no` form of this command.

#### Syntax Description

This command has no arguments or keywords.

#### Command Modes

Privileged EXEC
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
</tbody>
</table>

Examples

The following is sample output from the `debug ip traffic-export events` command:

```
Router# debug ip traffic-export events
RITE: exported input packet # 547
RITE: exported input packet # 548
RITE: exported input packet # 549
RITE: exported input packet # 550
RITE: exported input packet # 551
RITE: exported input packet # 552
RITE: exported input packet # 553
RITE: exported input packet # 554
RITE: exported input packet # 555
RITE: exported input packet # 556
RITE: exported input packet # 557
RITE: exported input packet # 558
RITE: exported input packet # 559
RITE: exported input packet # 560
RITE: exported input packet # 561
RITE: exported input packet # 562
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip traffic-export profile</code></td>
<td>Creates or edits an IP traffic export profile and enables the profile on an ingress interface.</td>
</tr>
</tbody>
</table>

**debug ip trigger-authentication**

To display information related to automated double authentication, use the `debug ip trigger-authentication` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip trigger-authentication [verbose]
no debug ip trigger-authentication [verbose]
```

Syntax Description

| verbose | (Optional) Specifies that the complete debugging output be displayed, including information about packets that are blocked before authentication is complete. |

Command Modes

Privileged EXEC

Usage Guidelines

Use this command when troubleshooting automated double authentication.

This command displays information about the remote host table. Whenever entries are added, updated, or removed, a new debugging message is displayed.

What is the remote host table? Whenever a remote user needs to be user-authenticated in the second stage of automated double authentication, the local device sends a User Datagram Protocol (UDP) packet to the host...
of the remote user. Whenever such a UDP packet is sent, the host IP address of the user is added to a table. If additional UDP packets are sent to the same remote host, a new table entry is not created; instead, the existing entry is updated with a new time stamp. This remote host table contains a cumulative list of host entries; entries are deleted after a timeout period or after you manually clear the table by using the `clear ip trigger-authentication` command.

If you include the `verbose` keyword, the debugging output also includes information about packet activity.

**Examples**

The following is sample output from the `debug ip trigger-authentication` command. In this example, the local device at 172.21.127.186 sends a UDP packet to the remote host at 172.21.127.114. The UDP packet is sent to request the remote user’s username and password (or PIN). (The output says “New entry added.”)

After a timeout period, the local device has not received a valid response from the remote host, so the local device sends another UDP packet. (The output says “Time stamp updated.”)

Then the remote user is authenticated, and after a length of time (the timeout period) the entry is removed from the remote host table. (The output says “remove obsolete entry.”)

```bash
myfirewall# debug ip trigger-authentication
TRIGGER_AUTH: UDP sent from 172.21.127.186 to 172.21.127.114, qdata=7C2504
   New entry added, timestamp=2940514234
TRIGGER_AUTH: UDP sent from 172.21.127.186 to 172.21.127.114, qdata=7C2504
   Time stamp updated, timestamp=2940514307
TRIGGER_AUTH: remove obsolete entry, remote host=172.21.127.114
```

The following is sample output from the `debug ip trigger-authentication verbose` command. In this example, messages about packet activity are included because of the use of the `verbose` keyword.

You can see many packets that are being blocked at the interface because the user has not yet been double authenticated. These packets will be permitted through the interface only after the user has been double authenticated. (You can see packets being blocked when the output says “packet enqueued” and then “packet ignored.”)

```bash
TRIGGER_AUTH: packet enqueued, qdata=69FEEC
   remote host=172.21.127.113, local host=172.21.127.186 (if: 0.0.0.0)
TRIGGER_AUTH: UDP sent from 172.21.127.186 to 172.21.127.113, qdata=69FEEC
   Time stamp updated
TRIGGER_AUTH: packet enqueued, qdata=69FEEC
   remote host=172.21.127.113, local host=172.21.127.186 (if: 0.0.0.0)
TRIGGER_AUTH: packet ignored, qdata=69FEEC
TRIGGER_AUTH: packet enqueued, qdata=69FEEC
   remote host=172.21.127.113, local host=172.21.127.186 (if: 0.0.0.0)
TRIGGER_AUTH: packet ignored, qdata=69FEEC
TRIGGER_AUTH: packet enqueued, qdata=69FEEC
   remote host=172.21.127.113, local host=172.21.127.186 (if: 0.0.0.0)
TRIGGER_AUTH: packet ignored, qdata=69FEEC
```

Cisco IOS Debug Command Reference - Commands I through L
**debug ip trm**

To enable debug information of the Trend Registration Module (TRM), use the `debug ip trm` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip trm [{detailed | timers}]
no debug ip trm [{detailed | timers}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>detailed</code></td>
<td>(Optional) The system prints detailed information about the TRM. If not specified, the system displays basic status information.</td>
</tr>
<tr>
<td><code>timers</code></td>
<td>(Optional) The system prints information about timer events on the TRM. If not specified, the system displays basic status information.</td>
</tr>
</tbody>
</table>

**Command Default**

This command is not enabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)XZ</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ip trm` to enable debug information of the TRM, which handles the registration between the system and the Trend Router Provisioning Server (TRPS).

**Examples**

The following is sample output from the `debug ip trm` command:

```
Router# debug ip trm
TRM: Exceeded retry timeouts. Setting server inactive
```

The following is sample output from the `debug ip trm detailed` command:

```
Router# debug ip trm detailed
TRM: Sending Reg Req to TRPS. Requesting AV Key = No
Modify Trend Global Parameter map
```

The following is sample output from the `debug ip trm timers` command:

```
Router# debug ip trm timers
TRM: Wait timer for active server. Sent Reg request
```

**debug ip urd**

To display debugging messages for URL Rendezvous Directory (URD) channel subscription report processing, use the `debug ip urd` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ip urd [{hostnameip-address}]
no debug ip urd
```
**debug ip urd**

To enable debug information of URL filter subsystems, use the `debug ip urlfilter` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
dump ip urlfilter {function-trace | detailed | events}
no dump ip urlfilter {function-trace | detailed | events}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>function-trace</th>
<th>The system displays a sequence of important functions that are called when configuring URL filtering.</th>
</tr>
</thead>
<tbody>
<tr>
<td>detailed</td>
<td>The system displays detailed information about various activities that occur during URL filtering.</td>
</tr>
<tr>
<td>events</td>
<td>The system displays various events such as queue event, timer event, and socket event.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(11)YU</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.4(15)XZ</td>
<td>This command was implemented on the Cisco 881 and Cisco 888 platforms.</td>
</tr>
</tbody>
</table>
This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the `debug ip urlfilter` command when SmartFilter URL filtering configured:

```
Router# debug ip urlfilter detailed
urlfilter:
   Urlfilter Detailed Debugs debugging is on
Router# show ip urlfilter config
N2H2 URL Filtering is ENABLED
Primary N2H2 server configurations
=========================================
N2H2 server IP address:192.168.1.103
N2H2 server port:4005
N2H2 retransmission time out:6 (in seconds)
N2H2 number of retransmission:2
Secondary N2H2 servers configurations
Other configurations
=========================================
Allow Mode:OFF
System Alert:ENABLED
Audit Trail:ENABLED
Log message on N2H2 server:DISABLED
Maximum number of cache entries:5
Maximum number of packet buffers:20
Maximum outstanding requests:1000
fw1_4#
1d15h:URLF:got a socket read event...
1d15h:URLF:socket recv failed.
1d15h:URLF:Closing the socket for server (192.168.1.103:4005)
1d15h:URLF-3-SERVER_DOWN:Connection to the URL filter server 192.168.1.103 is down
1d15h:URLF:Opening a socket for server (192.168.1.103:4005)
1d15h:URLF:socket fd 0
1d15h:URLF-5-SERVER_UP:Connection to an URL filter server(192.168.1.103) is made, the router is returning from ALLOW MODE
1d15h:URLF:got cache idle timer event...
1d16h:URLF:got cache absolute timer event...
1d16h:URLF:got cache idle timer event...
1d16h:URLF:got cache absolute timer event...
1d16h:URLF:got cache idle timer event...
1d16h:URLF:creating uis 0x63A95DB4, pending request 1
1d16h:URLF:domain name not found in the exclusive list
1d16h:URLF:got an cbac queue event...
1d16h:URLF:socket send successful...172.17.192.130:8080) -> 192.168.1.103:1052 seq 3344720064 wnd 24820
1d16h:URLF:holding pak 0x634A8A08 (172.17.192.130:8080) -> 192.168.1.103:1052 seq 3344721524 wnd 24820
1d16h:URLF:holding pak 0x634A98CC (172.17.192.130:8080) -> 192.168.1.103:1052 seq 3344722984 wnd 24820
1d16h:URLF:got a socket read event...
1d16h:URLF:socket recv (header) successful.
1d16h:URLF:socket recv (data) successful.
1d16h:URLF:N2H2 lookup code = -1
1d16h:URLF:Site/URL Blocked:sis 0x63675DC4, uis 0x63A95DB4
1d16h:URLF:(192.168.1.103:1052) RST -> 172.17.192.130:8080 seq 3361738063 wnd 0
```
debug ip verify mib

To view debug output that displays the operation of Unicast Reverse Path Forwarding (RPF) MIB objects and the helper software, use the **debug ip verify mib** command in privileged EXEC mode. To disable debugging for Unicast RPF, use the **no** form of this command.

**debug ip verify mib**  
**no debug ip verify mib**

**Syntax Description**  
This command has no arguments or keywords.

**Command Default**  
Debugging activity for the operation of Unicast RPF MIB objects and helper software does not occur.

**Command Modes**  
Privileged EXEC (#)
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(31)SB2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
<tr>
<td>12.2(33)SXI2</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI2.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Debug information for the Unicast RPF MIB is collected only when logging is enabled. Unicast RPF messages are stored in the logging buffer, and they are not displayed on the console unless you use the `debug ip verify mib` command.

Examples

The following example shows sample output of the `debug ip verify mib` command:

```
Router> enable
Router# debug ip verify mib
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
01:29:45: cipUrpfScalar_get, searchType 161
01:29:45: ipurpfmib_get_scalars
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip interface</code></td>
<td>Displays the usability status of interfaces configured for IP.</td>
</tr>
</tbody>
</table>
**debug ip virtual-reassembly**

To enable debugging of the virtual fragment reassembly (VFR) subsystem, use the `debug ip virtual-reassembly` command in privileged EXEC mode. To disable VFR debugging, use the `no` form of this command.

```
deproc ip virtual-reassembly [list {access-list | extended-access-list}]
no debug ip virtual-reassembly [list {access-list | extended-access-list}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>(Optional) Enables VFR conditional debugging.</td>
</tr>
<tr>
<td>access-list</td>
<td>Filters the generated list of VFR conditional debugging messages. The valid range is from 1 to 199.</td>
</tr>
<tr>
<td>extended-access-list</td>
<td>Filters the generated list of extended VFR conditional debugging messages. The valid range is from 1300 to 2699.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>The list keyword was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following sample output from the `debug ip virtual-reassembly` command allows you to monitor datagram fragmentation and reassembly status—such as whether a datagram is incomplete and when fragments (from the datagram) are created (after a datagram is determined to be complete).

```
Router# debug ip virtual-reassembly
00:17:35: IP_VFR: fragment (sa:13.0.0.2, da:17.0.0.2, id:11745, offset:0, len:104) in fast path...
00:17:35: IP_VFR: created frag state for sa:13.0.0.2, da:17.0.0.2, id:11745...
00:17:35: IP_VFR: pak incomplete cpak-offset:0, cpak-len:104, flag: 1
00:17:35: IP_VFR: dgrm incomplete, returning...
00:17:35: IP_VFR: fragment (sa:13.0.0.2, da:17.0.0.2, id:11745, offset:104, len:104) in fast path...
00:17:35: IP_VFR: cpak-offset:0, cpak-len:104, npak-offset:104
00:17:35: IP_VFR: dgrm incomplete, returning...
00:17:35: IP_VFR: fragment (sa:13.0.0.2, da:17.0.0.2, id:11745, offset:208, len:104) in fast path...
00:17:35: IP_VFR: cpak-offset:0, cpak-len:104, npak-offset:104
00:17:35: IP_VFR: dgrm incomplete, returning...
00:17:35: IP_VFR: fragment (sa:13.0.0.2, da:17.0.0.2, id:11745, offset:312, len:104) in fast path...
00:17:35: IP_VFR: cpak-offset:0, cpak-len:104, npak-offset:104
00:17:35: IP_VFR: dgrm incomplete, returning...
00:17:35: IP_VFR: fragment (sa:13.0.0.2, da:17.0.0.2, id:11745, offset:416, len:92) in fast path...
```
00:17:35: IP_VFR: cpak-offset:0, cpak-len:104, npak-offset:104
00:17:35: IP_VFR: cpak-offset:104, cpak-len:104, npak-offset:208
00:17:35: IP_VFR: cpak-offset:208, cpak-len:104, npak-offset:312
00:17:35: IP_VFR: cpak-offset:312, cpak-len:104, npak-offset:416
00:17:35: IP_VFR: dgrm complete, switching the frags.
00:17:35: IP_VFR: switching fragment (sa:13.0.0.2, da:17.0.0.2, id:11745, offset:0, len:104)
00:17:35: IP_VFR: switching fragment (sa:13.0.0.2, da:17.0.0.2, id:11745, offset:104, len:104)
00:17:35: IP_VFR: switching fragment (sa:13.0.0.2, da:17.0.0.2, id:11745, offset:208, len:104)
00:17:35: IP_VFR: switching fragment (sa:13.0.0.2, da:17.0.0.2, id:11745, offset:312, len:92)
00:17:35: IP_VFR: all fragments have been switched.
00:17:35: IP_VFR: pak_subblock_free - pak 0x64A3DC30
00:17:35: IP_VFR: pak_subblock_free - pak 0x6430F010
00:17:35: IP_VFR: pak_subblock_free - pak 0x6430F678
00:17:35: IP_VFR: pak_subblock_free - pak 0x643119B4
00:17:35: IP_VFR: deleted frag state for sa:13.0.0.2, da:17.0.0.2, id:11745
00:17:35: IP_VFR: pak_subblock_free - pak 0x64A3D5C8

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip virtual-reassembly</td>
<td>Enables VFR on an interface.</td>
</tr>
</tbody>
</table>

**debug ip wccp**

To display information about IPv4 Web Cache Communication Protocol (WCCP) services, use the `debug ip wccp` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
dump ip wccp {default | vrf vrf-name {events | packets [control]} | events | packets [{bypass | control | redirect]} | platform | subblocks}
no debug ip wccp {default | vrf vrf-name events | packets [control]} | events | packets [{bypass | control | redirect]} | platform | subblocks}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Displays information about default WCCP services.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>Specifies a virtual routing and forwarding (VRF) instance to associate with a service group.</td>
</tr>
<tr>
<td>events</td>
<td>Displays information about significant WCCP events.</td>
</tr>
<tr>
<td>packets</td>
<td>Displays information about every WCCP packet received or sent by the router.</td>
</tr>
<tr>
<td>control</td>
<td>(Optional) Displays information about WCCP control packets.</td>
</tr>
<tr>
<td>bypass</td>
<td>(Optional) Displays information about WCCP bypass packets.</td>
</tr>
<tr>
<td>redirect</td>
<td>(Optional) Displays information about WCCP redirect packets.</td>
</tr>
<tr>
<td>platform</td>
<td>Displays information about the WCCP platform application programming interface (API).</td>
</tr>
<tr>
<td>subblocks</td>
<td>Displays information about WCCP subblocks.</td>
</tr>
</tbody>
</table>

**Command Default**

Debug information is not displayed.
**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced. This command replaces the <code>debug ip wccp packets</code> and <code>debug ip wccp events</code> commands.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.1S</td>
<td>This command was integrated into Cisco IOS XE Release 3.1S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the `vrf` keyword is not used, the command displays debug information about all WCCP services on the router. The `default` keyword is used to specify default WCCP services.

**Examples**

The following is sample output from the `debug ip wccp events` command when a Cisco Cache Engine is added to the list of available Web caches:

```
Router# debug ip wccp events
WCCP-EVNT: Built I_See_You msg body w/1 usable web caches, change # 0000000A
WCCP-EVNT: Web Cache 192.168.25.3 added
WCCP-EVNT: Built I_See_You msg body w/2 usable web caches, change # 0000000B
WCCP-EVNT: Built I_See_You msg body w/2 usable web caches, change # 0000000C
```

The following is sample output from the `debug ip wccp packets` command. The router is sending keepalive packets to the Cisco Cache Engines at 192.168.25.4 and 192.168.25.3. Each keepalive packet has an identification number associated with it. When the Cisco Cache Engine receives a keepalive packet from the router, it sends a reply with the identification number back to the router.

```
Router# debug ip wccp packets
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.4 w/rcvd_id 00003532
WCCP-PKT: Sending I_See_You packet to 192.168.25.4 w/ rcvd_id 00003534
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.3 w/rcvd_id 00003533
WCCP-PKT: Sending I_See_You packet to 192.168.25.3 w/ rcvd_id 00003535
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.4 w/rcvd_id 00003534
WCCP-PKT: Sending I_See_You packet to 192.168.25.4 w/ rcvd_id 00003536
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.3 w/rcvd_id 00003535
WCCP-PKT: Sending I_See_You packet to 192.168.25.3 w/ rcvd_id 00003535
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.4 w/rcvd_id 00003536
WCCP-PKT: Sending I_See_You packet to 192.168.25.4 w/ rcvd_id 00003538
WCCP-PKT: Received valid Here_I_Am packet from 192.168.25.3 w/rcvd_id 00003537
WCCP-PKT: Sending I_See_You packet to 192.168.25.3 w/ rcvd_id 00003539
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip wccp</td>
<td>clears the counter for packets redirected using WCCP.</td>
</tr>
<tr>
<td>ip wccp</td>
<td>Enables support of the specified WCCP service for participation in a service group.</td>
</tr>
<tr>
<td>ip wccp redirect</td>
<td>Enables packet redirection on an outbound or inbound interface using WCCP.</td>
</tr>
<tr>
<td>show ip interface</td>
<td>Lists a summary of the IP information and status of an interface.</td>
</tr>
</tbody>
</table>
**debug ipc**

To display debugging messages about interprocess communication (IPC) activity, use the `debug ipc` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ipc {all | ports | seats | sessions | zones}
no debug ipc {all | ports | seats | sessions | zones}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>Displays all debugging IPC messages. A confirmation message will appear because enabling this keyword can severely impact performance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ports</td>
<td>Displays debugging messages related to the creation and deletion of IPC ports.</td>
</tr>
<tr>
<td></td>
<td>seats</td>
<td>Displays debugging messages related to the creation and deletion of IPC nodes (seats).</td>
</tr>
<tr>
<td></td>
<td>sessions</td>
<td>Displays debugging messages related to the creation and deletion of IPC sessions.</td>
</tr>
<tr>
<td></td>
<td>zones</td>
<td>Displays debugging messages related to the creation and deletion of IPC zones.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(11)T</td>
<td>The <code>sessions</code> and <code>zones</code> keywords were added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ipc` command to troubleshoot IPC issues discovered when the `show ipc` command is run. The debugging output varies depending on the types of IPC packets that are selected by the different keywords.

⚠️ **Caution**

Use the `debug ipc all` command with caution because it enables the `debug ipc packets` command and the volume of output can severely impact system performance. A confirmation message is displayed. We recommend that you use one of the other keywords to focus on a specific IPC activity and to limit the volume of output.

**Examples**

The following example shows the confirmation message that appears when the `debug ipc all` command is entered:

```
Router# debug ipc all
This may severely impact system performance. Continue? [confirm]
```

The following example shows how to enable the display of debugging messages about IPC sessions. The debugging output varies depending on the type of IPC activity that is specified. Each entry includes some text explanation--the example below shows that the IPC control session was opened to port 0x1030000, closed, and then cleared--followed by a series of header or data fields.
Router# debug ipc sessions
Session level events debugging is on
*Sep 14 13:13:35.435: IPC: Control Session opened to port 0x1030000
*Sep 14 13:13:35.439: -Traceback= 40779898 4077649C 40776A00 40777040 4077554C
*Sep 14 13:13:35.439: IPC: Session 0 to port 0x1030000 closed
*Sep 14 13:13:35.439: -Traceback= 4077A9D4 40776370 4077132C 40771A58 4062EC7C 4028EC8C 40649710 4057F87C
*Sep 14 13:13:35.439: IPC: Session handle of session 0 to port 0x1030000 cleared
*Sep 14 13:13:35.439: -Traceback= 407798EC 4077A9E0 40776370 4077132C 40771A58 4062EC7C 4028EC8C 40649710 4057F87C

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipc packets</td>
<td>Displays debugging messages about IPC packets.</td>
</tr>
<tr>
<td>show ipc</td>
<td>Displays IPC information.</td>
</tr>
</tbody>
</table>

**debug ipc acks**

To display debugging messages about interprocess communication (IPC) acknowledgments (ACKs), use the `debug ipc acks` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```plaintext
debug ipc acks [{{rx | tx}}] [dest destination-port-id] [source source-seat-id] [session session-id] [header dump]
no debug ipc acks [{{rx | tx}}] [dest destination-port-id] [source source-seat-id] [session session-id] [header dump]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rx</td>
<td>(Optional) Displays debugging messages related to the retrieval of IPC ACK messages.</td>
</tr>
<tr>
<td>tx</td>
<td>(Optional) Displays debugging messages related to the transmission of IPC ACK messages.</td>
</tr>
</tbody>
</table>
| dest     | (Optional) Displays debugging messages related to a destination port of IPC ACK messages. If not specified, information about all destinations is displayed.  
  - Use the `destination-port-id` argument to specify a hexadecimal number that represents a destination port ID. The range is from 0 to FFFFFFFF. |
| source   | (Optional) Displays debugging information about messages from an IPC node. If not specified, information about all nodes is displayed.  
  - Use the `source-seat-id` argument to specify a hexadecimal number that represents a source seat ID. The range is from 0 to FFFFFFFF. |
| session  | (Optional) Displays debugging messages related to an IPC session. If not specified, information about all sessions is displayed.  
  - Use the `session-id` argument to specify a session ID. The range is from 0 to 65535. |
| header dump | (Optional) Displays only the packet header information. |
### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `debug ipc acks` command to troubleshoot IPC ACK issues. To enable debugging for other IPC activities, use the `debug ipc` command.

### Examples

The following example shows how to enable the display of packet headers only when debugging IPC ACK messages. The debugging output varies depending on the type of IPC activity that is specified. Each entry includes some text explanation—the example below shows that the server received an ACK HDR—followed by a series of header or data fields.

```
Router# debug ipc acks header dump
Aug 19 03:52:36.136:IPC:Server received ACK HDR:442A64E0 src:100000A, dst:406116E8, index:-1, seq:22045, sz:0, type:65535, flags:2 hi:1F371, lo:0
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipc</td>
<td>Displays IPC debugging information.</td>
</tr>
</tbody>
</table>

### debug ipc errors

To display debugging messages about interprocess communication (IPC) errors and warnings, use the `debug ipc errors` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
dump ipc errors [driver] [sequence] [timeout]
no dump ipc errors [driver] [sequence] [timeout]
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>driver</td>
<td>(Optional) Displays debugging messages related to IPC errors at the driver (transport) medium.</td>
</tr>
<tr>
<td>sequence</td>
<td>(Optional) Displays information related to IPC messages that have sequence-related issues, such as duplicate or unexpected messages.</td>
</tr>
<tr>
<td>timeout</td>
<td>(Optional) Displays only information related to IPC messages that have timed out.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(11)T</td>
<td>The <code>driver</code>, <code>sequence</code>, and <code>timeout</code> keywords were added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Use the `debug ipc errors` command to troubleshoot IPC error issues. To enable debugging for other IPC activities, use the `debug ipc` command. The debugging output varies depending on the type of IPC activity that is specified.

Examples

The following example shows how to enable the display of error debugging information about IPC messages that have timed out. The debugging output varies depending on the type of IPC activity that is specified. Each entry includes some text explanation—the example below shows that the message number 4428D3D0 timed out waiting for an acknowledgment (Ack)—followed by a series of header or data fields.

```
Router# debug ipc errors timeout
Message Timeouts debugging is on
*Sep 14 14:42:17.103: IPC: Message 4428D3D0 timed out waiting for Ack
*Sep 14 14:42:17.103: IPC: MSG: ptr: 0x4428D3D0, flags: 0x88, retries: 6, seq: 0x10300002, refcount: 2, retry: 00:00:00, rpc_result = 0x0, data_buffer = 0x4442AB10, header = 0x4442AED4, data = 0x4442AEF4
HDR: src: 0x10000, dst: 0x103000A, index: 0, seq: 2, sz: 512, type: 0, flags: 0x400
hi: 0x1EC, lo: 0x4442AEF4
DATA: 00 00 00 05 00 00 00 00 00 00 00 3A 00 00 00 00 00 00 00 00 00 00
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ipc</code></td>
<td>Displays IPC debugging information.</td>
</tr>
</tbody>
</table>

**debug ipc events**

To display debugging messages about interprocess communication (IPC) events, use the `debug ipc events` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ipc events [flushes] [retries]
no debug ipc events [flushes] [retries]
```

**Syntax Description**

- `flushes` (Optional) Displays only information related to IPC messages that are flushed.
- `retries` (Optional) Displays only information related to IPC messages that are re-sent.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(11)T</td>
<td>The <code>flushes</code> and <code>retries</code> keywords were added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ipc events` command to troubleshoot IPC events issues. To enable debugging for other IPC activities, use the `debug ipc` command.
Examples

The following example shows how to enable the display of debugging messages about IPC events:

Router# debug ipc events
Special Events debugging is on

The following example shows how to enable the display of event debugging information about IPC messages that are re-sent. The debugging output varies depending on the type of IPC activity that is specified. Each entry includes some text explanation--the example below shows that there was a retry attempt for a specific message--followed by a series of header or data fields.

Router# debug ipc events retries
Message Retries debugging is on
*Sep 14 14:46:44.151: IPC: Retry attempt for MSG: ptr: 0x442AFE74, flags: 0x88, retries:4, seq: 0x1030003, refcount: 2, retry: 00:00:00, rpc_result = 0x0, data_buffer = 0x445EBA44, header =0x445EBE28, data = 0x445EBE28
HDR: src: 0x10000, dst: 0x103000A, index: 0, seq: 3, sz: 512, type: 0, flags: 0x400 hi:0x201, lo: 0x445EBE28
DATA: 00 00 00 05 00 00 00 00 00 00 00 3A 00 00 00 00 00 00 03 D2

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipc</td>
<td>Displays IPC debugging information.</td>
</tr>
</tbody>
</table>

**debug ipc fragments**

To display debugging messages about interprocess communication (IPC) fragments, use the `debug ipc fragments` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
display ipc fragments [rx | tx] [dest destination-port-id] [source source-seat-id] [session session-id] [type application-type] [flags header-flag] [sequence sequence] [msgidhi msg-id-high] [msgidlo msg-id-low] [data offset offset-from-header value value-to-match dump bytes] [size size] [header dump]
```

**Syntax Description**

<p>| rx | (Optional) Displays debugging messages related to the retrieval of IPC fragments. |
| tx | (Optional) Displays debugging messages related to the transmission of IPC fragments. |
| dest | (Optional) Displays debugging messages related to a destination port of IPC fragments. If not specified, information about all destinations is displayed. |
|     | • Use the <code>destination-port-id</code> argument to specify a hexadecimal number that represents a destination port ID. The range is from 0 to FFFFFFFF. |</p>
<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>source</strong></td>
<td>(Optional) Displays debugging information about messages from an IPC node. If not specified, information about all nodes is displayed.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>source-seat-id</code> argument to specify a hexadecimal number that represents a source seat ID. The range is from 0 to FFFFFFFF.</td>
</tr>
<tr>
<td><strong>session</strong></td>
<td>(Optional) Displays debugging messages related to an IPC session. If not specified, information about all sessions is displayed.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>session-id</code> argument to specify a session ID. The range is from 0 to 65535.</td>
</tr>
<tr>
<td><strong>type</strong></td>
<td>(Optional) Displays debugging messages related to a type of IPC fragments. If not specified, information about all application types is displayed.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>application-type</code> argument to specify a hexadecimal number that represents an application. The range is from 0 to FFFF.</td>
</tr>
<tr>
<td><strong>flags</strong></td>
<td>(Optional) Displays debugging messages related to an IPC fragment’s header flag. If not specified, information about all header flags is displayed.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>header-flag</code> argument to specify a hexadecimal number that represents a header flag value. The range is from 0 to FFFF.</td>
</tr>
<tr>
<td><strong>sequence</strong></td>
<td>(Optional) Displays debugging messages related to a sequence number of an IPC fragment. If not specified, information about all sequence numbers is displayed.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>sequence</code> argument to specify a sequence number. The range is from 0 to 65535.</td>
</tr>
<tr>
<td><strong>msgidhi</strong></td>
<td>(Optional) Displays debugging messages related to the higher byte of the unique ID of an IPC fragment.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>msg-id-high</code> argument to specify a hexadecimal number that represents a higher byte of the unique ID. The range is from 0 to FFFFFFFF.</td>
</tr>
<tr>
<td><strong>msgidlo</strong></td>
<td>(Optional) Displays debugging messages related to the lower byte of the unique ID of an IPC fragment.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>msg-id-low</code> argument to specify a hexadecimal number that represents a lower byte of the unique ID. The range is from 0 to FFFFFFFF.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>data</td>
<td>(Optional) Displays debugging messages related to the IPC fragment payload. If not specified, information about all of the IPC fragment's payload is displayed.</td>
</tr>
<tr>
<td>• offset</td>
<td>(Optional) Displays offset IPC data. If this keyword is configured, the value keyword must also be configured.</td>
</tr>
<tr>
<td>• dump</td>
<td>(Optional) Configures the number of data bytes to display. Use the bytes argument to specify the number of data bytes. The range is from 0 to 65535.</td>
</tr>
<tr>
<td>size</td>
<td>(Optional) Displays IPC fragment debugging messages of a specific size. If not specified, information about messages of any size is displayed.</td>
</tr>
<tr>
<td>• size</td>
<td>Use the size argument to specify the message size in rows. The range is from 0 to 65535.</td>
</tr>
<tr>
<td>header dump</td>
<td>(Optional) Displays only the packet header information.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ipc fragments` command to troubleshoot IPC fragment issues. To enable debugging for other IPC activities, use the `debug ipc` command.

**Examples**

The following example shows how to enable the display of debugging information about IPC fragments. The debugging output varies depending on the type of IPC activity that is specified. Each entry includes some text explanation--the example below shows that the server received a fragment message--followed by a series of header or data fields.

```
Router# debug ipc fragments
IPC Fragments debugging is on
01:43:55: IPC: Server received fragment MSG: ptr: 0x503A4348, flags: 0x100, retries: 0, seq: 0x0, refcount: 1, retry: never, rpc_result = 0x0, data_buffer = 0x433809E8, header = 0x8626748, data = 0x8626768
HDR: src: 0x10000, dst: 0x2210015, index: 0, seq: 1, sz: 1468, type: 0, flags: 0x10, hi:0x9AA, lo: 0x7D0
DATA: 00 00 00 01 00 00 00 00 00 00 AA 00 00 00 00 17 E4
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipc</td>
<td>Displays IPC debugging information.</td>
</tr>
</tbody>
</table>

**debug ipc nacks**

To display debugging messages about interprocess communication (IPC) negative acknowledgments (NACKs), use the **debug ipc nacks** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ipc nacks**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rx</td>
<td>(Optional) Displays debugging messages related to the retrieval of IPC NACK messages.</td>
</tr>
<tr>
<td>tx</td>
<td>(Optional) Displays debugging messages related to the transmission of IPC NACK messages.</td>
</tr>
<tr>
<td>dest</td>
<td>(Optional) Displays debugging messages related to a destination port of IPC NACK messages. If not specified, information about all destinations is displayed.</td>
</tr>
<tr>
<td>source</td>
<td>(Optional) Displays debugging information about messages from an IPC node. If not specified, information about all nodes is displayed.</td>
</tr>
<tr>
<td>session</td>
<td>(Optional) Displays debugging messages related to an IPC session. If not specified, information about all sessions is displayed.</td>
</tr>
<tr>
<td>header dump</td>
<td>(Optional) Displays only the packet header information.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **debug ipc nacks** command to troubleshoot IPC NACK issues. To enable debugging for other IPC activities, use the **debug ipc** command.
Examples

The following example shows how to enable the display of packet headers only when debugging IPC NACK messages. The debugging output varies depending on the type of IPC activity that is specified. Each entry includes some text explanation--the example below shows that the server sent a NACK message and received a NACK header--followed by a series of header or data fields.

Router# debug ipc nacks header dump
IPC Nacks debugging is on
01:46:11: IPC: Server sent NACK MSG: ptr: 0x432A7428, flags: 0x100, retries: 0, seq: 0x0, refcount: 1, retry: never, rpc_result = 0x0, data_buffer = 0x431E4B50, header = 0x855F508, data = 0x855F528
HDR: src: 0x2210015, dst: 0x10000, index: 1, seq: 0, type: 0, flags: 0x100
hi: 0x4A9, lo: 0x85AA3E8
01:46:11: SP: IPC: Server received NACK HDR: E46A448 src: 2210015, dst: 10000, index: 1, seq: 3, sz: 0, type: 0, flags: 0x100 hi: 4A9, lo: 85AA3E8

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipc</td>
<td>Displays IPC debugging information.</td>
</tr>
</tbody>
</table>

debug ipc packets

To display debugging messages about interprocess communication (IPC) packets, use the debug ipc packets command in privileged EXEC mode. To disable debugging output, use the no form of this command.

ddebug ipc packets [[rx | tx]] [dest destination-port-id] [source source-seat-id] [session session-id] [type application-type] [flags header-flag] [sequence sequence] [msgidhi msg-id-high] [msgidlo msg-id-low] [data offset offset-from-header value value-to-match dump bytes] [size size] [header dump]

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rx</td>
<td>(Optional) Displays debugging messages related to the retrieval of IPC packets.</td>
</tr>
<tr>
<td>tx</td>
<td>(Optional) Displays debugging messages related to the transmission of IPC packets.</td>
</tr>
<tr>
<td>dest</td>
<td>(Optional) Displays debugging messages related to a destination port of IPC packets. If not specified, information about all destinations is displayed.</td>
</tr>
<tr>
<td></td>
<td>• Use the destination-port-id argument to specify a hexadecimal number that represents a destination port ID. The range is from 0 to FFFFFFFF.</td>
</tr>
<tr>
<td>source</td>
<td>(Optional) Displays debugging information about messages from an IPC node. If not specified, information about all nodes is displayed.</td>
</tr>
<tr>
<td></td>
<td>• Use the source-seat-id argument to specify a hexadecimal number that represents a source seat ID. The range is from 0 to FFFFFFFF.</td>
</tr>
</tbody>
</table>
### session
(Optional) Displays debugging messages related to an IPC session. If not specified, information about all sessions is displayed.

- Use the `session-id` argument to specify a session ID. The range is from 0 to 65535.

### type
(Optional) Displays debugging messages related to a type of IPC packet. If not specified, information about all application types is displayed.

- Use the `application-type` argument to specify a hexadecimal number that represents an application. The range is from 0 to FFFF.

### flags
(Optional) Displays debugging messages related to an IPC packet header flag. If not specified, information about all header flags is displayed.

- Use the `header-flag` argument to specify a hexadecimal number that represents a header flag value. The range is from 0 to FFFF.

### sequence
(Optional) Displays debugging messages related to a sequence number of an IPC packet. If not specified, information about all sequence numbers is displayed.

- Use the `sequence` argument to specify a sequence number. The range is from 0 to 65535.

### msgidhi
(Optional) Displays debugging messages related to the higher byte of the unique ID of an IPC packet.

- Use the `msg-id-high` argument to specify a hexadecimal number that represents a higher byte of the unique ID. The range is from 0 to FFFFFFFF.

### msgidlo
(Optional) Displays debugging messages related to the lower byte of the unique ID of an IPC packet.

- Use the `msg-id-low` argument to specify a hexadecimal number that represents a lower byte of the unique ID. The range is from 0 to FFFFFFFF.

### data
(Optional) Displays debugging messages related to the IPC packet payload. If not specified, information about all of the IPC packet’s payload is displayed.

- **offset** --(Optional) Displays offset IPC data. If this keyword is configured, the `value` keyword must also be configured.
  - Use the `offset-from-header` argument to specify the offset value from the start of the IPC data. The range is from 0 to 65535.
  - Use the `value` keyword to configure the value expected at the offset of the IPC data.
  - Use the `value-to-match` argument to specify the hexadecimal number that represents the value expected at the offset of the IPC data. The range is from 0 to FF.

- **dump** --(Optional) Configures the number of data bytes to display.
  - Use the `bytes` argument to specify the number of data bytes. The range is from 0 to 65535.
 Displays IPC packet debugging messages of a specific size. If not specified, information about messages of any size is displayed.

- Use the size argument to specify the message size in rows. The range is from 0 to 65535.

(Optional) Displays only the packet header information.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ipc packets` command to troubleshoot IPC packet issues. To enable debugging for other IPC activities, use the `debug ipc` command.

⚠️ **Caution**

Use the `debug ipc packets` command with caution because the volume of output can severely impact system performance. A confirmation message is displayed. We recommend that you use one of the optional keywords to focus on a specific IPC activity and to limit the volume of output.

**Examples**

The following example shows how to enable the display of IPC packet debugging messages and includes some sample output. The debugging output varies depending on the type of IPC activity that is specified. Each entry includes some text explanation—the example below shows that the IPC server received a message—followed by a series of header or data fields.

```
Router# debug ipc packets
This may severely impact system performance. Continue?[confirm] Y
Aug 19 030612.297 IPC Server received MSG ptr 0x441BE75C, flags 0x80, retries 0, seq 0x0, refcount 1, retry never, rpc_result = 0x0, data_buffer = 0x443152A8, header = 0x4431566C, data = 0x4431568C
HDR src 0x106000, dst 0x1000C, index 2, seq 0, sz 28, type 770, flags 0x40 hi 0x1F25B, lo 0x442F0BC0
DATA 00 00 00 06 00 00 00 02 00 00 00 06 00 E7 00 02 00 00 00 00
```

The following example shows how to enable the display of IPC messages received with a destination port of 0x1000C in session 1 with a message size of 500 rows.

```
Router# debug ipc packets rx dest 1000C session 1 size 500
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipc</td>
<td>Displays IPC debugging information.</td>
</tr>
</tbody>
</table>
debug ipc rpc

To display debugging messages about interprocess communication (IPC) remote-procedure call (RPC) packets, use the `debug ipc rpc` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ipc rpc [(rx|tx)] [({query|response})] [dest destination-port-id] [source source-seat-id] [session session-id] [type application-type] [flags header-flag] [sequence sequence] [msgidhi msg-id-high] [msgidlo msg-id-low] [data offset offset-from-header value value-to-match dump bytes] [size size] [header dump]
```

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rx</td>
<td>(Optional) Displays debugging messages related to the retrieval of IPC RPC packets.</td>
</tr>
<tr>
<td>tx</td>
<td>(Optional) Displays debugging messages related to the transmission of IPC RPC packets.</td>
</tr>
<tr>
<td>query</td>
<td>(Optional) Displays debugging messages related to IPC RPC queries.</td>
</tr>
<tr>
<td>response</td>
<td>(Optional) Displays debugging messages related to IPC RPC responses.</td>
</tr>
<tr>
<td>dest</td>
<td>(Optional) Displays debugging messages related to a destination port of IPC RPC packets. If not specified, information about all destinations is displayed.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>destination-port-id</code> argument to specify a hexadecimal number that represents a destination port ID. The range is from 0 to FFFFFFFF.</td>
</tr>
<tr>
<td>source</td>
<td>(Optional) Displays debugging information about messages from an IPC node. If not specified, information about all nodes is displayed.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>source-seat-id</code> argument to specify a hexadecimal number that represents a source seat ID. The range is from 0 to FFFFFFFF.</td>
</tr>
<tr>
<td>session</td>
<td>(Optional) Displays debugging messages related to an IPC session. If not specified, information about all sessions is displayed.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>session-id</code> argument to specify a session ID. The range is from 0 to 65535.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Displays debugging messages related to a type of IPC RPC message. If not specified, information about all application types is displayed.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>application-type</code> argument to specify a hexadecimal number that represents an application. The range is from 0 to FFFF.</td>
</tr>
<tr>
<td>flags</td>
<td>(Optional) Displays debugging messages related to an IPC RPC message header flag. If not specified, information about all header flags is displayed.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>header-flag</code> argument to specify a hexadecimal number that represents a header flag value. The range is from 0 to FFFF.</td>
</tr>
</tbody>
</table>
| **sequence** | (Optional) Displays debugging messages related to a sequence number of an IPC RPC message. If not specified, information about all sequence numbers is displayed.  
  - Use the `sequence` argument to specify a sequence number. The range is from 0 to 65535. |
| **msgidhi** | (Optional) Displays debugging messages related to the higher byte of the unique ID of an IPC RPC message.  
  - Use the `msg-id-high` argument to specify a hexadecimal number that represents a higher byte of the unique ID. The range is from 0 to FFFFFFFF. |
| **msgidlo** | (Optional) Displays debugging messages related to the lower byte of the unique ID of an IPC RPC message.  
  - Use the `msg-id-low` argument to specify a hexadecimal number that represents a lower byte of the unique ID. The range is from 0 to FFFFFFFF. |
| **data** | (Optional) Displays debugging messages related to the IPC RPC payload. If not specified, information about all of the IPC RPC’s payload is displayed.  
  - **offset** -- (Optional) Displays offset IPC data. If this keyword is configured, the `value` keyword must also be configured.  
    - Use the `offset-from-header` argument to specify the offset value from the start of the IPC data. The range is from 0 to 65535.  
    - Use the `value` keyword to configure the value expected at the offset of the IPC data.  
    - Use the `value-to-match` argument to specify the hexadecimal number that represents the value expected at the offset of the IPC data. The range is from 0 to FF.  
  - **dump** -- (Optional) Configures the number of data bytes to display.  
    - Use the `bytes` argument to specify the number of data bytes. The range is from 0 to 65535. |
| **size** | (Optional) Displays IPC RPC debugging messages of a specific size. If not specified, information about messages of any size is displayed.  
  - Use the `size` argument to specify the message size in rows. The range is from 0 to 65535. |
| **header dump** | (Optional) Displays only the packet header information. |

**Command Modes**

- Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

Use the `debug ipc rpc` command to troubleshoot IPC RPC packet issues. To enable debugging for other IPC activities, use the `debug ipc` command. The debugging output varies depending on the type of IPC activity that is specified.

### Examples

The following example shows how to enable the display of packet headers only when debugging IPC RPC response messages. The debugging output varies depending on the type of IPC activity that is specified. Each entry includes some text explanation—the example below shows that the server received an RPC response—followed by a series of header or data fields.

```
Router# debug ipc rpc response header dump source 2210003
RPC debugging is on
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipc</td>
<td>Displays IPC debugging information.</td>
</tr>
</tbody>
</table>

### debug iphc ipc

To display the IP header compression (IPHC) interprocessor communication (IPC) messages that are passed between the route processor (RP) and line cards (LCs), use the `debug iphc ipc` command in privileged EXEC mode. To disable the display of these messages, use the `no` form of this command.

```
depth iphc ipc [{events | statistics}]
no debug iphc ipc [{events | statistics}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>(Optional) Displays IPHC IPC command and control events.</td>
</tr>
<tr>
<td>statistics</td>
<td>(Optional) Displays IPHC IPC counter updates.</td>
</tr>
</tbody>
</table>

### Command Default

IPHC IPC messages are not displayed.

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(32)SY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(10)</td>
<td>This command was integrated into Cisco IOS Release 12.4(10).</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If you issue the `debug iphc ipc` command without keywords, all the IPC messages that are passed between the RP and the LC are displayed. On routers with many interfaces and distributed systems, the number of IPC messages becomes unwieldy, because of all the counter updates. To display only the events that indicate interface state changes, issue the `debug iphc ipc events` command.
Examples

The following example enables the display of all IPHC IPC messages:

```
Router# debug iphc ipc
IPHC IPC statistics debugging is on
IPHC IPC event debugging is on
```

The following example disables IPHC IPC statistics debugging:

```
Router# no debug iphc ipc statistics
IPHC IPC statistics debugging is off
```

The following example enables the display of IPHC IPC event messages:

```
Router# debug iphc ipc events
IPHC IPC event debugging is on
```

The command output shows the event messages as the interface changes from enabled to administratively down:

```
%OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on Multilink8 from FULL to DOWN
%LINK-5-CHANGED: Interface Multilink8, changed state to administratively down.
IPHC IPC 2: Set Negotiated mesg (Mu PPP 128 2 0)
IPHC Mu8: Distributed FS disabled
IPHC IPC 2: Send Set Configured mesg (Mu PPP 128 2 0)
IPHC IPC Mu8: i/f state change complete (Up/Down: 0/1)
```

The following example enables the display of IPHC IPC counter updates:

```
Router# debug iphc ipc statistics
IPHC IPC statistics debugging is on
```

The command output shows the interface counter updates:

```
IPHC IPC 2: recv Stats msg, count:4
IPHC IPC Mu8: stats update from LC
IPHC IPC Mu6: stats update from LC
IPHC IPC Se2/0/0/3:0: stats update from LC
IPHC IPC Se2/0/0/1:0: stats update from LC
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces</td>
<td>Displays statistics for all interfaces.</td>
</tr>
<tr>
<td>show ipc</td>
<td>Displays IPC statistics.</td>
</tr>
</tbody>
</table>

### debug ipv6 cef drop

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) dropped packets, use the `debug ipv6 cef drop` command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 dropped packets, use the `no` form of this command.

```
depbug ipv6 cef drop [rpf]
no debug ipv6 cef drop
```
Syntax Description

<table>
<thead>
<tr>
<th>rpf</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Displays packets dropped by the IPv6 CEF Unicast Reverse-Path Forwarding (Unicast RPF) feature.</td>
</tr>
</tbody>
</table>

Command Default

Debugging for CEFv6 and dCEFv6 dropped packets is not enabled.

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(22)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>The rpf keyword was added.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The `debug ipv6 cef drop` command is similar to the `debug ip cef drops` command, except that it is IPv6-specific.

Note

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the `logging` command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the Release 12.3 Cisco IOS Debug Command Reference.

Examples

The following is sample output from the `debug ipv6 cef drop` command:

```
Router# debug ipv6 cef drop
*Aug 30 08:20:51.169: IPv6-CEF: received packet on Serial6/0/2
*Aug 30 08:20:51.169: IPv6-CEF: found no adjacency for 2001:0DB8::1 reason 2
*Aug 30 08:20:51.169: IPv6-CEF: packet not switched: code 0x1
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6-CEF: received packet on Serial6/0/2</td>
<td>Cisco Express Forwarding has received a packet addressed to the router via serial interface 6/0/2.</td>
</tr>
</tbody>
</table>
### debug ipv6 cef events

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) general events, use the `debug ipv6 cef events` command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 general events, use the `no` form of this command.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging for CEFv6 and dCEFv6 general events is not enabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(22)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ipv6 cef events` command is similar to the `debug ip cef events` command, except that it is IPv6-specific.
By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the Release 12 Cisco IOS Debug Command Reference.

**Note**

The following is sample output from the `debug ipv6 cef events` command:

```
Router# debug ipv6 cef events
IPv6 CEF packet events debugging is on
Router# *
Aug 30 08:22:57.809: %LINK-3-UPDOWN: Interface Serial6/0/2, changed state to up
Aug 30 08:22:58.809: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial6/0/2, changed state to up
Aug 30 08:23:00.821: CEFv6-IDB: Serial6/0/2 address 2001:0DB8::248 add download succeeded
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Serial6/0/2, changed state to up</td>
<td>Indicates that the interface hardware on serial interface 6/0/2 is currently active.</td>
</tr>
<tr>
<td>Line protocol on Interface Serial6/0/2, changed state to up</td>
<td>Indicates that the software processes that handle the line protocol consider the line usable for serial interface 6/0/2.</td>
</tr>
<tr>
<td>Serial6/0/2 address 2001:0DB8::248 add download succeeded</td>
<td>The IPv6 address 2001:0DB8::248 was downloaded successfully.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipv6 cef table</td>
<td>Displays debug messages for CEFv6 and dCEFv6 table modification events.</td>
</tr>
</tbody>
</table>

**debug ipv6 cef hash**

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) load-sharing hash algorithm events, use the `debug ipv6 cef hash` command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 load-sharing hash algorithm events, use the `no` form of this command.

```
ddebug ipv6 cef hash
no debug ipv6 cef hash
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging for CEFv6 and dCEFv6 load-sharing hash algorithm events is not enabled.
**debug ipv6 cef receive**

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) packets that are process-switched on the router, use the `debug ipv6 cef receive` command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 packets that are process-switched on the router, use the `no` form of this command.

```
decom bvpv6 cef receive
no debug bvpv6 cef receive
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging for CEFv6 and dCEFv6 packets that are process-switched on the router is not enabled.

**Command Modes**

Privileged EXEC
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(22)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The `debug ipv6 cef receive` command is similar to the `debug ip cef receive` command, except that it is IPv6-specific.

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the Release 12 *Cisco IOS Debug Command Reference*.

Examples

The following is sample output from the `debug ipv6 cef receive` command when another router in the network pings 2001:0DB8::2 which is a local address on this box:

```
Router# debug ipv6 cef receive
IPv6 CEF packet receives debugging is on
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6CEF-receive: Receive packet for 2001:0DB8::2</td>
<td>Cisco Express Forwarding has received a packet addressed to the router.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ipv6 cef events</code></td>
<td>Displays debug messages for CEFv6 and dCEFv6 general events.</td>
</tr>
<tr>
<td><code>debug ipv6 cef table</code></td>
<td>Displays debug messages for CEFv6 and dCEFv6 table modification events.</td>
</tr>
</tbody>
</table>
**debug ipv6 cef table**

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) table modification events, use the `debug ipv6 cef table` command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 table modification events, use the `no` form of this command.

```
debug ipv6 cef table [background]
no debug ipv6 cef table [background]
```

**Syntax Description**

- **background** (Optional) Sets CEFv6 and dCEFv6 table background updates.

**Command Default**

Debugging for CEFv6 and dCEFv6 table modification events is not enabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(22)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ipv6 cef table` command is similar to the `debug ip cef table` command, except that it is IPv6-specific. This command is used to record CEFv6 and dCEFv6 table events related to the Forwarding Information Base (FIB) tables. Types of events include the following:

- Routing updates that populate the FIB tables
- Flushing of the FIB tables
- Adding or removing of entries to the FIB tables
- Table reloading process

**Note**

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*. 
The following is sample output from the `debug ipv6 cef table` command when a static route is added:

```
Router# debug ipv6 cef table
IPv6 CEF table debugging is on
router(config)# ipv6 route 5555::/64 serial 2/0 3000::2
router(config)#
*Feb 24 08:46:09.187: IPv6CEF-Table: Event add, 5555::/64
*Feb 24 08:46:09.187: IPv6 CEF table: Created path_list 01184570
*Feb 24 08:46:09.187: IPv6 CEF table: Adding path 01181A80 to path_list 01184570 old path count=0
*Feb 24 08:46:09.187: IPv6 CEF table: No matching list for path list 01184570
*Feb 24 08:46:09.187: IPv6 CEF table: Adding fib entry 0117EE80 to path_list 01184570 old refcount=0
*Feb 24 08:46:09.187: IPv6 CEF table: Created 0 loadinfos for path_list 01184570
*Feb 24 08:46:09.187: IPv6CEF-Table: Validated 5555::/64
```

The following is sample output when the static route is removed:

```
router(config)# no ipv6 route 5555::/64 serial 2/0 3000::2
router(config)#
*Feb 24 08:46:43.871: IPv6CEF-Table: Event delete, 5555::/64
*Feb 24 08:46:43.871: IPv6CEF-Table: Invalidated 5555::/64
*Feb 24 08:46:43.871: IPv6CEF-Table: Deleted 5555::/64
*Feb 24 08:46:43.871: IPv6 CEF table: Removing fib entry 0117EE80 from path_list 01184570 old refcount=1
*Feb 24 08:46:43.871: IPv6 CEF table: Removed path_list 01184570 from path_list 01184570 hash 50
*Feb 24 08:46:43.871: IPv6 CEF table: Freeing path_list 01184570 refcount=0
*Feb 24 08:46:43.871: IPv6 CEF table: Freeing all 1 paths in path_list 01184570
*Feb 24 08:46:43.871: IPv6 CEF: deleting path 01181A80
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ipv6 cef events</code></td>
<td>Displays debug messages for CEFv6 and dCEFv6 general events.</td>
</tr>
</tbody>
</table>

### `debug ipv6 dhcp`

To enable debugging for Dynamic Host Configuration Protocol (DHCP) for IPv6, use the `debug ipv6 dhcp` command in privileged EXEC mode. To disable debugging for DHCP for IPv6, use the `no` form of this command.

```
download dhcp [detail]
download dhcp [no detail]
```

### Syntax Description

| detail | (Optional) Displays detailed information about DHCP for IPv6 message decoding. |

### Command Default

Debugging for the DHCP for IPv6 is disabled.

### Command Modes

Privileged EXEC
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(24)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(24)T.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ipv6 dhcp detail` command is used to show debug information related to the server address assignment.

**Examples**

The following example enables debugging for DHCP for IPv6:

```
Router# debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipv6 dhcp database</td>
<td>Enables debugging for the DHCP for IPv6 binding database agent.</td>
</tr>
<tr>
<td>debug ipv6 dhcp relay</td>
<td>Enables the DHCP for IPv6 relay agent debugging.</td>
</tr>
</tbody>
</table>

**debug ipv6 dhcp database**

To enable debugging for the Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent, use the `debug ipv6 dhcp database` command in privileged EXEC mode. To disable the display of debug messages for the DHCP for IPv6 binding database agent, use the `no` form of this command.

```
default ipv6 dhcp database
no debug ipv6 dhcp database
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Debugging for the DHCP for IPv6 binding database agent is disabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ipv6 dhcp database` command enables debugging for DHCP for IPv6 database processing.
The following example enables debugging for the DHCP for IPv6 binding database agent:

```plaintext
Router# debug ipv6 dhcp database
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipv6 dhcp</td>
<td>Enables debugging for DHCP for IPv6.</td>
</tr>
</tbody>
</table>

### debug ipv6 dhcp redundancy

To enable Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server redundancy debugging, use the `debug ipv6 dhcp redundancy` command in privileged EXEC mode. To disable DHCPv6 server redundancy debugging, use the `no` form of this command.

```plaintext
debug ipv6 dhcp redundancy [detail]
no debug ipv6 dhcp redundancy [detail]
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed DHCPv6 High Availability (HA) packet information.</td>
</tr>
</tbody>
</table>

#### Command Default

DHCPv6 server redundancy debugging is disabled by default.

#### Command Modes

Privileged EXEC (#)

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(1)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.5S</td>
<td>This command was integrated into Cisco IOS XE Release 3.5S.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

To debug DHCPv6 server redundancy, use the `debug ipv6 dhcp redundancy` command in privileged EXEC mode. To view detailed DHCPv6 HA packet information, use the optional `detail` keyword.

#### Examples

The following example shows how to enable DHCPv6 redundancy debugging:

```plaintext
Router# debug ipv6 dhcp redundancy
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipv6 dhcp relay</td>
<td>Enables DHCPv6 relay agent debugging.</td>
</tr>
</tbody>
</table>

### debug ipv6 dhcp relay

To enable DHCP for IPv6 relay agent debugging, use the `debug ipv6 dhcp relay` command in user EXEC or privileged EXEC mode. To disable DHCP for IPv6 relay agent debugging, use the `no` form of this command.
debug ipv6 dhcp relay [bulk-lease]
no debug ipv6 dhcp relay [bulk-lease]

Syntax Description
- **bulk-lease**: (Optional) Enables bulk lease query debugging flows.

Command Modes
- **User EXEC (>)**
- **Privileged EXEC (#)**

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(11)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
<tr>
<td>15.1(1)S</td>
<td>This command was modified. The bulk-lease keyword was added.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The DHCP functions for IPv6 client, server, and relay agent are mutually exclusive on an interface. When one of these functions is enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: Interface is in DHCP client mode, Interface is in DHCP server mode, or Interface is in DHCP relay mode.

Examples

The following example enables DHCP for IPv6 relay agent debugging:

```sh
Router# debug ipv6 dhcp relay
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipv6 dhcp</td>
<td>Enables DHCP debugging for IPv6.</td>
</tr>
</tbody>
</table>

**debug ipv6 eigrp**

To display information about the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 protocol, use the `debug ipv6 eigrp` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```sh
debug ipv6 eigrp [as-number] [{neighbor ipv6-address | notification | summary}]
no debug ipv6 eigrp
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>as-number</code></td>
</tr>
<tr>
<td><code>neighbor ipv6-address</code></td>
</tr>
<tr>
<td><code>notification</code></td>
</tr>
<tr>
<td><code>summary</code></td>
</tr>
</tbody>
</table>
debug ipv6 icmp

To display debugging messages for IPv6 Internet Control Message Protocol (ICMP) transactions (excluding IPv6 ICMP neighbor discovery transactions), use the `debug ipv6 icmp` command in privileged EXEC mode.

To disable debugging output, use the `no` form of this command.

```
debug ipv6 icmp
do debug ipv6 icmp
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

Debugging for IPv6 ICMP is not enabled.

### Command Modes

Privileged EXEC

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.2(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.0(21)ST</td>
<td>This command was integrated into Cisco IOS Release 12.0(21)ST.</td>
</tr>
<tr>
<td></td>
<td>12.0(22)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(22)S.</td>
</tr>
<tr>
<td></td>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td></td>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td></td>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Release | Modification
--- | ---
12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB | This command’s output was modified on the Cisco 10000 series router for the PRE3 and PRE4.
15.1(1)S | This command was integrated into Cisco IOS 15.1(1)S.

**Usage Guidelines**

The `debug ipv6 icmp` command is similar to the `debug ip icmp` command, except that it is IPv6-specific. When you run this command, you can view echo reply messages that are generated in response to echo requests.

---

**Note**

By default, the network server sends the output from `debug` commands and system error messages to the console. To redirect debugging output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server.

This command helps you determine whether the router is sending or receiving IPv6 ICMP messages. Use it, for example, when you are troubleshooting an end-to-end connection problem.

---

**Note**

For more information about the fields in `debug ipv6 icmp` output, refer to RFC 2463, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)*.

---

**Cisco 10000 Series Router Usage Guidelines**

In Cisco IOS Release 12.2(33)SB, output from the `debug ipv6 icmp` command displays information similar to the following:

ICMPv6: Received echo reply from 2010:1:1:1:1:1:1:2

In Cisco IOS Release 12.2(31)SB, the `debug ipv6 icmp` command output displays information similar to the following:

ICMPv6: Received ICMPv6 packet from 2010:1:1:1:1:1:2, type 129

---

**Examples**

The following is sample output from the `debug ipv6 icmp` command:

```
Router# debug ipv6 icmp
13:28:40:ICMPv6:Received ICMPv6 packet from 2000::0:0:3::2, type 136
13:28:45:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
13:28:50:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 136
13:28:55:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
```

The table below describes significant fields shown in the first line of the display.
### Table 76: debug ipv6 icmp Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:28:40:</td>
<td>Indicates the time (hours:minutes:seconds) at which the ICMP neighbor discovery event occurred.</td>
</tr>
<tr>
<td>$n , w , n , d$: (not shown in sample output)</td>
<td>Indicates time (weeks, days) since last reboot of the event occurring. For example, 1w4d: indicates the time (since the last reboot) of the event occurring was 1 week and 4 days ago.</td>
</tr>
<tr>
<td>ICMPv6:</td>
<td>Indication that this message describes an ICMP version 6 packet.</td>
</tr>
<tr>
<td>Received ICMPv6 packet from 2000:0:0:3::2</td>
<td>IPv6 address from which the ICMP version 6 packet is received.</td>
</tr>
<tr>
<td>type 136</td>
<td>The number variable indicates one of the following IPv6 ICMP message types:</td>
</tr>
<tr>
<td></td>
<td>• 1 -- Destination unreachable. The router cannot forward a packet that was sent or received.</td>
</tr>
<tr>
<td></td>
<td>• 2 -- Packet too big. The router attempts to send a packet that exceeds the maximum transmission unit (MTU) of a link between itself and the packet destination.</td>
</tr>
<tr>
<td></td>
<td>• 3 -- Time exceeded. Either the hop limit in transit or the fragment reassembly time is exceeded.</td>
</tr>
<tr>
<td></td>
<td>• 4 -- Parameter problem. The router attempts to send an IPv6 packet that contains invalid parameters. An example is a packet containing a next header type unsupported by the router that is forwarding the packet.</td>
</tr>
<tr>
<td></td>
<td>• 128 -- Echo request. The router received an echo reply.</td>
</tr>
<tr>
<td></td>
<td>• 129 -- Echo reply. The router sent an echo reply.</td>
</tr>
<tr>
<td></td>
<td>• 133 -- Router solicitation messages. Hosts send these messages to prompt routers on the local link to send router advertisement messages.</td>
</tr>
<tr>
<td></td>
<td>• 134 -- Router advertisement messages. Routers periodically send these messages to advertise their link-layer addresses, prefixes for the link, and other link-specific information. These messages are also sent in response to router solicitation messages.</td>
</tr>
<tr>
<td></td>
<td>• 135 -- Neighbor solicitation messages. Nodes send these messages to request the link-layer address of a station on the same link.</td>
</tr>
<tr>
<td></td>
<td>• 136 -- Neighbor advertisement messages. Nodes send these messages, containing their link-local addresses, in response to neighbor solicitation messages.</td>
</tr>
<tr>
<td></td>
<td>• 137 -- Redirect messages. Routers send these messages to hosts when a host attempts to use a less-than-optimal first hop address when forwarding packets. These messages contain a better first hop address that should be used instead.</td>
</tr>
</tbody>
</table>

Following are examples of the IPv6 ICMP messages types that can be displayed by the **debug ipv6 icmp** command:
• ICMP echo request and ICMP echo reply messages. In the following example, an ICMP echo request is sent to address 2052::50 and an ICMP echo reply is received from address 2052::50.

lw4d: ICMPv6: Sending echo request to 2052::50
lw4d: ICMPv6: Received echo reply from 2052::50

• ICMP packet too big messages. In the following example, a router tried to forward a packet to destination address 2052::50 via the next hop address 2052::52. The size of the packet was greater than 1280 bytes, which is the MTU of destination address 2052::50. As a result, the router receives an ICMP packet too big message from the next hop address 2052::52.

lw4d: Received ICMP too big from 2052::52 about 2052::50, MTU=1300

• ICMP parameter problem messages. In the following example, an ICMP parameter problem message is received from address 2052::52.

lw4d: Received ICMP parameter problem from 2052::52

• ICMP time exceeded messages. In the following example, an ICMP time exceeded message is received from address 2052::52.

lw4d: Received ICMP time exceeded from 2052::52

• ICMP unreachable messages. In the following example, an ICMP unreachable message with code 1 is received from address 2052::52. Additionally, an ICMP unreachable message with code 1 is sent to address 2060::20 about address 2062::20.

lw4d: Received ICMP unreachable code 1 from 2052::52
lw4d: Sending ICMP unreachable code 1 to 2060::20 about 2062::20

The table below lists the codes for ICMP unreachable messages.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The router has no route to the packet destination.</td>
</tr>
<tr>
<td>1</td>
<td>Although the router has a route to the packet destination, communication is administratively prohibited.</td>
</tr>
<tr>
<td>3</td>
<td>The address is unreachable.</td>
</tr>
<tr>
<td>4</td>
<td>The port is unreachable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>debug ipv6 nd</td>
<td>Displays debugging messages for IPv6 ICMP neighbor discovery transactions.</td>
</tr>
</tbody>
</table>
debug ipv6 icmp
debug ipv6 inspect through debug local-ack state

- debug ipv6 inspect, on page 436
- debug ipv6 mfib, on page 438
- debug ipv6 mld, on page 440
- debug ipv6 mld explicit, on page 442
- debug ipv6 mld ssm-map, on page 443
- debug ipv6 mobile, on page 444
- debug ipv6 mobile mag, on page 445
- debug ipv6 mobile networks, on page 449
- debug ipv6 mobile packets, on page 450
- debug ipv6 mobile router, on page 452
- debug ipv6 mobile mag, on page 445
- debug ipv6 mobile networks, on page 449
- debug ipv6 mobile packets, on page 450
- debug ipv6 mobile router, on page 452
- debug ipv6 mrib client, on page 453
- debug ipv6 mrib io, on page 454
- debug ipv6 mrib proxy, on page 455
- debug ipv6 mrib route, on page 456
- debug ipv6 mrib table, on page 457
- debug ipv6 multicast aaa, on page 458
- debug ipv6 multicast rpf, on page 460
- debug ipv6 multicast rwatch, on page 461
- debug ipv6 nat, on page 462
- debug ipv6 nd, on page 464
- debug ipv6 ospf, on page 467
- debug ipv6 ospf database-timer rate-limit, on page 469
- debug ipv6 ospf events, on page 470
- debug ipv6 ospf graceful-restart, on page 471
- debug ipv6 ospf lsdb, on page 473
- debug ipv6 ospf monitor, on page 474
- debug ipv6 ospf packet, on page 475
- debug ipv6 ospf spf statistic, on page 476
- debug ipv6 packet, on page 477
- debug ipv6 pim, on page 480
- debug ipv6 pim df-election, on page 482
- debug ipv6 pim limit, on page 484
- debug ipv6 policy, on page 485
• debug ipv6 pool, on page 486
• debug ipv6 rip, on page 487
• debug ipv6 routing, on page 491
• debug ipv6 snooping, on page 493
• debug ipv6 snooping raguard, on page 495
• debug ipv6 spd, on page 496
• debug ipv6 static, on page 497
• debug ipv6 wccp, on page 498
• debug ipx ipxwan, on page 500
• debug ipx nasi, on page 502
• debug ipx packet, on page 504
• debug ipx routing, on page 506
• debug ipx sap, on page 508
• debug ipx spoof, on page 513
• debug ipx spx, on page 515
• debug isdn, on page 516
• debug isdn event, on page 519
• debug isdn q921, on page 524
• debug isdn q931, on page 539
• debug isdn tgrm, on page 544
• debug isis adj packets, on page 546
• debug isis authentication, on page 547
• debug isis ipv6 rib, on page 548
• debug isis mpls traffic-eng advertisements, on page 549
• debug isis mpls traffic-eng events, on page 551
• debug isis nsf, on page 552
• debug isis rib, on page 554
• debug isis rib redistribution, on page 556
• debug isis spf statistics, on page 558
• debug isis spf-events, on page 560
• debug isis update-packets, on page 561
• debug iua as, on page 563
• debug iua asp, on page 564
• debug kerberos, on page 566
• debug kpml, on page 568
• debug kron, on page 574
• debug l2ctrl, on page 576
• debug l2fib, on page 577
• debug l2relay events, on page 579
• debug l2relay packets, on page 580
• debug l2tp, on page 581
• debug l2tp redundancy, on page 583
• debug l2vpn acircuit, on page 590
• debug l2vpn atom checkpoint, on page 592
• debug l2vpn atom event-trace, on page 594
• debug l2vpn atom fast-failure-detect, on page 595
• debug l2vpn atom signaling, on page 596
• debug l2vpn atom static-oam, on page 598
• debug l2vpn atom vc, on page 599
• debug l2vpn atom vc vccv, on page 602
• debug l2vpn pseudowire, on page 604
• debug l2vpn vfi, on page 605
• debug l2vpn xconnect, on page 606
• debug 13-mgr tunnel, on page 607
• debug 14f, on page 609
• debug lacp, on page 611
• debug lane client, on page 614
• debug lane config, on page 623
• debug lane finder, on page 625
• debug lane server, on page 626
• debug lane signaling, on page 629
• debug lapb, on page 631
• debug lapb-ta, on page 636
• debug lat packet, on page 638
• debug ldap, on page 640
• debug lex rcmd, on page 642
• debug license, on page 645
• debug link monitor, on page 647
• debug list, on page 648
• debug llc2 dynwind, on page 651
• debug llc2 errors, on page 652
• debug llc2 packet, on page 653
• debug llc2 state, on page 655
• debug lnm events, on page 656
• debug lnm llc, on page 659
• debug lnm mac, on page 662
• debug local-ack state, on page 664
debug ipv6 inspect

To display messages about Cisco IOS firewall events, use the `debug ipv6 inspect` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ipv6 inspect \{function-trace | object-creation | object-deletion | events | timers | protocol | detailed\}
no debug ipv6 inspect detailed
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>function-trace</td>
<td>Displays messages about software functions called by the Cisco IOS firewall.</td>
</tr>
<tr>
<td>object-creation</td>
<td>Displays messages about software objects being created by the Cisco IOS firewall. Object creation corresponds to the beginning of Cisco IOS firewall-inspected sessions.</td>
</tr>
<tr>
<td>object-deletion</td>
<td>Displays messages about software objects being deleted by the Cisco IOS firewall. Object deletion corresponds to the closing of Cisco IOS firewall-inspected sessions.</td>
</tr>
<tr>
<td>events</td>
<td>Displays messages about Cisco IOS firewall software events, including information about Cisco IOS firewall packet processing.</td>
</tr>
<tr>
<td>timers</td>
<td>Displays messages about Cisco IOS firewall timer events such as when a Cisco IOS firewall idle timeout is reached.</td>
</tr>
<tr>
<td>protocol</td>
<td>Displays messages about Cisco IOS firewall-inspected protocol events, including details about the protocol's packets.</td>
</tr>
<tr>
<td>detailed</td>
<td>Use this form of the command in conjunction with other Cisco IOS firewall debugging commands. This causes detailed information to be displayed for all the other enabled Cisco IOS firewall debugging.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)T</td>
<td>This command was introduced</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(22)S.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>
The following example enables the display of messages about Cisco IOS firewall events:

```
debug ipv6 inspect
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 inspect audit-trail</td>
<td>Turns on CBAC audit trail messages, which are displayed on the console after each Cisco IOS firewall session closes.</td>
</tr>
<tr>
<td>ipv6 inspect name</td>
<td>Defines a set of ipv6 inspection rules.</td>
</tr>
<tr>
<td>show ipv6 inspect</td>
<td>Displays CBAC configuration and session information.</td>
</tr>
</tbody>
</table>
debug ipv6 mfib

To enable debugging output on the IPv6 Multicast Forwarding Information Base (MFIB), use the `debug ipv6 mfib` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ipv6 mfib [vrf vrf-name] [{group-name|group-address}] [{adjacency | db | fs | init | interface | mrib | detail | nat | pak | platform | ppr | ps | signal | table}]
```

```
no debug ipv6 mfib
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>group-name</td>
<td>(Optional) IPv6 address, name, or interface of the multicast group as defined</td>
</tr>
<tr>
<td>group-address</td>
<td>in the Domain Name System (DNS) hosts table.</td>
</tr>
<tr>
<td>adjacency</td>
<td>(Optional) Enables debugging output for adjacency management activity.</td>
</tr>
<tr>
<td>db</td>
<td>(Optional) Enables debugging output for route database management activity.</td>
</tr>
<tr>
<td>fs</td>
<td>(Optional) Enables debugging output for fast switching activity.</td>
</tr>
<tr>
<td>init</td>
<td>(Optional) Enables debugging output for initialization or deinitialization activity.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Enables debugging output for IPv6 MFIB interfaces.</td>
</tr>
<tr>
<td>mrib</td>
<td>(Optional) Enables debugging output for communication with the MRIB.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Enables detailed debugging output regarding the MRIB.</td>
</tr>
<tr>
<td>nat</td>
<td>(Optional) Enables debugging output for Network Address Translation (NAT)</td>
</tr>
<tr>
<td></td>
<td>events associated with all tables.</td>
</tr>
<tr>
<td>pak</td>
<td>(Optional) Enables debugging output for packet forwarding activity.</td>
</tr>
<tr>
<td>platform</td>
<td>(Optional) Enables debugging output related to the hardware platform use of</td>
</tr>
<tr>
<td></td>
<td>application program interfaces (APIs).</td>
</tr>
<tr>
<td>ppr</td>
<td>(Optional) Enables debugging output for packet preservation events.</td>
</tr>
<tr>
<td>ps</td>
<td>(Optional) Enables debugging output for process-level-only packet forwarding</td>
</tr>
<tr>
<td></td>
<td>activity.</td>
</tr>
<tr>
<td>signal</td>
<td>(Optional) Enables debugging output for activity regarding MFIB data-driven</td>
</tr>
<tr>
<td></td>
<td>signaling to routing protocols.</td>
</tr>
<tr>
<td>table</td>
<td>(Optional) Enables debugging output for IPv6 MFIB table activity.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC
### Usage Guidelines

If no keywords are used, all IPv6 MFIB activity debugging output is displayed.

### Examples

The following example enables debugging output for adjacency management activity on the IPv6 MFIB:

```
Router# debug ipv6 mfib adjacency
```
debug ipv6 mld

To enable debugging on Multicast Listener Discovery (MLD) protocol activity, use the `debug ipv6 mld` command in privileged EXEC mode. To restore the default value, use the `no` form of this command.

```
done ipv6 mld [{group-namegroup-addressinterface-type}]
no debug ipv6 mld [{group-namegroup-addressinterface-type}]
```

Cisco IOS Release 12.0(26)S
`debug ipv6 mld [{group group-namegroup-address | interface interface-type}]`
`no debug ipv6 mld [{group group-namegroup-address | interface interface-type}]`

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group-name</code></td>
<td>(Optional) IPv6 address or name of the multicast group.</td>
</tr>
<tr>
<td><code>group-address</code></td>
<td>(Optional) IPv6 address or name of the multicast group.</td>
</tr>
<tr>
<td><code>interface-type</code></td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(26)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on Cisco ASR 1000 Series Routers.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command helps discover whether the MLD protocol activities are working correctly. In general, if MLD is not working, the router process never discovers that there is a host on the network that is configured to receive multicast packets.

The messages displayed by the `debug ipv6 mld` command show query and report activity received from other routers and hosts. Use this command in conjunction with `debug ipv6 pim` to display additional multicast activity, to learn more information about the multicast routing process, or to learn why packets are forwarded out of particular interfaces.

### Examples

The following example enables debugging on MLD protocol activity:
Router# debug ipv6 mld

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>debug ipv6 pim</td>
<td>Enables debugging on PIM protocol activity.</td>
</tr>
</tbody>
</table>
debug ipv6 mld explicit

To display information related to the explicit tracking of hosts, use the `debug ipv6 mld explicit` command in privileged EXEC mode. To disable debugging, use the `no` form of this command.

```
depbug ipv6 mld explicit [{group-name|group-address}]
no debug ipv6 mld explicit [{group-name|group-address}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>group-name</th>
<th>group-address</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) IPv6 address or name of the multicast group.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

Debugging for the explicit tracking of hosts is not enabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on Cisco ASR 1000 Series Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the optional `group-name` or `group-address` argument is not used, all debugging information is displayed.

**Examples**

The following example shows how to enable information to be displayed about the explicit tracking of hosts. The command output is self-explanatory:

```
Router# debug ipv6 mld explicit
00:00:56:MLD:ET host FE80::A8BB:CCFF:FE00:800 report for FF05::6 (0 srcs) on Ethernet1/0
00:00:56:MLD:ET host FE80::A8BB:CCFF:FE00:800 switch to exclude for FF05::6 on Ethernet1/0
00:00:56:MLD:ET MRIB modify for (*,FF05::6) on Ethernet1/0 new 100, mdf 100
```
debug ipv6 mld ssm-map

To display debug messages for Source Specific Multicast (SSM) mapping related to Multicast Listener Discovery (MLD), use the `debug ipv6 mld ssm-map` command in privileged EXEC mode. To disable debug messages for SSM mapping, use the `no` form of this command.

```
debug ipv6 mld ssm-map [source-address]
no debug ipv6 mld ssm-map [source-address]
```

### Syntax Description

| source-address | (Optional) Source address associated with an MLD membership for a group identified by the access list. |

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SXE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Consult Cisco technical support before using this command.

### Examples

The following example allows debugging information for SSM mapping to be displayed:

```
Router# debug ipv6 mld ssm-map
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 mld ssm-map enable</code></td>
<td>Enables the SSM mapping feature for groups in the configured SSM range.</td>
</tr>
<tr>
<td><code>ipv6 mld ssm-map query dns</code></td>
<td>Enables DNS-based SSM mapping.</td>
</tr>
<tr>
<td><code>ipv6 mld ssm-map static</code></td>
<td>Configures static SSM mappings.</td>
</tr>
<tr>
<td><code>show ipv6 mld ssm-map</code></td>
<td>Displays SSM mapping information.</td>
</tr>
</tbody>
</table>
debug ipv6 mobile

To enable the display of debugging information for Mobile IPv6, use the `debug ipv6 mobile` command in privileged EXEC mode.

```
debug ipv6 mobile {binding-cache | forwarding | home-agent | registration}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>binding-cache</td>
<td>Events associated with the binding cache.</td>
</tr>
<tr>
<td>forwarding</td>
<td>Events associated with forwarding (tunneling) packets for which the router is acting as home agent.</td>
</tr>
<tr>
<td>home-agent</td>
<td>Events associated with the home agent, Dynamic Home Address Agent Discovery (DHAAD), Mobile prefix discovery (MPD), and generic home agent (HA) debugging and binding acknowledgments.</td>
</tr>
<tr>
<td>registration</td>
<td>Events associated with binding updates that are registrations.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ipv6 mobile` command enables the display of selected debugging information. You may use multiple command lines to enable concurrent debugging of multiple classes of information.

**Examples**

In the following example, debugging information is displayed for binding updates processing:

```
Router# debug ipv6 mobile registration
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>binding</td>
<td>Configures binding options for the Mobile IPv6 home agent feature in home-agent configuration mode.</td>
</tr>
<tr>
<td>ipv6 mobile home-agent (global configuration)</td>
<td>Enters home agent configuration mode.</td>
</tr>
<tr>
<td>ipv6 mobile home-agent (interface configuration)</td>
<td>Initializes and start the IPv6 Mobile home agent on a specific interface.</td>
</tr>
<tr>
<td>ipv6 mobile home-agent preference</td>
<td>Configures the home agent preference value on the interface.</td>
</tr>
</tbody>
</table>
**debug ipv6 mobile mag**

To debug the Mobile Access Gateway (MAG) application programming interface (API), information, or events, use the `debug ipv6 mobile mag` command in privileged EXEC mode. To disable display of the debugging output, use the `no` form of this command.

```
depbug ipv6 mobile mag  {api | events | info}
no debug ipv6 mobile mag  {api | events | info}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>api</td>
<td>Enables API-specific debug events.</td>
</tr>
<tr>
<td>events</td>
<td>Enables all events occurring within the Local Mobility Anchor (LMA) and the MAG.</td>
</tr>
<tr>
<td>info</td>
<td>Provides debug information within the Proxy Mobile IPv6 (PMIPv6) module.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging is not enabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.4S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(4)M</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)M.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ipv6 mobile mag events` command to enable events occurring within the LMA and MAG. The following table lists the common causes for Proxy Binding Update (PBU) rejections:

<table>
<thead>
<tr>
<th>PBU Reject Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMIPv6_BA_ACCEPTED</td>
<td>The PBU is accepted.</td>
</tr>
<tr>
<td>GRE_KEY_OPTION_NOT_REQUIRED</td>
<td>The PBU is processed successfully but the GRE encapsulation and GRE keys are not required.</td>
</tr>
<tr>
<td>PMIPv6_BA_UNSPEC_FAIL</td>
<td>The PBU is rejected for an unspecified reason.</td>
</tr>
<tr>
<td>PMIPv6_BA_ADMIN_FAIL</td>
<td>The PBU is rejected due to administrative reasons.</td>
</tr>
<tr>
<td>PMIPv6_BA_Resource_FAIL</td>
<td>The PBU is rejected due to insufficient resources.</td>
</tr>
<tr>
<td>PMIPv6_BA_HM_REG_FAIL</td>
<td>The PBU is rejected because it has an unsupported home registration.</td>
</tr>
<tr>
<td>PMIPv6_BA_HM_SUBNET_FAIL</td>
<td>The PBU is rejected because the current subnet is not the home subnet.</td>
</tr>
<tr>
<td>PMIPv6_BA_BAD_SEQ_FAIL</td>
<td>The PBU is rejected because the sequence number is out of the specified range.</td>
</tr>
</tbody>
</table>
### PBU Reject Status

<table>
<thead>
<tr>
<th>PBU Reject Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMIPV6_BA_CHANGE_FAIL</td>
<td>The PBU is rejected because the registration type has changed.</td>
</tr>
<tr>
<td>PMIPV6_BA_AUTH_FAIL</td>
<td>The PBU is rejected because the authorization has failed.</td>
</tr>
<tr>
<td>PROXY_REG_NOT_ENABLED</td>
<td>The PBU is rejected because the registration of the proxy is not enabled for the mobile node.</td>
</tr>
<tr>
<td>NOT_LMA_FOR_THIS_MOBILE_NODE</td>
<td>The PBU is rejected because the current Local Mobility Anchor (LMA) is not the appropriate LMA for the mobile node.</td>
</tr>
<tr>
<td>MAG_NOT_AUTHORIZED_FOR_PROXY_REG</td>
<td>The PBU is rejected because the Mobile Access Gateway (MAG) is not authorized to send PBUs.</td>
</tr>
<tr>
<td>NOT_AUTHORIZED_FOR_HNP</td>
<td>The PBU is rejected because it is not authorized for the Home Network Prefix (HNP).</td>
</tr>
<tr>
<td>TIMESTAMP_MISMATCH</td>
<td>The PBU is rejected because it has an invalid timestamp value.</td>
</tr>
<tr>
<td>TIMESTAMP_LOWER_THAN_PREV_ACCEPTED</td>
<td>This PBU is rejected because the timestamp value is lower than the previously accepted value.</td>
</tr>
<tr>
<td>MISSING_HNP_OPTION</td>
<td>The PBU is rejected because it is the Home Network Prefix (HNP) option.</td>
</tr>
<tr>
<td>BCE_PBU_PREFIX_SET_DO_NOT_MATCH</td>
<td>The PBU is rejected because the Home Network Prefixes (HNPs) that are received in the PBU do not match with the Binding Cache Entry (BCE).</td>
</tr>
<tr>
<td>MISSING_MN_IDENTIFIER_OPTION</td>
<td>The PBU is rejected because the mobile node identifier option is missing.</td>
</tr>
<tr>
<td>MISSING_HANDOFF_INDICATOR_OPTION</td>
<td>The PBU is rejected because the Handoff Indicator is missing.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `debug ipv6 mobile mag api` command displays the APIs that are called during the call setup flow:

```
Device# debug ipv6 mobile mag api
07:52:08.051: MIP_PDL_API: pmipv6_pdl_get_att API Called
07:52:08.051: [PMIPv6_BINDING_API]: pmipv6_get_binding API called
07:52:08.051: [PMIPv6_BINDING_API]: pmipv6_get_binding API called
07:52:08.051: [PMIPv6_MAG_API]: mag_bul_do_state_transition API called
07:52:08.051: [PMIPv6_MAG_API]: pmipv6_mag_bul_null_state_hndlr API called
07:52:08.051: [PMIPv6_MAG_API]: pmipv6_mag_bul_null_state_exit API called
07:52:08.051: [PMIPv6_BINDING_API]: pmipv6_get_binding API called
07:52:08.051: [PMIPv6_BINDING_API]: pmipv6_get_binding API called
07:52:08.053: [PMIPv6_MAG_API]: pmipv6_mag_should_handle_pkt called
07:52:08.053: [PMIPv6_MAG_API]: pmipv6_mag_message_handler called
07:52:08.053: [PMIPv6_BINDING_API]: pmipv6_get_binding API called
07:52:08.053: [PMIPv6_BINDING_API]: pmipv6_get_binding API called
```
The following is sample output from the `debug ipv6 mobile mag events` command:

```
Device# debug ipv6 mobile mag events
PMIPv6 MAG Event debug is turned on

The following line shows that the DHCP Discover trigger is received from the mobile node (MN):

07:48:31.638: [PMIPv6_MAG_EVENT]: Trigger request received (DHCP Discover trigger) from (example3@example.com)

The following line shows the MAG machine state change. A new MN attaches to the MAG and the state changes from NULL to INIT:

07:48:31.638: [PMIPv6_MAG_EVENT]: Event received New MN intf attached in state: NULL, new state: INIT

The following line shows that the Proxy Binding Update (PBU) message is sent from a MAG to an MN:

07:48:31.638: [PMIPv6_MAG_EVENT]: PBU message sent

The following lines show that the Proxy Binding Acknowledgment (PBA) is received from the LMA for the MN. The incoming parameters are link layer identifier (lli) length, value, and access technology type (att). The status 0 indicates success.

07:48:31.639: [PMIPv6_MAG_EVENT]: message received: PBA
07:48:31.639: [PMIPv6_MAG_EVENT]: PBA: nai(example3@example.com), nai len: 14, lli (aabb.cc00.ce00), ll len: 16, att:3, status:0

The following line shows that the refresh timer has started:

07:48:31.639: [PMIPv6_MAG_EVENT]: Starting Refresh timer, period (300000)

The following lines show that a v4 route is added to the MN, which has a new address assigned. A new v6 tunnel is created and a reverse tunnel entry is added for the MN.
```
The following lines show that a new binding is created and added to the AV tree:

```
07:50:31.714: [PMIPv6_PDB_INFO]: MN entry example3@example.com found in hashset
07:50:31.714: [PMIPv6_BINDING_INFO]: binding added New NAI AVL node created
```

The following line provides more information about the PBU's that are sent:

```
07:50:31.714: [PMIPv6_MAG_INFO]: PBU message nai(example3@example.com), nai len: 14, hoa(0), att(3) llid(aabb.cc00.ce00) , li len: 16
```

The following lines show that a binding for the MN using the Network Access Identifier (NAI) example3@example.com is found:

```
07:50:31.717: [PMIPv6_BINDING_INFO_KEY]: Keytype as NAI. NAI: example3@example.com
07:50:31.717: [PMIPv6_BINDING_INFO]: binding found on NAI tree
```

The following line shows that a virtual interface is created in the MAG and assigned the MAC address aaaa.aaaa.aaaa:

```
07:50:31.717: [PMIPv6_MAG_EVENT]: Creating virtual interface handle (IFNAME_PMIP_VIF4)
07:50:31.717: [PMIPv6_MAG_INFO]: Setting Mac Address (aaaa.aaaa.aaaa) on (IFNAME_PMIP_VIF4)
```

The following line shows a route for the MN is added in the MAG:

```
07:50:31.717: MIP_PDL_INFO: Route via: GigabitEthernet0/1/0 (IPv6)
```

The following line shows that a tunnel is created with a source address and a destination address:

```
07:50:31.718: MIP_PDL_INFO: Tunnel0 (IPv6) created with src 2000::4 dst 2001::2
07:50:31.718: MIP_PDL_INFO: Rev. Tunnel acl entry added for subnet (10.10.0.0)
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 mobile pmipv6-mag</code></td>
<td>Configures the MAG for the PMIPv6 domain.</td>
</tr>
</tbody>
</table>
**debug ipv6 mobile networks**

To display debugging messages for IPv6 mobile networks, use the `debug ipv6 mobile networks` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ipv6 mobile networks
no debug ipv6 mobile networks
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ipv6 mobile networks` command enables the display of selected debugging information.

**Examples**

The following example shows how to enable the display of debugging messages for IPv6 mobile networks:

```
Router# debug ipv6 mobile networks
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 mobile router</td>
<td>Enables IPv6 NEMO functionality on a router and places the router in IPv6 mobile router configuration mode.</td>
</tr>
</tbody>
</table>
**debug ipv6 mobile packets**

To debug the proxy mobile IPv4 or IPv6 packets, use the `debug ipv6 mobile packets` command in privileged EXEC mode. To disable the debugging output, use the `no` form of this command.

```
debug ipv6 mobile packets
no debug ipv6 mobile packets
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging is not enabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.4S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(4)M</td>
<td>This command was integrated into Cisco IOS Releases 15.2(4)M.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug ipv6 mobile packets` command:

```
Device# debug ipv6 mobile packets
PMIPv6 FKT debug is turned on
The following lines show the newly allocated packet size and the inner packet details:

07:51:17.693: [PMIPv6-MM]:Allocated packet of size 164 with tlv length 84
07:51:17.693: [PMIPv6-MM] Sending UDP Packet, src: 0x2020202, dst: 0x6060602, sport: 5436, dport:5436

The following lines show the mobility options, the value, and the length:

07:51:17.693: [PMIPv6-MM] NAI option included len 14
  2A986107E0: 4D 4E334063 6973636F ..example3@example
  2A986107F0: 2E636F6D 1702 ..com..
07:51:17.693: [PMIPv6-MM] HI option included len 2 val 4
07:51:17.694: [PMIPv6-MM] ATT option included len 2 val 3
07:51:17.694: [PMIPv6-MM] TIMESTAMP option included len 8 value 3517199477
07:51:17.694: [PMIPv6-MM] LLI option included len 16
  2A98610810: 61616262 2E633630 302E6365 30300100 aabb.cc00.ce00..
  2A98610820: 24 $
07:51:17.694: [PMIPv6-MM] V4HOAREQ option included len 6 val 0.0.0.0
07:51:17.694: [PMIPv6-MM] V4DFT_RTR option included len 6 val 0.0.0.0
07:51:17.694: **** Dumping the TLVs ****
  2A986107E0: 01020000 080E014D 4E334063 6973636F ..example3@example
```
The following lines show the dump of the packet with all the Type Length Values (TLVs):

```
07:51:17.696: **** Dumping the TLVs ****
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 mobile pmipv6-mag</code></td>
<td>Configures the MAG for the PMIPv6 domain.</td>
</tr>
</tbody>
</table>
debug ipv6 mobile router

To display debugging messages for the IPv6 mobile router, use the debug ipv6 mobile router command in privileged EXEC mode. To disable debugging output, use the no form of this command.

```
default ipv6 mobile router [detail]
no debug ipv6 mobile router
```

**Syntax Description**

- `detail` (Optional) Displays detailed mobile router debug messages.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The IPv6 mobile router operations can be debugged. The following conditions trigger debugging messages:

- Agent discovery
- Registration
- Mobile router state change
- Routes and tunnels created or deleted
- Roaming information

Debugging messages are prefixed with "MobRtr," and detail messages are prefixed with "MobRtrX."

**Examples**

The following example shows how to enable the display of debugging messages for the IPv6 mobile router:

```
Router# debug ipv6 mobile router
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 mobile router</td>
<td>Enables IPv6 NEMO functionality on a router and places the router in IPv6 mobile router configuration mode.</td>
</tr>
</tbody>
</table>
**debug ipv6 mrib client**

To enable debugging on Multicast Routing Information Base (MRIB) client management activity, use the `debug ipv6 mrib client` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
d debug ipv6 mrib [vrf vrf-name] client
no debug ipv6 mrib client
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a virtual routing and forwarding (VRF) configuration.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(26)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on Cisco ASR 1000 Series Routers.</td>
</tr>
<tr>
<td>15.1(4)M</td>
<td>The <code>vrf vrf-name</code> keyword and argument were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ipv6 mrib client` command is used to display the activity in the MRIB associated with clients such as Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD). If you are having difficulty with your client connections, use this command to display new clients being added and deleted.

The `debug ipv6 mrib client` command also displays information on when a new client is added to or deleted from the MRIB, when a client connection is established or torn down, when a client binds to a particular MRIB table, and when a client is informed that there are updates to be read.

**Examples**

The following example enables debugging on MRIB client management activity:

```
Router# debug ipv6 mrib client
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipv6 mrib route</td>
<td>Displays MRIB routing entry-related activity.</td>
</tr>
</tbody>
</table>
debug ipv6 mrib io

To enable debugging on Multicast Routing Information Base (MRIB) I/O events, use the `debug ipv6 mrib io` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

`debug ipv6 mrib [vrf vrf-name] io`  
`no debug ipv6 mrib io`

**Syntax Description**

| vrf vrf-name | (Optional) Specifies a virtual routing and forwarding (VRF) configuration. |

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(26)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on Cisco ASR 1000 Series Routers.</td>
</tr>
<tr>
<td>15.1(4)M</td>
<td>The <code>vrf vrf-name</code> keyword and argument were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ipv6 mrib io` command to display information on when clients open and close MRIB I/O connections, when MRIB entry and interface updates are received and processed from clients, and when MRIB entry and interface updates are sent to clients.

**Examples**

The following example enables debugging on MRIB I/O events:

```
Router# debug ipv6 mrib io
```
debug ipv6 mrib proxy

To enable debugging on multicast routing information base (MRIB) proxy activity between the route processor and line cards on distributed router platforms, use the `debug ipv6 mrib proxy` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
diag 1000 2000
no debug ipv6 mrib proxy
```

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(26)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on Cisco ASR 1000 Series Routers.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the `debug ipv6 mrib proxy` command to display information on connections that are being opened and closed and on MRIB transaction messages that are being passed between the route processor and line cards.

Examples

The following example enables debugging on MRIB proxy events:

```
Router# debug ipv6 mrib proxy
```
**debug ipv6 mrib route**

To display information about Multicast Routing Information Base (MRIB) routing entry-related activity, use the `debug ipv6 mrib route` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
dbg ipv6 mrib [vrf vrf-name] route [{group-name} group-address]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>group-name</td>
<td>(Optional) IPv6 address or name of the multicast group.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(26)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on Cisco ASR 1000 Series Routers.</td>
</tr>
<tr>
<td>15.1(4)M</td>
<td>The <code>vrf vrf-name</code> keyword and argument were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays update information related to the route database made by MRIB clients, which is then redistributed to the clients.

Use this command to monitor MRIB route activity when discontinuity is found between the MRIB and the client database or between the individual client databases.

**Examples**

The following example enables the display of information about MRIB routing entry-related activity:

```
Router# debug ipv6 mrib route
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 mrib client</td>
<td>Displays information about the MRIB client management activity.</td>
</tr>
</tbody>
</table>
debug ipv6 mrib table

To enable debugging on Multicast Routing Information Base (MRIB) table management activity, use the `debug ipv6 mrib table` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ipv6 mrib [vrf vrf-name] table
no debug ipv6 mrib table
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a virtual routing and forwarding (VRF) configuration.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(26)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on Cisco ASR 1000 Series Routers.</td>
</tr>
<tr>
<td>15.1(4)M</td>
<td>The <code>vrf vrf-name</code> keyword and argument were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ipv6 mrib table` command to display information on new MRIB tables being added and deleted.

**Examples**

The following example enables debugging on MRIB table management activity:

```
Router# debug ipv6 mrib table
```
debug ipv6 multicast aaa

To enable debugging of authentication, authorization, and accounting (AAA) events related to IPv6 multicast routing, use the **debug ipv6 multicast aaa** command in privileged EXEC mode. To disable debugging of events, use the **no** form of this command.

```
def debug ipv6 multicast aaa { detail | error | verbose }
no debug ipv6 multicast aaa { detail | error | verbose }
```

**Syntax Description**
- **aaa** Enables debugging of IPv6 AAA events.
- **detail** Enables debugging of IPv6 multicast AAA details.
- **error** Enables debugging of IPv6 multicast AAA errors.
- **verbose** Enables debugging of IPv6 multicast AAA verbose.

**Command Modes**
- Privileged EXEC(#)

**Command History**
- **Release** modification
  - 15.3(1)S This command was introduced.

**Usage Guidelines**
You must configure multicast routing in an IPv6 environment. Use the **ipv6 multicast-routing** command in global configuration mode to enable IPv6 multicast routing. The **ipv6 multicast-routing** command applies on all IPv6-enabled interfaces on a device, which are then automatically enabled for Protocol-Independent Multicast version 6 (PIMv6). PIM is used between devices so that the devices can track which multicast packets to forward to each other and to the devices that are on the directly connected LANs.

**Command Example**
The following example shows how to enable debugging of IPv6 multicast AAA information:

```
Device# debug ipv6 multicast aaa detail
AAA details debugging is on
Device# debug ipv6 multicast aaa error
AAA errors debugging is on
Device# debug ipv6 multicast aaa verbose
AAA verbose debugging is on
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ipv6 multicast-routing</td>
<td>Enables multicast routing using MLD on all IPv6-enabled interfaces of the device and enables multicast forwarding.</td>
</tr>
</tbody>
</table>
debug ipv6 multicast rpf

To enable debugging of Reverse Path Forwarding (RPF) events related to IPv6 multicast routing, use the `debug ipv6 multicast rpf` command in privileged EXEC mode. To disable debugging of events, use the `no` form of this command.

```
debug ipv6 multicast rpf
no debug ipv6 multicast rpf
```

### Syntax Description

| rpf | Enables debugging of IPv6 multicast RPF events. |

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3(1)S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

You must configure multicast routing in an IPv6 environment. Use the `ipv6 multicast-routing` command in global configuration mode to enable IPv6 multicast routing. The `ipv6 multicast-routing` command applies on all IPv6-enabled interfaces on a device, which are then automatically enabled for Protocol-Independent Multicast version 6 (PIMv6). PIM is used between devices so that the devices can track which multicast packets to forward to each other and to the devices that are on the directly connected LANs.

### Command Example

The following example shows how to enable debugging of IPv6 multicast RPF events:

```
Device# debug ipv6 multicast rpf
IPv6 Multicast RPF debugging is on
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 multicast-routing</code></td>
<td>Enables multicast routing using MLD on all IPv6-enabled interfaces of the device and enables multicast forwarding.</td>
</tr>
</tbody>
</table>
debug ipv6 multicast rwatch

To enable debugging of route watch tracking events related to IPv6 multicast routing, use the `debug ipv6 multicast rwatch` command in privileged EXEC mode. To disable debugging of events, use the `no` form of this command.

```
devagle# debug ipv6 multicast rwatch
IPv6 Route-watch debugging is on
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>rwatch</code></td>
<td>Enables debugging of IPv6 multicast route watch tracking events.</td>
</tr>
</tbody>
</table>

**Command Modes**

- Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3(1S)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure multicast routing in an IPv6 environment. Use the `ipv6 multicast-routing` command in global configuration mode to enable IPv6 multicast routing. The `ipv6 multicast-routing` command applies on all IPv6-enabled interfaces on a device, which are then automatically enabled for Protocol-Independent Multicast version 6 (PIMv6). PIM is used between devices so that the devices can track which multicast packets to forward to each other and to the devices that are on the directly connected LANs.

**Command Example**

The following example shows how to enable debugging of IPv6 multicast route watch tracking events:

```
devagle# debug ipv6 multicast rwatch
IPv6 Route-watch debugging is on
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 multicast-routing</code></td>
<td>Enables multicast routing using MLD on all IPv6-enabled interfaces of the device and enables multicast forwarding.</td>
</tr>
</tbody>
</table>
debug ipv6 nat

To display debug messages for Network Address Translation--Protocol Translation (NAT-PT) translation events, use the `debug ipv6 nat` command in privileged EXEC mode. To disable debug messages for NAT-PT translation events, use the `no` form of this command.

```
debug ipv6 nat [{detailed | port}]
no debug ipv6 nat [{detailed | port}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detailed</td>
<td>(Optional) Displays detailed information about NAT-PT translation events.</td>
</tr>
<tr>
<td>port</td>
<td>(Optional) Displays port allocation events.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging for NAT-PT translation events is not enabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(2)T</td>
<td>The <code>port</code> keyword was added to support Port Address Translation (PAT), or overload, multiplexing multiple IPv6 addresses to a single IPv4 address or to an IPv4 address pool.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ipv6 nat` command can be used to troubleshoot NAT-PT translation issues. If no keywords are specified, debugging messages for all NAT-PT protocol translation events are displayed.

**Note**

By default, the network server sends the output from `debug` commands and system error messages to the console. To redirect debugging output, use the `logging` command options within global configuration mode. Destinations are the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server.

**Caution**

Because the `debug ipv6 nat` command generates a substantial amount of output, use it only when traffic on the IPv6 network is low, so other activity on the system is not adversely affected.

**Examples**

The following example shows output for the `debug ipv6 nat` command:

```
Router# debug ipv6 nat
00:06:06: IPv6 NAT: icmp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: icmp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) -> (3002::8)
00:06:06: IPv6 NAT: icmp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: icmp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) -> (3002::8)
```
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) -> (3002::8)
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) -> (3002::8)

The table below describes the significant fields shown in the display.

### Table 78: debug ipv6 nat Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 NAT:</td>
<td>Indicates that this is a NAT-PT packet.</td>
</tr>
<tr>
<td>icmp</td>
<td>Protocol of the packet being translated.</td>
</tr>
<tr>
<td>src (3000::8)-&gt;(192.168.124.8)</td>
<td>The source IPv6 address and the NAT-PT mapped IPv4 address. Note If mapping IPv4 hosts to IPv6 hosts the first address would be an IPv4 address, and the second address an IPv6 address.</td>
</tr>
<tr>
<td>dst (2001::2)-&gt;(192.168.123.2)</td>
<td>The destination IPv6 address and the NAT-PT mapped IPv4 address. Note If mapping IPv4 hosts to IPv6 hosts the first address would be an IPv4 address, and the second address an IPv6 address.</td>
</tr>
</tbody>
</table>

The following example shows output for the `debug ipv6 nat` command with the detailed keyword:

Router# debug ipv6 nat detailed
00:14:12: IPv6 NAT: address allocated 192.168.124.8
00:14:16: IPv6 NAT: deleted a NAT entry after timeout
**debug ipv6 nd**

To display debug messages for IPv6 Internet Control Message Protocol (ICMP) neighbor discovery transactions, use the `debug ipv6 nd` command in privileged EXEC mode. To disable debug messages for IPv6 ICMP neighbor discovery transactions, use the `no` form of this command.

```
ddebug ipv6 nd

no debug ipv6 nd
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging for IPv6 ICMP neighbor discovery is not enabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(4)T</td>
<td>The DAD: <code>&lt;nnnn :: nn :&gt;</code> is unique, DAD: duplicate link-local <code>&lt;nnnn :: nn :&gt;</code> on <code>&lt;interface type &gt;</code>, interface stalled, and Received NA for <code>&lt;nnnn :: nn :&gt;</code> on <code>&lt;interface type &gt;</code> from <code>&lt;nnnn :: nn :&gt;</code> fields were added to the command output.</td>
</tr>
<tr>
<td>12.0(21)ST</td>
<td>This command was integrated into Cisco IOS Release 12.0(21)ST.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(22)S.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command can help determine whether the router is sending or receiving IPv6 ICMP neighbor discovery messages.

**Note**

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

**Examples**

The following example shows output for the `debug ipv6 nd` command:
The table below describes the significant fields shown in the display.

**Table 79: debug ipv6 nd Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:22:40:</td>
<td>Indicates the time (hours:minutes:seconds) at which the ICMP neighbor discovery event occurred.</td>
</tr>
<tr>
<td>ICMPv6-ND</td>
<td>Indicates that a state change is occurring for an entry in the IPv6 neighbors cache.</td>
</tr>
<tr>
<td>STALE</td>
<td>Stale state. This state of an neighbor discovery cache entry used to be &quot;reachable,&quot; but is now is &quot;stale&quot; due to the entry not being used. In order to use this address, the router must go through the neighbor discovery process in order to confirm reachability.</td>
</tr>
<tr>
<td>DELAY</td>
<td>Delayed state. Reachability for this ND cache entry is currently being reconfirmed. While in the delay state, upper-layer protocols may inform IPv6 that they have confirmed reachability to the entry. Therefore, there is no need to send a neighbor solicitation for the entry.</td>
</tr>
<tr>
<td>PROBE</td>
<td>Probe state. While in the probe state, if no confirmation is received from the upper-layer protocols about the reachability of the entry, a neighbor solicitation message is sent. The entry remains in the &quot;probe&quot; state until a neighbor advertisement message is received in response to the neighbor solicitation message.</td>
</tr>
<tr>
<td>Sending NS for...</td>
<td>Sending a neighbor solicitation message. In the example output, a neighbor solicitation message is sent on Fast Ethernet interface 0/0 to determine the link-layer address of 2000:0:0:3::2 on Fast Ethernet interface 0/0.</td>
</tr>
</tbody>
</table>
Received a neighbor advertisement message. In the example output, a neighbor advertisement message is received from the address 2000::0:3::2 (the second address) that includes the link-layer address of 2000::0:3::2 (first address) from Ethernet interface 0/0.

REACH
Reachable state. An ND cache entry in this state is considered reachable, and the corresponding link-layer address can be used without needing to perform neighbor discovery on the address.

Received neighbor solicitations. In the example output, the address FE80::203:A0FF:FED6:1400 (on Fast Ethernet interface 0/0) is trying to determine the link-local address of 2000::0:3::1.

Sending neighbor advertisements. In the example output, a neighbor advertisement containing the link-layer address of 2000::0:3::1 (an address assigned to the Fast Ethernet interface 0/0 address) was sent.

Duplicate address detection processing was performed on the unicast IPv6 address (a neighbor solicitation message was not received in response to a neighbor advertisement message that contained the unicast IPv6 address) and the address is unique.

Indicates time (days, hours) since the last reboot of the event occurring; 3d19h: indicates the time (since the last reboot) of the event occurring was 3 days and 19 hours ago.

Duplicate address detection processing was performed on the link-local IPv6 address (the link-local address FE80::2 is used in the example). A neighbor advertisement message was received in response to a neighbor solicitation message that contained the link-local IPv6 address. The address is not unique, and the processing of IPv6 packets is disabled on the interface.

System error message indicating the duplicate address.

Duplicate address detection processing was performed on the global IPv6 address (the global address 3000::4 is used in the example). A neighbor advertisement message was received in response to a neighbor solicitation message that contained the global IPv6 address. The address is not unique and is not used.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipv6 icmp</td>
<td>Displays debug messages for IPv6 ICMP transactions.</td>
</tr>
<tr>
<td>show ipv6 neighbors</td>
<td>Displays IPv6 neighbor discovery cache information.</td>
</tr>
</tbody>
</table>
debug ipv6 ospf

To display debugging information for Open Shortest Path First (OSPF) for IPv6, use the `debug ipv6 ospf` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

`debug ipv6 ospf [adj | ipsec | database-timer | flood | hello | lsa-generation | retransmission]`

`no debug ipv6 ospf [adj | ipsec | database-timer | flood | hello | lsa-generation | retransmission]`

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adj</td>
<td>(Optional) Displays adjacency information.</td>
</tr>
<tr>
<td>ipsec</td>
<td>(Optional) Displays the interaction between OSPF and IPSec in IPv6 networks, including creation and removal of policy definitions.</td>
</tr>
<tr>
<td>database-timer</td>
<td>(Optional) Displays database-timer information.</td>
</tr>
<tr>
<td>flood</td>
<td>(Optional) Displays flooding information.</td>
</tr>
<tr>
<td>hello</td>
<td>(Optional) Displays hello packet information.</td>
</tr>
<tr>
<td>l2api</td>
<td>(Optional) Enables layer 2 and layer 3 application program interface (API) debugging.</td>
</tr>
<tr>
<td>lsa-generation</td>
<td>(Optional) Displays link-state advertisement (LSA) generation information for all LSA types.</td>
</tr>
<tr>
<td>retransmission</td>
<td>(Optional) Displays retransmission information.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging of OSPF for IPv6 is not enabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(24)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated in Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated in Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>The <code>ipsec</code> keyword was added to support OSPF for IPv6 authentication for IPSec.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.4(25)T</td>
<td>The <code>l2api</code> keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Consult Cisco technical support before using this command.
Examples

The following example displays adjacency information for OSPF for IPv6:

Router# debug ipv6 ospf adj
debug ipv6 ospf database-timer rate-limit

To display debugging information about the current wait-time used for SPF scheduling, use the `debug ipv6 ospf database-timer rate-limit` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```bash
debug ipv6 ospf database-timer rate-limit [acl-number]
no debug ipv6 ospf database-timer rate-limit
```

**Syntax Description**
- `acl-number` (Optional) Access list number.

**Command Modes**
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Consult Cisco technical support before using this command.

**Examples**
The following example shows how to turn on debugging for SPF scheduling:

```bash
Router# debug ipv6 ospf database-timer rate-limit
```
debug ipv6 ospf events

To display information on Open Shortest Path First (OSPF)-related events, such as designated router selection and shortest path first (SPF) calculation, use the `debug ipv6 ospf events` command in privileged EXEC command. To disable debugging output, use the `no` form of this command.

```
d debug ipv6 ospf events
no debug ipv6 ospf events
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(24)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)XNE</td>
<td>This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Consult Cisco technical support before using this command.

**Examples**

The following example displays information on OSPF-related events:

```
Router#
d debug ipv6 ospf events
```
debug ipv6 ospf graceful-restart

To enable debugging for IPv6 graceful-restart-related events, use the `debug ipv6 ospf graceful-restart` command in privileged EXEC mode.

**debug ipv6 ospf graceful-restart**

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging is not enabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ipv6 ospf graceful-restart` command helps troubleshoot graceful-restart-related events on both graceful-restart-capable and graceful-restart-aware routers.

**Examples**

The following example enables debugging for graceful-restart-related events:

```
Router# debug ipv6 ospf graceful-restart
00:03:41: OSPFv3: GR timer started for ospf process 1 for 120 secs,
00:03:43: OSPFv3: GR Build Grace LSA for interface Ethernet0/0
00:03:43: OSPFv3: GR Flood grace lsa on Ethernet0/0
00:03:43: OSPFv3: GR complete check for area 0 process 1
00:03:43: OSPFv3: GR wait, Ethernet0/0 in area 0 not yet complete
00:03:45: OSPFv3: GR Re-flood Grace LSA on Ethernet0/0
00:04:01: OSPFv3: GR initial wait expired
00:04:01: OSPFv3: GR complete check for area 0 process 1
00:04:01: OSPFv3: GR wait, Ethernet0/0 in area 0 not yet complete
00:04:07: OSPFv3: GR complete check for area 0 process 1
00:04:07: OSPFv3: GR re-sync completed in area 0, process 1
00:04:07: OSPFv3: GR complete check for process 1
00:04:07: OSPFv3: process 1: GR re-sync completed for all neighbors
00:04:07: OSPFv3: scheduling rtr lsa for area 0 process 1
00:04:07: OSPFv3: Post GR, flood maxaged grace-LSA on Ethernet0/0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graceful-restart</td>
<td>Enables the OSPFv3 graceful restart feature on a graceful-restart-capable router.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>graceful-restart helper</td>
<td>Enables the OSPFv3 graceful restart feature on a graceful-restart-aware router.</td>
</tr>
<tr>
<td>show ipv6 ospf graceful-restart</td>
<td>Displays OSPFv3 graceful restart information.</td>
</tr>
</tbody>
</table>
debug ipv6 ospf lsdb

To display database modifications for Open Shortest Path First (OSPF) for IPv6, use the `debug ipv6 ospf lsdb` command in privileged EXEC mode. To disable debugging output, use the `no debug ipv6 ospf lsdb` form of this command.

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(24)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Consult Cisco technical support before using this command.

**Examples**

The following example displays database modification information for OSPF for IPv6:

```bash
Router# debug ipv6 ospf lsdb
```
**debug ipv6 ospf monitor**

To display debugging information about the current wait-time used for shortest path first (SPF) scheduling, use the `debug ipv6 ospf monitor` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ipv6 ospf monitor
no debug ipv6 ospf monitor
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Consult Cisco technical support before using this command.

**Examples**

The following example shows debugging information about SPF scheduling:

```
Router# debug ipv6 ospf monitor
Sep 27 08:29:49.319: OSPFv3: Schedule SPF in area 0
  Change in LS ID 0.0.0.0, LSA type P
*Sep 27 08:29:49.327: OSPFv3: reset throttling to 5000ms next wait-interval 10000ms
*Sep 27 08:29:49.327: OSPFv3: schedule SPF: spf_time 00:09:36.032 wait_interval 5000ms
IOU_Topvar#  
*Sep 27 08:29:54.331: OSPFv3: Begin SPF at 581.036ms, process time 40ms
*Sep 27 08:29:54.331:   spf_time 00:09:36.032, wait_interval 5000ms
*Sep 27 08:29:54.331: OSPFv3: Setting next wait-interval to 10000ms
*Sep 27 08:29:54.331: OSPFv3: End SPF at 581.036ms, Total elapsed time 0ms
*Sep 27 08:29:54.331:   Schedule time 00:09:41.036, Next wait_interval 10000ms
*Sep 27 08:29:54.331:   Intra: 0ms, Inter: 0ms, External: 0ms
*Sep 27 08:29:54.331:   R: 0, N: 0
*Sep 27 08:29:54.331:   SN: 0, SA: 0, X5: 0, X7: 0
*Sep 27 08:29:54.331:   SPF suspends: 0 intra, 0 total
```
debug ipv6 ospf packet

To display information about each Open Shortest Path First (OSPF) for IPv6 packet received, use the debug ipv6 ospf packet command in privileged EXEC mode. To disable debugging output, use the no form of this command.

```
debug ipv6 ospf packet
no debug ipv6 ospf packet
```

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(24)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays information about each OSPF for IPv6 packet received:

```
Router# debug ipv6 ospf packet
```
**debug ipv6 ospf spf statistic**

To display statistical information while running the shortest path first (SPF) algorithm, use the `debug ipv6 ospf spf statistic` command in privileged EXEC mode. To disable the debugging output, use the `no` form of this command.

```
deploy ipv6 ospf spf statistic
no debug ipv6 ospf spf statistic
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(24)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ipv6 ospf spf statistic` command displays the SPF calculation times in milliseconds, the node count, and a time stamp. Consult Cisco technical support before using this command.

**Examples**

The following example displays statistical information while running the SPF algorithm:

```
Router# debug ipv6 ospf spf statistics
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ipv6 ospf</code></td>
<td>Displays debugging information for the OSPFv3 for IPv6 feature.</td>
</tr>
<tr>
<td><code>debug ipv6 ospf events</code></td>
<td>Displays information on OSPFv3-related events.</td>
</tr>
<tr>
<td><code>debug ipv6 ospf packet</code></td>
<td>Displays information about each OSPFv3 packet received.</td>
</tr>
</tbody>
</table>
# debug ipv6 packet

To display debug messages for IPv6 packets, use the `debug ipv6 packet` command in privileged EXEC mode. To disable debug messages for IPv6 packets, use the `no` form of this command.

```plaintext
d debug ipv6 packet [access-list access-list-name] [detail]
no debug ipv6 packet [access-list access-list-name] [detail]
```

## Syntax Description

<table>
<thead>
<tr>
<th>Access-List Access-List-Name</th>
<th>(Optional) Specifies an IPv6 access list. The access list name cannot contain a space or quotation mark, or begin with a numeric digit.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detail</td>
<td>(Optional) May display additional detailed information about the IPv6 packet.</td>
</tr>
</tbody>
</table>

## Command Default

Debugging for IPv6 packets is not enabled.

## Command Modes

Privileged EXEC

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(21)ST</td>
<td>This command was integrated into Cisco IOS Release 12.0(21)ST.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(22)S.</td>
</tr>
<tr>
<td>12.0(23)S</td>
<td>The <code>access-list</code> and <code>detail</code> keywords, and the <code>access-list-name</code> argument, were added.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>The <code>access-list</code> and <code>detail</code> keywords, and the <code>access-list-name</code> argument, were added.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

The `debug ipv6 packet` command is similar to the `debug ip packet` command, except that it is IPv6-specific.

## Note

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the Cisco IOS Debug Command Reference.
IPv6 debugging information includes packets received, generated, and forwarded. Fast-switched packets do not generate messages. When an IPv6 access list is specified by using the `access-list` keyword and `access-list-name` argument, only packets matching the access list permit entries are displayed.

Caution

Because the `debug ipv6 packet` command generates a substantial amount of output, use it only when traffic on the IPv6 network is low, so other activity on the system is not adversely affected.

Examples

The following example shows output for the `debug ipv6 packet` command:

```
Router# debug ipv6 packet
13:25:40:IPV6:source 2000:0:0:3::1 (local)
13:25:40: dest 2000:0:0:3::2 (FastEthernet0/0)
13:25:40: traffic class 96, flow 0x0, len 143+195, prot 6, hops 64, originating
13:25:40:IPV6:Sending on FastEthernet0/0
13:25:40:IPV6:source 2000:0:0:3::2 (FastEthernet0/0)
13:25:40: dest 2000:0:0:3::1
13:25:40: traffic class 96, flow 0x0, len 60+14, prot 6, hops 64, forward to ulp
13:25:45: dest FF02::9 (Ethernet1/1)
13:25:45: traffic class 112, flow 0x0, len 72+1428, prot 17, hops 255, originating
13:25:45:IPV6:Sending on Ethernet1/1
13:25:45: dest 2000:0:0:3::2 (FastEthernet0/0)
13:25:45: traffic class 112, flow 0x0, len 72+8, prot 58, hops 255, originating
13:25:45:IPV6:Sending on FastEthernet0/0
13:25:45:IPV6:source 2000:0:0:3::2 (FastEthernet0/0)
13:25:45: dest FE80::203:E4FF:FE12:CC00
13:25:45: traffic class 112, flow 0x0, len 64+14, prot 58, hops 255, forward to ulp
13:25:45:IPV6:source FE80::203:A0FF:FED6:1400 (FastEthernet0/0)
13:25:45: dest FE80::203:E4FF:FE12:CC00
13:25:45: traffic class 112, flow 0x0, len 72+14, prot 58, hops 255, forward to ulp
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6:</td>
<td>Indicates that this is an IPv6 packet.</td>
</tr>
<tr>
<td>source 2000:0:3::1 (local)</td>
<td>The source address in the IPv6 header of the packet.</td>
</tr>
<tr>
<td>dest 2000:0:3::2 (FastEthernet0/0)</td>
<td>The destination address in the IPv6 header of the packet.</td>
</tr>
<tr>
<td>traffic class 96</td>
<td>The contents of the traffic class field in the IPv6 header.</td>
</tr>
<tr>
<td>flow 0x0</td>
<td>The contents of the flow field of the IPv6 header. The flow field is used to label sequences of packets for which special handling is necessary by IPv6 routers.</td>
</tr>
<tr>
<td>len 64+14</td>
<td>The length of the IPv6 packet. The length is expressed as two numbers with a plus (+) character between the numbers. The first number is the length of the IPv6 portion (IPv6 header length plus payload length). The second number is the entire datagram size minus the first number.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>prot 6</td>
<td>The protocol field in the IPv6 header. Describes the next layer protocol that is carried by the IPv6 packet. In the example, the protocol 58 signifies that the next layer protocol is ICMPv6.</td>
</tr>
<tr>
<td>hops 64</td>
<td>The hops field in the IPv6 packet. This field is similar in function to the IPv4 time-to-live field.</td>
</tr>
<tr>
<td>originating</td>
<td>The presence of this field indicates that the packet shown was originated by the router.</td>
</tr>
<tr>
<td>Sending on FastEthernet0/0</td>
<td>Specifies the interface on which the packet was sent.</td>
</tr>
<tr>
<td>forward to ulp</td>
<td>Indicates that the packet was received by the router at the destination address and was forwarded to an upper-layer protocol (ulp) for processing.</td>
</tr>
</tbody>
</table>
**debug ipv6 pim**

To enable debugging on Protocol Independent Multicast (PIM) protocol activity, use the **debug ipv6 pim** command in privileged EXEC mode. To restore the default value, use the **no** form of this command.

```
depbug ipv6 pim [{vrf vrf-name|group-name|group-address | interface interface-type | bsr | group | neighbor}]  
```  
```
no debug ipv6 pim [{vrf vrf-name|group-name|group-address | interface interface-type | bsr | group | neighbor}]  
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>(Optional) Displays information based on the specified virtual routing and forwarding (VRF) name.</td>
</tr>
<tr>
<td>group-name</td>
<td>(Optional) IPv6 address or name of the multicast group.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Displays debugging statistics about a specific interface type.</td>
</tr>
<tr>
<td>bsr</td>
<td>(Optional) Displays debugging statistics specific to bootstrap router (BSR) protocol operation.</td>
</tr>
<tr>
<td>group</td>
<td>(Optional) Displays debugging information about group-related activity.</td>
</tr>
<tr>
<td>neighbor</td>
<td>(Optional) Displays debugging statistics related to hello message processing and neighbor cache management.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(26)S.</td>
</tr>
<tr>
<td>12.0(28)S</td>
<td>The bsr keyword was added.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>The bsr keyword was added.</td>
</tr>
<tr>
<td>12.3(11)T</td>
<td>The bsr keyword was added.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on Cisco ASR 1000 Series Routers.</td>
</tr>
</tbody>
</table>
**Modification Release**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar Release 16.10.1</td>
<td>This command was modified. The vrf keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command helps discover whether the PIM protocol activities are working correctly.

The messages displayed by the `debug ipv6 pim` command show all PIM protocol messages, such as joins and prunes, received from or sent to other routers. Use this command in conjunction with `debug ipv6 mld` to display additional multicast activity, to learn more information about the multicast routing process, or to learn why packets are forwarded out of particular interfaces.

**Examples**

The following example enables debugging on PIM activity:

```
Router# debug ipv6 pim
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipv6 mld</td>
<td>Enables debugging on MLD protocol activity.</td>
</tr>
</tbody>
</table>
### debug ipv6 pim df-election

To display debug messages for Protocol Independent Multicast (PIM) bidirectional designated forwarder (DF) election message processing, use the `debug ipv6 pim df-election` command in privileged EXEC mode. To disable debug messages for PIM bidirectional DF election message processing, use the `no` form of this command.

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>(Optional) Specifies that debug messages on a specified interface will be displayed.</td>
</tr>
<tr>
<td><code>type number</code></td>
<td>(Optional) Interface type and number. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>rp</code></td>
<td>(Optional) Specifies that debug messages on a specified Route Processor (RP) will be displayed.</td>
</tr>
<tr>
<td><code>rp-name</code></td>
<td>(Optional) The name of the specified RP.</td>
</tr>
<tr>
<td><code>rp-address</code></td>
<td>(Optional) The IPv6 address of the specified RP.</td>
</tr>
</tbody>
</table>

#### Command Default

Debugging for PIM bidirectional DF election message processing is not enabled.

#### Command Modes

Privileged EXEC (#)

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

Use the `debug ipv6 pim df-election` command if traffic is not flowing properly when operating in PIM bidirectional mode or if the `show ipv6 pim df` and `show ipv6 pim df winner` commands do not display the expected information.

#### Examples

The following example shows how to enable debugging for PIM bidirectional DF election message processing on Ethernet interface 1/0 and at 200::1:

```
Route# debug ipv6 pim df-election interface ethernet 1/0 rp 200::1
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 pim rp-address</code></td>
<td>Configures the address of a PIM RP for a particular group range.</td>
</tr>
<tr>
<td><code>show ipv6 pim df</code></td>
<td>Displays the DF-election state of each interface for each RP.</td>
</tr>
<tr>
<td><code>show ipv6 pim df winner</code></td>
<td>Displays the DF-election winner on each interface for each RP.</td>
</tr>
</tbody>
</table>
### debug ipv6 pim limit

To enable debugging for Protocol Independent Multicast (PIM) interface limits, use the `debug ipv6 pim limit` command in privileged EXEC mode. To restore the default value, use the `no` form of this command.

```
debug ipv6 pim limit [group]
no debug ipv6 pim limit
```

**Syntax Description**

- `group` (Optional) Specific group to be debugged.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ipv6 pim limit` command to display debugging information for interface limits and costs. Use the optional `group` argument to specify a particular group to debug.

**Examples**

The following example enables PIM interface limit debugging:

```
Router# debug ipv6 pim limit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 multicast limit</code></td>
<td>Configures per-interface mroute state limiters in IPv6.</td>
</tr>
<tr>
<td><code>ipv6 multicast limit cost</code></td>
<td>Applies a cost to mroutes that match per interface mroute state limiters in IPv6.</td>
</tr>
</tbody>
</table>
**debug ipv6 policy**

To enable debugging of IPv6 policy routing packet activity, use the `debug ipv6 policy` command in user EXEC or privileged EXEC mode. To disable debugging, use the `no` form of this command.

```
deploy ipv6 policy [access-list-name]
no debug ipv6 policy [access-list-name]
```

**Syntax Description**

`access-list-name` (Optional) Name of the IPv6 access list. Names cannot contain a space or quotation mark or begin with a numeric.

**Command Default**

If no access list is specified using the optional `access-list-name` argument, information about all policy-matched and policy-routed packets is displayed.

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(30)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(30)S.</td>
</tr>
<tr>
<td>12.2(33)SXI4</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI4.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2S</td>
<td>This command was integrated into Cisco IOS XE Release 3.2S.</td>
</tr>
<tr>
<td>15.1(1)SY</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)SY.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

After you configure IPv6 policy routing, use the `debug ipv6 policy` command to verify that IPv6 policy-based routing (PBR) is policy-routing packets normally. Policy routing analyzes various parts of the packet and then routes the packet based on certain user-defined attributes in the packet. The `debug ipv6 policy` command helps you determine what policy is followed during routing. It displays information about whether a packet matches the given criteria, and if yes, the resulting routing information for the packet.

Do not use the `debug ipv6 policy` command unless you suspect a problem with IPv6 PBR policy routing.

**Examples**

The following example shows how to enable debugging of IPv6 policy routing packet activity. The output of this command is self-explanatory:

```
Device# debug ipv6 policy
00:02:38:IPv6 PBR:Ethernet0/0, matched src 2003::90 dst 2001:DB8::1 protocol 58
00:02:38:IPv6 PBR:next hop 2001:DB8::F, interface Ethernet1/0
00:02:38:IPv6 PBR:policy route via Ethernet1/0/2001:DB8::F
```
debug ipv6 pool

To enable debugging on IPv6 prefix pools, use the debug ipv6 pool command in privileged EXEC mode. To disable debugging, use the no form of this command.

```
debug ipv6 pool
no debug ipv6 pool
```

**Syntax Description**
- This command has no keywords or arguments.

**Command Default**
- No debugging is active.

**Command Modes**
- Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**
The following example enables debugging for IPv6 prefix pools:

```
Router# debug ipv6 pool
2w4d: IPv6 Pool: Deleting route/prefix 2001:0DB8::/29 to Virtual-Access1 for cisco
2w4d: IPv6 Pool: Returning cached entry 2001:0DB8::/29 for cisco on Virtual-Access1 to pool1
2w4d: IPv6 Pool: Installed route/prefix 2001:0DB8::/29 to Virtual-Access1 for cisco
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 local pool</td>
<td>Configures a local IPv6 prefix pool.</td>
</tr>
<tr>
<td>show ipv6 interface</td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
<tr>
<td>show ipv6 local pool</td>
<td>Displays information about defined IPv6 prefix pools.</td>
</tr>
</tbody>
</table>
debug ipv6 rip

To display debug messages for IPv6 Routing Information Protocol (RIP) transactions, use the `debug ipv6 rip` command in privileged EXEC mode. To disable debug messages for IPv6 RIP routing transactions, use the `no` form of this command.

**Cisco IOS XE Release 3.9S, Cisco IOS Release 15.3(2)S, and Later Releases**

```
depbug ipv6 rip [interface-type interface-number] [vrf vrf-name]
no debug ipv6 rip [interface-type interface-number] [vrf vrf-name]
```

**Releases Prior to Cisco IOS XE Release 3.9S and Cisco IOS Release 15.3(2)S**

```
depbug ipv6 rip [interface-type interface-number]
no debug ipv6 rip [interface-type interface-number]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-type</td>
<td>(Optional) Interface type for which to display the debug messages.</td>
</tr>
<tr>
<td>interface-number</td>
<td>(Optional) Interface number for which to display the debug messages.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Displays information about the specified virtual routing and forwarding (VRF) instance.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(21)ST</td>
<td>This command was integrated into Cisco IOS Release 12.0(21)ST.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was implemented on Cisco 1000 Series Aggregation Services Routers.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was modified. The <code>vrf vrf-name</code> keyword-argument pair was added.</td>
</tr>
<tr>
<td>15.3(2)S</td>
<td>This command was integrated into Cisco IOS Release 15.3(2)S.</td>
</tr>
<tr>
<td>15.3(3)M</td>
<td>This command was integrated into Cisco IOS Release 15.3(3)M.</td>
</tr>
</tbody>
</table>
The `debug ipv6 rip` command is similar to the `debug ip rip` command, except that it is IPv6-specific.

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the `logging` command in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the Cisco IOS Debug Command Reference.

Use the `debug ipv6 rip` command to enable IPv6 RIP debugging for RIP packets that are sent and received on all device interfaces. Use the `debug ipv6 rip interface-type interface-number` command to enable IPv6 RIP debugging for RIP packets that are sent and received only on the specified interface.

Use the `debug ipv6 rip vrf vrf-name` command to troubleshoot issues in the IPv6 RIP functionality when the VRF has already been enabled using a `vrf definition vrf-name` command. Ensure that the specified VRF name has already been defined. If a VRF name has not been defined, the following message is displayed:

```
% VRF <undefined VRF name> does not exist or does not have a RD.
```

The following is sample output from the `debug ipv6 rip` command:

```
Device# debug ipv6 rip
13:09:10:RIPng:Sending multicast update on Ethernet1/1 for as1_rip
13:09:10: src=2001:DB8::1
dst=2001:DB8:0:ABCD::1 (Ethernet1/1)
sport=521, dport=521, length=32
command=2, version=1, mbz=0, #rte=1
tag=0, metric=1, prefix=::/0
13:09:28:RIPng:response received from 2001:DB8:0:0:E000::F on Ethernet1/1 for as1_rip
13:09:28: src=FE80::202:FDFF:FE77:1E42 (Ethernet1/1)
dst=FF02::9
sport=521, dport=521, length=32
command=2, version=1, mbz=0, #rte=1
tag=0, metric=1, prefix=2000:0:0:1::/80
```

The above example shows two RIP packets; both are known as “responses” in RIP terminology and indicated by a “command” value of 2. The first is an update sent by the device, and the second is an update received by the device. Multicast update packets are sent to all neighboring IPv6 RIP devices (all devices that are on the same links as the device sending the update and have IPv6 RIP enabled). An IPv6 RIP device advertises the contents of its routing table to its neighbors by periodically sending update packets over those interfaces on which IPv6 RIP is configured. An IPv6 device may also send “triggered” updates immediately following a routing table change. In this case, the updates include only the changes to the routing table. An IPv6 RIP device may solicit the contents of the routing table of a neighboring device by sending a Request (command =1) message to the device. The device responds by sending an update (Response, command=2) containing its routing table. In the example, the received response packet could be a periodic update from the address 2001:DB8:0:0:E000::F or a response to a RIP request message that was previously sent by the local device.

The following is sample output from the `debug ipv6 rip vrf` command:

```
Device# debug ipv6 rip vrf blue
RIP Routing Protocol debugging is on for vrf blue
```
Sending:
*Mar 15 11:23:08.508: RIPng: Sending multicast update on Ethernet0/0 for vrf for vrf blue
*Mar 15 11:23:08.508: dst=2001:DB8:0:1::1 (Ethernet0/0)
*Mar 15 11:23:08.508: sport=521, dport=521, length=52
*Mar 15 11:23:08.508: command=2, version=1, mbz=0, #rte=2
*Mar 15 11:23:08.508: tag=0, metric=1, prefix=6000::/64
*Mar 15 11:23:08.508: tag=0, metric=1, prefix=2000::/64
*Mar 15 11:23:08.508: RIPng: Process vrf received own response on Loopback1

Receiving
*Mar 15 11:23:20.316: RIPng: response received from FE80::A8BB:CCFF:FE00:7C00 on Ethernet0/0 for vrf
*Mar 15 11:23:20.316: command=2, version=1, mbz=0, #rte=1
*Mar 15 11:23:20.316: tag=0, metric=1, prefix=AAAA::/64

The table below describes the significant fields shown in the display.

**Table 81: debug ipv6 rip vrf Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>src</td>
<td>The address from which the update was originated.</td>
</tr>
<tr>
<td>dst</td>
<td>The destination address for the update.</td>
</tr>
<tr>
<td>sport, dport, length</td>
<td>The source, destination ports and the length for the update. (IPv6 RIP uses port 521, as shown in the display.)</td>
</tr>
<tr>
<td>command</td>
<td>The command field within the RIP packet. A value of 2 indicates that the RIP packet is a response (update); a value of 1 indicates that the RIP packet is a request.</td>
</tr>
<tr>
<td>version</td>
<td>The version of IPv6 RIP being used. The current version is 1.</td>
</tr>
<tr>
<td>mbz</td>
<td>There must be a 0 (mbz) field within the RIP packet.</td>
</tr>
<tr>
<td>#rte</td>
<td>Indicates the number of routing table entries (RTEs) that the RIP packet contains.</td>
</tr>
<tr>
<td>tag</td>
<td>The tag, metric, and prefix fields are specific to each RTE contained in the update.</td>
</tr>
<tr>
<td>metric</td>
<td>The tag field is intended to allow for the flagging of IPv6 RIP “internal” and “external” routes.</td>
</tr>
<tr>
<td>prefix</td>
<td>The metric field is the distance metric from the device (sending this update) to the prefix.</td>
</tr>
<tr>
<td></td>
<td>The prefix field is the IPv6 prefix of the destination being advertised.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>clear ipv6 rip</td>
<td>Deletes routes from the IPv6 RIP routing table.</td>
</tr>
<tr>
<td>ipv6 rip vrf-mode enable</td>
<td>Enables VRF support for IPv6 RIP.</td>
</tr>
<tr>
<td>show ipv6 rip</td>
<td>Displays information about current IPv6 RIP processes.</td>
</tr>
<tr>
<td>vrf definition</td>
<td>Configures a VRF routing table instance.</td>
</tr>
</tbody>
</table>
debug ipv6 routing

To display debug messages for IPv6 routing table updates and route cache updates, use the `debug ipv6 routing` command in privileged EXEC mode. To disable debug messages for IPv6 routing table updates and route cache updates, use the `no` form of this command.

```
dependent ipv6 routing
no debug ipv6 routing
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging for IPv6 routing table updates and route cache updates is not enabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(21)ST</td>
<td>This command was integrated into Cisco IOS Release 12.0(21)ST.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(22)S.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ipv6 routing` command is similar to the `debug ip routing` command, except that it is IPv6-specific.

**Note**

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server.

For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

**Examples**

The following example shows output for the `debug ipv6 routing` command:

```
Router# debug ipv6 routing
13:18:43:IPv6RT0:Add 2000:0:0:1:1::/80 to table
13:18:43:IPv6RT0:Better next-hop for 2000:0:0:1:1::/80, [120/2]
13:19:09:IPv6RT0:Add 2000:0:0:2::/64 to table
```
The `debug ipv6 routing` command displays messages whenever the routing table changes. For example, the following message indicates that a route to the prefix 2000:0:0:1::/80 was added to the routing table at the time specified in the message.

13:18:43:IPv6RT0:Add 2000:0:0:1::1::/80 to table

The following message indicates that the prefix 2000:0:0:2::/64 was already in the routing table; however, a received advertisement provided a lower cost path to the prefix. Therefore, the routing table was updated with the lower cost path. (The [20/1] in the example is the administrative distance [20] and metric [1] of the better path.)

13:19:09:IPv6RT0:Better next-hop for 2000:0:0:2::/64, [20/1]

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ipv6 rip</code></td>
<td>Displays debug messages for IPv6 RIP routing transactions.</td>
</tr>
</tbody>
</table>
debug ipv6 snooping

To enable debugging for security snooping information in IPv6, use the `debug ipv6 snooping` command in privileged EXEC mode.

```
default ipv6 snooping [ { binding-table | classifier | errors | feature-manager | filter acl | ha | hw-api | interface interface | memory | ndp-inspection | policy | vlan vlanid | switcher | filter acl | interface interfacevlan-id } ]
```

```
no debug ipv6 snooping
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>binding-table</td>
<td>(Optional) Displays information about the neighbor binding table.</td>
</tr>
<tr>
<td>classifier</td>
<td>(Optional) Displays information about the classifier.</td>
</tr>
<tr>
<td>errors</td>
<td>(Optional) Displays information about snooping security errors.</td>
</tr>
<tr>
<td>feature-manager</td>
<td>(Optional) Displays feature manager information.</td>
</tr>
<tr>
<td>filter acl</td>
<td>(Optional) Allows users to configure an access list to filter debugged traffic.</td>
</tr>
<tr>
<td>ha</td>
<td>(Optional) Displays information about high availability (HA) and stateful switchover (SSO).</td>
</tr>
<tr>
<td>hw-api</td>
<td>(Optional) Displays information about the hardware API.</td>
</tr>
<tr>
<td>interface interface</td>
<td>(Optional) Provides debugging information on a specified interface.</td>
</tr>
<tr>
<td>memory</td>
<td>(Optional) Displays information about security snooping memory.</td>
</tr>
<tr>
<td>ndp-inspection</td>
<td>(Optional) Displays information about Neighbor Discovery inspection.</td>
</tr>
<tr>
<td>policy</td>
<td>(Optional)</td>
</tr>
<tr>
<td>switcher</td>
<td>(Optional) Displays packets handled by the switcher.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>(Optional) Provides debugging information about a specified VLAN ID.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `debug ipv6 snooping` command provides debugging output for IPv6 snooping information.

Because debugging output is assigned high priority in the CPU process, you should use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff.

### Examples

The following example enables debugging for all IPv6 snooping information:
Router# debug ipv6 snooping
debug ipv6 snooping raguard

To enable debugging for security snooping information in the IPv6 router advertisement (RA) guard feature, use the debug ipv6 snooping raguard command in privileged EXEC mode.

**debug ipv6 snooping raguard** [{filterinterfacevlanid}]

**no debug ipv6 snooping raguard**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>filter</code></td>
<td>(Optional) Allows users to configure an access list to filter debugged traffic.</td>
</tr>
<tr>
<td><code>interface</code></td>
<td>(Optional) Provides debugging information about a specified interface configured with the IPv6 RA guard feature.</td>
</tr>
<tr>
<td><code>vlanid</code></td>
<td>(Optional) Provides debugging information about a specified VLAN ID configured with the IPv6 RA guard feature.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(54)SG</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(50)SY</td>
<td>This command was integrated into Cisco IOS Release 12.2(50)SY.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The debug ipv6 snooping raguard command provides debugging output for IPv6 RA guard events and errors that may occur.

Because debugging output is assigned high priority in the CPU process, you should use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, you should use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

**Examples**

The following example shows the command enabling debugging for the IPv6 RA guard feature:

```
Router# debug ipv6 snooping raguard
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd raguard</td>
<td>Applies the IPv6 RA guard feature.</td>
</tr>
</tbody>
</table>
**debug ipv6 spd**

To enable debugging output for the most recent Selective Packet Discard (SPD) state transition, use the `debug ipv6 spd` command in privileged EXEC mode.

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(3)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug ipv6 spd` command enables debugging information to be reviewed for the most recent SPD state transition and any trend historical data.

**Examples**

The following example shows how to enable debugging for the most recent SPD state transition:

```
Router# debug ipv6 spd
```
debug ipv6 static

To enable Bidirectional Forwarding Detection for IPv6 (BFDv6) debugging, use the `debug ipv6 static` command in privileged EXEC mode.

**debug ipv6 static**

**Command Default**

Debugging is not enabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(2)T</td>
<td>This command was modified. It was integrated into Cisco IOS Release 15.1(2)T.</td>
</tr>
<tr>
<td>15.1(1)SG</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)SG.</td>
</tr>
<tr>
<td>15.1(1)SY</td>
<td>This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(1)SY.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug ipv6 static` command to monitor BFDv6 operation.

**Examples**

The following example enables BFDv6 debugging:

```
Router# debug ipv6 static
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor event ipv6 static</td>
<td>Monitors the operation of the IPv6 static and IPv6 static BFDv6 neighbors using event trace.</td>
</tr>
<tr>
<td>show ipv6 static</td>
<td>Displays the current contents of the IPv6 routing table.</td>
</tr>
</tbody>
</table>
**debug ipv6 wccp**

To display information about IPv6 Web Cache Communication Protocol (WCCP) services, use the `debug ipv6 wccp` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ipv6 wccp {default | vrf vrf-name {events | packets [control]} | events | packets [{bypass | control | redirect}] | platform | subblocks}
no debug ipv6 wccp {default | vrf vrf-name {events | packets [control]} | events | packets [{bypass | control | redirect}] | platform | subblocks}
```

**Syntax Description**

- **default**: Displays information about default WCCP services.
- **vrf vrf-name**: Specifies a virtual routing and forwarding (VRF) instance to associate with a service group.
- **events**: Displays information about significant WCCP events.
- **packets**: Displays information about every WCCP packet received or sent by the router.
- **control**: (Optional) Displays information about WCCP control packets.
- **bypass**: (Optional) Displays information about WCCP bypass packets.
- **redirect**: (Optional) Displays information about WCCP redirect packets.
- **platform**: Displays information about the WCCP platform application programming interface (API).
- **subblocks**: Displays information about WCCP subblocks.

**Command Default**

Debug information is not displayed.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(3)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(1)SY1</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)SY1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the **vrf** keyword is not used, the command displays debug information about all WCCP services on the router. The **default** keyword is used to specify default WCCP services.

**Examples**

The following is sample output from the `debug ipv6 wccp events` command when a Cisco Cache Engine is added to the list of available Web caches:

```
Router# debug ipv6 wccp events
WCCP-EVNT: Built I_See_You msg body w/1 usable web caches, change # 0000000A
WCCP-EVNT: Built I_See_You msg body w/2 usable web caches, change # 0000000B
WCCP-EVNT: Built I_See_You msg body w/2 usable web caches, change # 0000000C
```
The following is sample output from the **debug ipv6 wccp packets** command. The router is sending keepalive packets to the Cisco Cache Engines at 2001:DB8:1::2 and 2001:DB8:1::1. Each keepalive packet has an identification number associated with it. When the Cisco Cache Engine receives a keepalive packet from the router, it sends a reply with the identification number back to the router.

Router# **debug ipv6 wccp packets**
WCCP-PKT: Received valid Here_I_Am packet from 2001:DB8:1::2 w/rcvd_id 00003532
WCCP-PKT: Sending I_See_You packet to 2001:DB8:1::2 w/ rcvd_id 00003534
WCCP-PKT: Received valid Here_I_Am packet from 2001:DB8:1::1 w/rcvd_id 00003533
WCCP-PKT: Sending I_See_You packet to 2001:DB8:1::1 w/ rcvd_id 00003535
WCCP-PKT: Received valid Here_I_Am packet from 2001:DB8:1::2 w/rcvd_id 00003534
WCCP-PKT: Sending I_See_You packet to 2001:DB8:1::2 w/ rcvd_id 00003536
WCCP-PKT: Received valid Here_I_Am packet from 2001:DB8:1::1 w/rcvd_id 00003535
WCCP-PKT: Sending I_See_You packet to 2001:DB8:1::1 w/ rcvd_id 00003537
WCCP-PKT: Received valid Here_I_Am packet from 2001:DB8:1::2 w/rcvd_id 00003536
WCCP-PKT: Sending I_See_You packet to 2001:DB8:1::2 w/ rcvd_id 00003538
WCCP-PKT: Received valid Here_I_Am packet from 2001:DB8:1::1 w/rcvd_id 00003537
WCCP-PKT: Sending I_See_You packet to 2001:DB8:1::1 w/ rcvd_id 00003539

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear ipv6 wccp</code></td>
<td>Clears the counter for packets redirected using WCCP.</td>
</tr>
<tr>
<td><code>ipv6 wccp</code></td>
<td>Enables support of the specified WCCP service for participation in a service group.</td>
</tr>
<tr>
<td><code>ipv6 wccp redirect</code></td>
<td>Enables packet redirection on an outbound or inbound interface using WCCP.</td>
</tr>
<tr>
<td><code>show ipv6 interface</code></td>
<td>Lists a summary of the IP information and status of an interface.</td>
</tr>
</tbody>
</table>
**debug ipx ipxwan**

To display debugging information for interfaces configured to use IPX wide-area network (IPXWAN), use the `debug ipx ipxwan` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```bash
debug ipx ipxwan
no debug ipx ipxwan
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

The `debug ipx ipxwan` command is useful for verifying the startup negotiations between two routers running the IPX protocol through a WAN. This command produces output only during state changes or startup. During normal operations, no output is produced.

**Examples**

The following is sample output from the `debug ipx ipxwan` command during link startup:

```bash
Router# debug ipx ipxwan
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state to up
IPXWAN: state (Disconnect -> Sending Timer Requests) [Serial1/6666:200 (IPX line state brought up)]
IPXWAN: state (Sending Timer Requests --> Disconnect) [Serial1/6666:200 (IPX line state brought down)]
IPXWAN: state (Disconnect --> Sending Timer Requests) [Serial1/6666:200 (IPX line state brought up)]
IPXWAN: Send TIMER_REQ [seq 0] out Serial1/6666:200
IPXWAN: Send TIMER_REQ [seq 1] out Serial1/6666:200
IPXWAN: Send TIMER_REQ [seq 2] out Serial1/6666:200
IPXWAN: Send TIMER_REQ [seq 0] out Serial1/6666:200
IPXWAN: Rcv TIMER_REQ on Serial1/6666:200, NodeID 1234, Seq 1
IPXWAN: Send TIMER_REQ [seq 1] out Serial1/6666:200
IPXWAN: Rcv TIMER_RSP on Serial1/6666:200, NodeID 1234, Seq 1, Del 6
IPXWAN: state (Sending Timer Requests --> Master: Sent RIP/SAP) [Serial1/6666:200 (Received Timer Response as master)]
IPXWAN: Send RIPSAP_INFO_REQ [seq 0] out Serial1/6666:200
IPXWAN: Rcv RIPSAP_INFO_RSP from Serial1/6666:200, NodeID 1234, Seq 0
IPXWAN: state (Master: Sent RIP/SAP --> Master: Connect) [Serial1/6666:200 (Received Router Info Rsp as Master)]

The following line indicates that the interface has initialized:

```bash
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state to up
```

The following lines indicate that the startup process failed to receive a timer response, brought the link down, then brought the link up and tried again with a new timer set:

```bash
IPXWAN: state (Sending Timer Requests --> Disconnect) [Serial1/6666:200 (IPX line state brought down)]
IPXWAN: state (Disconnect --> Sending Timer Requests) [Serial1/6666:200 (IPX line state brought up)]
```
The following lines indicate that the interface is sending timer requests and waiting for a timer response:

IPXWAN: Send TIMER_REQ [seq 0] out Serial1/6666:200
IPXWAN: Send TIMER_REQ [seq 1] out Serial1/6666:200

The following lines indicate that the interface has received a timer request from the other end of the link and has sent a timer response. The fourth line shows that the interface has come up as the master on the link.

IPXWAN: Rcv TIMER_REQ on Serial1/6666:200, NodeID 1234, Seq 1
IPXWAN: Send TIMER_REQ [seq 1] out Serial1/6666:200
IPXWAN: Rcv TIMER_RSP on Serial1/6666:200, NodeID 1234, Seq 1, Del 6
IPXWAN: state (Sending Timer Requests -> Master: Sent RIP/SAP) [Serial1/6666:200 (Received Timer Response as master)]

The following lines indicate that the interface is sending RIP/SAP requests:

IPXWAN: Send RIPSAP_INFO_REQ [seq 0] out Serial1/6666:200
IPXWAN: Rcv RIPSAP_INFO_RSP from Serial1/6666:200, NodeID 1234, Seq 0
IPXWAN: state (Master: Sent RIP/SAP -> Master: Connect) [Serial1/6666:200 (Received Router Info Rsp as Master)]
debug ipx nasi

To display information about NetWare Asynchronous Services Interface (NASI) connections, use the debug ipx nasi command in Privileged EXEC configuration mode. To disable debugging output, use the no form of this command.

dbg ipx nasi {packets | error | activity}
no debug ipx nasi {packets | error | activity}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>packets</td>
<td>Displays normal operating messages relating to incoming and outgoing NASI packets. This is the default.</td>
</tr>
<tr>
<td>error</td>
<td>Displays messages indicating an error or failure in the protocol processing.</td>
</tr>
<tr>
<td>activity</td>
<td>Displays messages relating to internal NASI processing of NASI connections. The activity option includes all NASI activity such as traffic indication, timer events, and state changes.</td>
</tr>
</tbody>
</table>

Command Default

Nasi protocol debugging is disabled.

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the debug ipx nasi command to display handshake or negotiation details between Sequenced Packet Exchange (SPX), NASI protocol, and other protocols or applications. Use the packets option to determine the NASI traffic flow, and use the error option as a quick check to see why NASI connections failed.

Examples

The following is sample output from the debug ipx nasi command with the packet and error options.

```
Router# debug ipx nasi packet
Router# debug ipx nasi error
NASI0: 6E6E Check server info
NASI0: 6E6E sending server-info 4F00 Good response: 43 bytes
NASI0: 7A6E Query Port. Find first
NASI0: FF: First: line 0 DE, port: TTY1-________ASYNC___^, group: ASYNC___^
NASI0: 7A6E sending Qport find-first response: 300 bytes
NASI0: 7B6E port request. setting up port
NASI: Check-login User: c h r i s
NASI: Check-login PW hash: C7 A6 C5 C7 C4 C0 C5 C3 C4 C5 CF C4 C8 C5 CB C4 D4 C5 D7 C4 D0 C5 D3 C4
NASI: Check-login PW: l a b
NASI1: 7B6E sending NCS Good server Data Ack in 0 bytes pkt in 13 size pkt
NASI1: 7B6E sending Freq response: 303 bytes Good
NASI1: 7B6E port request. setting up port
NASI1: 7B6E sending NCS Good server Data Ack in 0 bytes pkt in 13 size pkt
NASI1: 7B6E sending Freq response: 303 bytes Good
NASI1: 7B6E Unknown NASI code 4500 Pkt Size: 13
   45 0 0 FC 0 2 0 20 0 0 FF 1 0
NASI1: 7B6E Flush Rx Buffers
```
In the following line:
  • 0 in NASI0 is the number of the terminal (TTY) to which this NASI connection is attached.
  • 0 in NASI0 is used by all NASI control connections.
  • 6E6E is the associated SPX connection pointer for this NASI connection.
  • Check server info is a type of incoming NASI packet.

The following message indicates that the router is sending back a server-info packet with a positive acknowledgment, and the packet size is 43 bytes:

The following line is a NASI packet type. Find first and Find next are NASI packet types.

The following line indicates that the outgoing find first packet for the NASI connection 7A6E has line 0 DE, port name TTY1, and general name ASYNC:

The following two lines indicate:
  • Received NASI packet for NASI connection in line 1. 7B6E is the NASI connection pointer. The packet code is 4500 and is not recognizable by Cisco.
  • Hexadecimal dump of the packet in line 2.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipx spx</td>
<td>Displays debugging messages related to the SPX protocol.</td>
</tr>
</tbody>
</table>
**debug ipx packet**

To display information about packets received, sent, and forwarded, use the `debug ipx packet` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
depug ipx packet
no debug ipx packet
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

This command is useful for learning whether Internetwork Packet Exchange (IPX) packets are traveling over a router.

**Note**

In order to generate `debug ipx packet` information on all IPX traffic traveling over the router, you must first configure the router so that fast switching is disabled. Use the `no ipx route-cache` command on all interfaces on which you want to observe traffic. If the router is configured for IPX fast switching, only non fast-switched packets will produce output. When the IPX cache is invalidated or cleared, one packet for each destination is displayed as the cache is repopulated.

**Examples**

The following is sample output from the `debug ipx packet` command:

```
Router# debug ipx packet
IPX: src=160.0260.8c4c.4f22, dst=1.0000.0000.0001, packet received
IPX: src=160.0260.8c4c.4f22, dst=1.0000.0000.0001, gw=183.0000.0c01.5d85, sending packet
```

The first line indicates that the router receives a packet from a Novell station (address 160.0260.8c4c.4f22); this trace does not indicate the address of the immediate router sending the packet to this router. In the second line, the router forwards the packet toward the Novell server (address 1.0000.0000.0001) through an immediate router (183.0000.0c01.5d85).

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPX</td>
<td>Indicates that this is an IPX packet.</td>
</tr>
<tr>
<td>src=160.0260.8c4c.4f22</td>
<td>Source address of the IPX packet. The Novell network number is 160. Its MAC address is 0260.8c4c.4f22.</td>
</tr>
<tr>
<td>dst=1.0000.0000.0001</td>
<td>Destination address for the IPX packet. The address 0000.0000.0001 is an internal MAC address, and the network number 1 is the internal network number of a Novell 3.11 server.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>packet received</td>
<td>Router received this packet from a Novell station, possibly through an intermediate router.</td>
</tr>
<tr>
<td>gw=183.0000.0c01.5d85</td>
<td>Router is sending the packet over to the next hop router; its address of 183.0000.0c01.5d85 was learned from the IPX routing table.</td>
</tr>
<tr>
<td>sending packet</td>
<td>Router is attempting to send this packet.</td>
</tr>
</tbody>
</table>
### debug ipx routing

To display information on Internetwork Packet Exchange (IPX) routing packets that the router sends and receives, use the `debug ipx routing` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
depbug ipx routing {activity | events}
no debug ipx routing {activity | events}
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>activity</td>
<td>Displays messages relating to IPX routing activity.</td>
</tr>
<tr>
<td>events</td>
<td>Displays messages relating to IPX routing events.</td>
</tr>
</tbody>
</table>

#### Command Modes

Privileged EXEC

#### Usage Guidelines

Normally, a router or server sends out one routing update per minute. Each routing update packet can include up to 50 entries. If many networks exist on the internetwork, the router sends out multiple packets per update. For example, if a router has 120 entries in the routing table, it would send three routing update packets per update. The first routing update packet would include the first 50 entries, the second packet would include the next 50 entries, and the last routing update packet would include the last 20 entries.

#### Examples

The following is sample output from the `debug ipx routing` command:

```
Router# debug ipx routing
IPXRIP: update from 9999.0260.8c6a.1733
110801 in 1 hops, delay 2
IPXRIP: sending update to 12FF02:ffff.ffff.ffff via Ethernet 1
   network 555, metric 2, delay 3
   network 1234, metric 3, delay 4
```

The table below describes the significant fields shown in the display.

#### Table 83: debug ipx routing Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPXRIP</td>
<td>IPX RIP packet.</td>
</tr>
<tr>
<td>update from 9999.0260.8c6a.1733</td>
<td>Routing update packet from an IPX server at address 9999.0260.8c6a.1733.</td>
</tr>
<tr>
<td>110801 in 1 hops</td>
<td>Network 110801 is one hop away from the router at address 9999.0260.8c6a.1733.</td>
</tr>
<tr>
<td>delay 2</td>
<td>Delay is a time measurement (1/18th second) that the NetWare shell uses to estimate how long to wait for a response from a file server. Also known as ticks.</td>
</tr>
</tbody>
</table>
Router is sending this IPX routing update packet to address 12FF02:ffff.ffff.ffff through Ethernet interface 1.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sending update to 12FF02:ffff.ffff.ffff via Ethernet 1</td>
<td>Router is sending this IPX routing update packet to address 12FF02:ffff.ffff.ffff through Ethernet interface 1.</td>
</tr>
<tr>
<td>network 555</td>
<td>Packet includes routing update information for network 555.</td>
</tr>
<tr>
<td>metric 2</td>
<td>Network 555 is two metrics (or hops) away from the router.</td>
</tr>
<tr>
<td>delay 3</td>
<td>Network 555 is a delay of 3 away from the router. Delay is a measurement that the NetWare shell uses to estimate how long to wait for a response from a file server. Also known as ticks.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipx sap</td>
<td>Displays information about IPX SAP packets.</td>
</tr>
</tbody>
</table>
debug ipx sap

To display information about Internetwork Packet Exchange (IPX) Service Advertisement Protocol (SAP) packets, use the `debug ipx sap` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ipx sap [activity | events]

no debug ipx sap [activity | events]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>activity</th>
<th>(Optional) Provides more detailed output of SAP packets, including displays of services in SAP packets.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>events</td>
<td>(Optional) Limits amount of detailed output for SAP packets to those that contain interesting events.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Usage Guidelines**

Normally, a router or server sends out one SAP update per minute. Each SAP packet can include up to seven entries. If many servers are advertising on the network, the router sends out multiple packets per update. For example, if a router has 20 entries in the SAP table, it would send three SAP packets per update. The first SAP would include the first seven entries, the second SAP would include the next seven entries, and the last update would include the last six entries.

Obtain the most meaningful detail by using the `debug ipx sap activity` and the `debug ipx sap events` commands together.

⚠️ **Caution**

Because the `debug ipx sap` command can generate a substantial amount of output, use it with caution on networks that have many interfaces and large service tables.

**Examples**

The following is sample output from the `debug ipx sap` command:

```
Router# debug ipx sap
IPXSAP: at 0023F778:
  I SAP Response type 0x2 len 160 src:160.0000.0c00.070d dest:160.ffff.ffff.ffff452
  type 0x4, "Hello2", 199.0002.0004.0006 451, 2 hops
  type 0x4, "Hello1", 199.0002.0004.0008 451, 2 hops
IPXSAP: sending update to 160
IPXSAP: at 00169080:
  O SAP Update type 0x2 len 96 ssoc:0x452 dest:160.ffff.ffff.ffff452
  IPX: type 0x4, "Magnolia", 42.0000.0000.0001 451, 2hops
```

The `debug ipx sap` command generates multiple lines of output for each SAP packet—a packet summary message and a service detail message.

The first line displays the internal router memory address of the packet. The technical support staff may use this information in problem debugging.

```
IPXSAP: at 0023F778:
```
The table below describes the significant fields shown in the display.

**Table 84: debug ipx sap Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Indicates whether the router received the SAP packet as input (I) or is sending an update as output (O).</td>
</tr>
<tr>
<td>SAP Response type 0x2</td>
<td>Packet type. Format is 0x(n); possible values for (n) include:</td>
</tr>
<tr>
<td></td>
<td>1--General query</td>
</tr>
<tr>
<td></td>
<td>2--General response</td>
</tr>
<tr>
<td></td>
<td>3--Get Nearest Server request</td>
</tr>
<tr>
<td></td>
<td>4--Get Nearest Server response</td>
</tr>
<tr>
<td>len 160</td>
<td>Length of this packet (in bytes).</td>
</tr>
<tr>
<td>src: 160.000.0c00.070d</td>
<td>Source address of the packet.</td>
</tr>
<tr>
<td>dest: 160.ffff.ffff.ffff</td>
<td>IPX network number and broadcast address of the destination IPX network for which the message is intended.</td>
</tr>
<tr>
<td>(452)</td>
<td>IPX socket number of the process sending the packet at the source address. This number is always 452, which is the socket number for the SAP process.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>type 0x4</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Indicates the type of service the server sending the packet provides. Format is 0x(n). Some of the values for (n) are proprietary to Novell. Those values for (n) that have been published include the following (contact Novell for more information):</td>
</tr>
<tr>
<td>0</td>
<td>Unknown</td>
</tr>
<tr>
<td>1</td>
<td>User</td>
</tr>
<tr>
<td>2</td>
<td>User group</td>
</tr>
<tr>
<td>3</td>
<td>Print queue</td>
</tr>
<tr>
<td>4</td>
<td>File server</td>
</tr>
<tr>
<td>5</td>
<td>Job server</td>
</tr>
<tr>
<td>6</td>
<td>Gateway</td>
</tr>
<tr>
<td>7</td>
<td>Print server</td>
</tr>
<tr>
<td>8</td>
<td>Archive queue</td>
</tr>
<tr>
<td>9</td>
<td>Archive server</td>
</tr>
<tr>
<td>A</td>
<td>Job queue</td>
</tr>
<tr>
<td>B</td>
<td>Administration</td>
</tr>
<tr>
<td>21</td>
<td>NAS SNA gateway</td>
</tr>
<tr>
<td>24</td>
<td>Remote bridge server</td>
</tr>
<tr>
<td>2D</td>
<td>Time Synchronization VAP</td>
</tr>
<tr>
<td>2E</td>
<td>Dynamic SAP</td>
</tr>
<tr>
<td>47</td>
<td>Advertising print server</td>
</tr>
<tr>
<td>4B</td>
<td>Btrieve VAP 5.0</td>
</tr>
<tr>
<td>4C</td>
<td>SQL VAP</td>
</tr>
<tr>
<td>7A</td>
<td>TES--NetWare for VMS</td>
</tr>
<tr>
<td>98</td>
<td>NetWare access server</td>
</tr>
<tr>
<td>9A</td>
<td>Named Pipes server</td>
</tr>
<tr>
<td>9E</td>
<td>Portable NetWare--UNIX</td>
</tr>
<tr>
<td>111</td>
<td>Test server</td>
</tr>
<tr>
<td>166</td>
<td>NetWare management</td>
</tr>
<tr>
<td>233</td>
<td>NetWare management agent</td>
</tr>
<tr>
<td>237</td>
<td>NetExplorer NLM</td>
</tr>
<tr>
<td>239</td>
<td>HMI hub</td>
</tr>
<tr>
<td>23A</td>
<td>NetWare LANalyzer agent</td>
</tr>
<tr>
<td>26A</td>
<td>NMS management</td>
</tr>
<tr>
<td>FFFF</td>
<td>Wildcard (any SAP service)</td>
</tr>
</tbody>
</table>
The fifth line of output indicates that the router sent a SAP update to network 160:

```
IPXSAP: sending update to 160
```

The format for `debug ipx sap` output describing a SAP update the router sends is similar to that describing a SAP update the router receives, except that the ssoc: field replaces the src: field, as the following line of output indicates:

```
O SAP Update type 0x2 len 96 ssoc:0x452 dest:160.ffff.ffff.ffff(452)
```

The ssoc:0x452 field indicates the IPX socket number of the process sending the packet at the source address. Possible values include the following:

- 451--Network Core Protocol
- 452--Service Advertising Protocol
- 453--Routing Information Protocol
- 455--NetBIOS
- 456--Diagnostics
- 4000 to 6000--Ephemeral sockets used for interaction with file servers and other network communications

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ipx routing</code></td>
<td>Displays information on IPX routing packets that the router sends and receives.</td>
</tr>
</tbody>
</table>
**debug ipx spoof**

To display information about Sequenced Packet Exchange (SPX) keepalive and Internetwork Packet Exchange (IPX) watchdog packets when `ipx watchdog` and `ipx spx-spoof` are configured on the router, use the `debug ipx spoof` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ipx spoof
no debug ipx spoof
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

Use this command to troubleshoot connections that use SPX spoofing when SPX keepalive spoofing is enabled.

**Examples**

The following is sample output from the `debug ipx spoof` command:

```
Router# debug ipx spoof

IPX: Tu1:200.0260.8c8d.da75->CC0001.0000.0000.0001 ln= 42 tc=02, SPX: 80 0 7004 4B8 8 1D 23 (new) (changed=yes) Last Changed 0
IPX: Tu1:200.0260.8c8d.c558->CC0001.0000.0000.0001 ln= 42 tc=02, SPX: 80 0 7104 2B8 7 29 2E (new) (changed=yes) Last Changed 0
IPX: Et1:CC0001.0000.0000.0001->200.0260.8c8d.c558 ln= 42 tc=02, SPX: 80 0 2B8 7104 29 7 7 (early)
IPX: Et1:CC0001.0000.0000.0001->200.0260.8c8d.da75 ln= 42 tc=02, SPX: 80 0 4B8 7004 1D 8 8 (early)
IPX: Et1:CC0001.0000.0000.0001->200.0260.8c8d.da75 ln= 32 tc=02, watchdog
IPX: local:200.0260.8c8d.da75->CC0001.0000.0000.0001 ln= 32 tc=00, watchdog snet
IPX: Tu1:200.0260.8c8d.da75->CC0001.0000.0000.0001 ln= 42 tc=02, SPX: 80 0 7004 4B8 8 1D 23 (changed:clear) Last Changed 0
IPX: Et1:CC0001.0000.0000.0001->200.0260.8c8d.c558 ln= 42 tc=02, SPX: C0 0 2B8 7104 29 7 7 (early)
IPX: Tu1:200.0260.8c8d.c558->CC0001.0000.0000.0001 ln= 42 tc=02, SPX: 80 0 7104 2B8 7 29 2E (changed:clear) Last Changed 0
IPX: Et1:CC0001.0000.0000.0001->200.0260.8c8d.c558 ln= 42 tc=02, SPX: C0 0 2B8 7104 29 7 7 (Last Changed 272 sec)
IPX: local:200.0260.8c8d.c558->CC0001.0000.0000.0001 ln= 42 tc=02, spx keepalive sent 80 0 7104 2B8 7 29 2E

The following lines show that SPX packets were seen, but they are not seen for a connection that exists in the SPX table:

```
IPX: Tu1:200.0260.8c8d.da75->CC0001.0000.0000.0001 ln= 42 tc=02, SPX: 80 0 7004 4B8 8 1D 23 (new) (changed=yes) Last Changed 0
IPX: Tu1:200.0260.8c8d.c558->CC0001.0000.0000.0001 ln= 42 tc=02, SPX: 80 0 7104 2B8 7 29 2E (new) (changed=yes) Last Changed 0
```

The following lines show SPX packets for connections that exist in the SPX table but that SPX idle time has not yet elapsed and spoofing has not started:

```
IPX: Et1:CC0001.0000.0000.0001->200.0260.8c8d.c558 ln= 42 tc=02, SPX: 80 0 2B8 7104 29 7 7 (early)
```
The following lines show an IPX watchdog packet and the spoofed reply:

```
IPX: E1:CC0001.0000.0000.0001->200.0260.8c8d.da75 ln= 42 tc=02, SPX: 80 0 4B8 7004 1D 8 8
(early)
```

The following lines show SPX packets that arrived more than two minutes after spoofing started. This situation occurs when the other sides of the SPX table are cleared. When the table is cleared, the routing processes stop spoofing the connection, which allows SPX keepalives from the local side to travel to the remote side and repopulate the SPX table.

```
IPX: Tu1:200.0260.8c8d.da75->CC0001.0000.0000.0001 ln= 42 tc=02, SPX: 80 0 7004 4B8 8 1D 23 (changed:clear) Last Changed 0
IPX: Et1:CC0001.0000.0000.0001->200.0260.8c8d.c558 ln= 42 tc=02, SPX: C0 0 2B8 7104 29 7 7 (early)
IPX: Tu1:200.0260.8c8d.c558->CC0001.0000.0000.0001 ln= 42 tc=02, SPX: 80 0 7104 2B8 7 29 2E (changed:clear) Last Changed 0
```

The following lines show that an SPX keepalive packet came in and was spoofed:

```
IPX: Et1:CC0001.0000.0000.0001->200.0260.8c8d.c558 ln= 42 tc=02, SPX: C0 0 2B8 7104 29 7 7 (Last Changed 272 sec)
IPX: local:200.0260.8c8d.c558->CC0001.0000.0000.0001 ln= 42 tc=02, spx keepalive sent 80 0 7104 2B8 7 29 2E
```
**debug ipx spx**

To display debugging messages related to the Sequenced Packet Exchange (SPX) protocol, use the `debug ipx spx` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug ipx spx
no debug ipx spx
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

Use the `debug ipx spx` command to display handshaking or negotiating details between the SPX protocol and the other protocols or applications. SPX debugging messages indicate various states of SPX connections such as incoming and outgoing traffic information, timer events, and related processing of SPX connections.

**Examples**

The following is sample output from the `debug ipx spx` command:

```
Router# debug ipx spx
SPX: Sent an SPX packet
SPX: I Con Src/Dst 776E/20A0 d-strm 0 con-ctl 80
SPX: I Con Src/Dst 776E/20A0 d-strm FE con-ctl 40
SPX: C847C Connection close requested by peer
SPX: Sent an SPX packet
SPX: purge timer fired. Cleaning up C847C
SPX: purging spxcon C847C from conQ
SPX: returning inQ buffers
SPX: returning outQ buffers
SPX: returning unackedQ buffers
SPX: returning spxcon
SPX: I Con Src/Dst 786E/FFFF d-strm 0 con-ctl C0
SPX: new connection request for listening socket
SPX: Sent an SPX packet
SPX: I Con Src/Dst 786E/20B0 d-strm 0 con-ctl 40
SPX: 300 bytes data recvd
SPX: Sent an SPX packet

The following line indicates an incoming SPX packet that has a source connection ID of 776E and a destination connection ID of 20A0 (both in hexadecimal). The data stream value in the SPX packet is indicated by `d-strm`, and the connection control value in the SPX packet is indicated by `con-ctl` (both in hexadecimal). All data packets received are followed by an SPX debugging message indicating the size of the packet. All control packets received are consumed internally.

SPX: I Con Src/Dst 776E/20A0 d-strm 0 con-ctl 80
```
debug isdn

To display messages about activity in the structure and operation of ISDN in the Cisco IOS software, use the debug isdn command in privileged EXEC mode. To disable the ISDN debugging command, use the no form of this command.

d debug isdn \{all | api name | cc [{detail | interface \{bri number | serial port/number\}}] | error [interface \{bri number | serial port/number\}] | events | mgmnt [{detail | interface \{bri number | serial port/number\}}] | q921 | q931 | standard [interface \{bri number | serial port/number\}] | tgrm\}

no debug isdn \{all | api name | cc [{detail | interface \{bri number | serial port/number\}}] | error [interface \{bri number | serial port/number\}] | events | mgmnt [{detail | interface \{bri number | serial port/number\}}] | q921 | q931 | standard [interface \{bri number | serial port/number\}] | tgrm\}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enables all debug isdn commands on all interfaces.</td>
</tr>
<tr>
<td>api name</td>
<td>Enables application programming interfaces (APIs) contained in ISDN on all interfaces. The name argument can be any one of the following APIs. The APIs must be entered one per command-line interface (CLI) command. To enable all of the APIs, use the all keyword.</td>
</tr>
<tr>
<td>cc</td>
<td>Enables ISDN Call Control debug messages on all interfaces or, optionally, on a specific interface if you use the interface keyword. Call Control is a layer of processing within ISDN that is above the Q.931 protocol processing layer, but below the host and API layers.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Generates more information during the processing of a specific request.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Limits the debug isdn capability to one BRI or serial interface.</td>
</tr>
<tr>
<td>bri number</td>
<td>(Optional) Identifies a single BRI interface number (BRI 2, for example) to which the debug isdn command is applied.</td>
</tr>
<tr>
<td>serial port / number</td>
<td>(Optional) Identifies a single serial port and number (serial 1/0, for example) to which the debug isdn command is applied. Acceptable values are 0 through 7.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>error</td>
<td>Generates error messages for normal exception conditions in the software on all interfaces or on a specific interface if you use the <code>interface</code> keyword. The actual significance of the message can be determined only by a detailed examination of surrounding debug messages.</td>
</tr>
<tr>
<td>events</td>
<td>Displays ISDN events occurring on the user side of the ISDN interface. See the <code>debug isdn event s</code> command page.</td>
</tr>
<tr>
<td>mgmnt</td>
<td>Enables ISDN Management Entity messages on all interfaces or, optionally, on a specific interface. Management Entity controls the activation and deactivation of Q.921 resources.</td>
</tr>
<tr>
<td>q921</td>
<td>Displays data link layer access procedures that are taking place at the router on the Link Access Protocol D-channel (LAPD) of its ISDN interface. See the <code>debug isdn q921</code> command page.</td>
</tr>
<tr>
<td>q931</td>
<td>Displays information about call setup and teardown of ISDN network connections between the local router and the network. See the <code>debug isdn q931</code> command page.</td>
</tr>
<tr>
<td>standard</td>
<td>Enables a selected set of <code>isdn debug</code> command messages on all interfaces or, optionally, on a specific interface if you use the <code>interface</code> keyword, that should provide sufficient information to determine why a problem is occurring.</td>
</tr>
<tr>
<td>tgrm</td>
<td>Displays ISDN trunk group resource manager information. See the <code>debug isdn tgrm</code> command page.</td>
</tr>
</tbody>
</table>

**Command Default**

Commands are enabled on all interfaces unless a specific interface is specified.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2T</td>
<td>This command was enhanced with the <code>all api cc error mgmnt</code>, and <code>standard</code> keywords.</td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>The <code>mgmnt</code> keyword was enhanced to display information about sharing the terminal endpoint identifier (TEI) when the <code>isdn x25 dchannel q93-broadcast</code> command is enabled for service access point identifier (SAPI) procedures that accept X.25 calls on the BRI D channel.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Please read the following caution before using this command.

⚠️ **Caution**

With the exception of the `debug isdn events`, `debug isdn q921`, `debug isdn q931`, and `debug isdn tgrm` commands, the commands described on this page are not intended for customer use and can cause ISDN or the Cisco IOS software to fail. The `debug isdn events`, `debug isdn q921`, `debug isdn q931`, and `debug isdn tgrm` commands are described on separate command pages.
Follow all instructions from Cisco technical support personnel when enabling and disabling these commands.

**Examples**

The general format of the `debug isdn` command messages is as follows:

- date and time: ISDN interface feature: text message

The text message can be used to determine activity in the structure and operation of ISDN in the Cisco IOS software, ISDN messages, and ISDN signaling procedures. The message must be interpreted by Cisco technical personnel.

The following example shows a typical message for the `debug isdn cc` command:

```
*Mar 1 02:29:27.751: ISDN Se1/0:23 CC: CCPRI_Go: source id 0x300, call id 0x8008, event
  0x341 (pre-ccb recovery)
```

The following example enables a selected set of `debug isdn` messages that should provide sufficient information for Cisco technical personnel to determine why a problem is occurring on BRI interface 2:

```
Router# debug isdn standard interface bri 2
```

The following report (highlighted in bold for purpose of example) is displayed when the isdn x25 dechannel q931-broadcast command is used to enable sharing the TEI:

```
Router# debug isdn mgmnt
*Jun 8 22:38:56.535: ISDN BR0 Q921: User TX -> IDREQ ri=29609 ai=127
*Jun 8 22:38:56.595: ISDN BR0 Q921: User RX <- IDASSN ri=29609 ai=86
*Jun 8 22:38:56.595: ISDN BR0 SERROR: L2_Go: at bailout DLCB is NULL
  L2: sapi 63 tei 127 ces 0 ev 0x3
*Jun 8 22:38:56.595: ISDN BR0 MGNT: LM_MDL_UI_DATA_IND: message 2 ri 29609 ai 86 switch
type 9
tei 85 tei 85
```
debug isdn event

To display ISDN events occurring on the user side (on the router) of the ISDN interface, use the `debug isdn event` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
default isdn event
no debug isdn event
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1x.x(x)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(3rd)T</td>
<td>This command was enhanced to display reports about SAPI 0 procedures that accept X.25 calls on the BRI D channel.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Although the `debug isdn event` and the `debug isdn q931` commands provide similar debug information, the information is displayed in a different format. If you want to see the information in both formats, enable both commands at the same time. The displays will be intermingled.

The ISDN events that can be displayed are Q.931 events (call setup and teardown of ISDN network connections).

Use the `show dialer` command to retrieve information about the status and configuration of the ISDN interface on the router.

Use the `service timestamps debug datetime msec` global configuration command to include the time with each message.

For more information on ISDN switch types, codes, and values, see Appendix B, “ISDN Switch Types, Codes, and Values.”

**Examples**

The following is sample output from the `debug isdn event` command of call setup events for an outgoing call:

```
Router# debug isdn event
ISDN Event: Call to 415555121202
  received HOST_PROCEEDING
  Channel ID i = 0x0101
-------------------
Channel ID i = 0x89
  received HOST_CONNECT
  Channel ID i = 0x0101
ISDN Event: Connected to 415555121202 on B1 at 64 Kb/s
```
The following shows sample `debug isdn event` output of call setup events for an incoming call. The values used for internal purposes are unpacked information elements. The values that follow the ISDN specification are an interpretation of the unpacked information elements.

```
Router# debug isdn event
received HOST_INCOMING_CALL
  Bearer Capability i = 0x080010
  Channel ID i = 0x0101
  Calling Party Number i = 0x0000, '415555121202'
  IE out of order or end of 'private' IEs --
  Bearer Capability i = 0x8890
  Channel ID i = 0x89
  Calling Party Number i = 0x0083, '415555121202'
ISDN Event: Received a call from 415555121202 on B1 at 64 Kb/s
ISDN Event: Accepting the call
received HOST_CONNECT
Channel ID i = 0x0101
ISDN Event: Connected to 415555121202 on B1 at 64 Kb/s
```

The following is sample output from the `debug isdn event` command of call teardown events for a call that has been disconnected by the host side of the connection:

```
Router# debug isdn event
received HOST_DISCONNECT
ISDN Event: Call to 415555121202 was hung up
```

The following is sample output from the `debug isdn event` command of a call teardown event for an outgoing or incoming call that has been disconnected by the ISDN interface on the router side:

```
Router# debug isdn event
ISDN Event: Hangup call to call id 0x8008
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bearer Capability</td>
<td>Indicates the requested bearer service to be provided by the network. See Table B-4 in Appendix B, “ISDN Switch Types, Codes, and Values.”</td>
</tr>
<tr>
<td>i=</td>
<td>Indicates the information element identifier. The value depends on the field it is associated with. Refer to the ITU-T Q.931 specification for details about the possible values associated with each field for which this identifier is relevant.</td>
</tr>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Channel ID</td>
<td>Channel Identifier. The values and corresponding channels might be identified in several ways:</td>
</tr>
<tr>
<td></td>
<td>- Channel ID (^0\times 0101) -- Channel B1</td>
</tr>
<tr>
<td></td>
<td>- Channel ID (^0\times 0102) -- Channel B2</td>
</tr>
<tr>
<td></td>
<td>ITU-T Q.931 defines the values and channels as exclusive or preferred:</td>
</tr>
<tr>
<td></td>
<td>- Channel ID (^0\times 083) -- Any B channel</td>
</tr>
<tr>
<td></td>
<td>- Channel ID (^0\times 089) -- Channel B1 (exclusive)</td>
</tr>
<tr>
<td></td>
<td>- Channel ID (^0\times 08A) -- Channel B2 (exclusive)</td>
</tr>
<tr>
<td></td>
<td>- Channel ID (^0\times 081) -- B1 (preferred)</td>
</tr>
<tr>
<td></td>
<td>- Channel ID (^0\times 082) -- B2 (preferred)</td>
</tr>
<tr>
<td>Calling Party Number</td>
<td>Identifies the called party. This field is only present in outgoing calls. The Calling Party Number field uses the IA5 character set. Note that it may be replaced by the Keypad facility field.</td>
</tr>
<tr>
<td>IE out of order or end of 'private’ IEs</td>
<td>Indicates that an information element identifier is out of order or there are no more private network information element identifiers to interpret.</td>
</tr>
<tr>
<td>Received a call from 41555121202 on B1 at 64 Kb/s</td>
<td>Identifies the origin of the call. This field is present only in incoming calls. Note that the information about the incoming call includes the channel and speed. Whether the channel and speed are displayed depends on the network delivering the calling party number.</td>
</tr>
</tbody>
</table>

The following is sample output from the `debug isdn event` command of a call teardown event for a call that has passed call screening and then has been hung up by the ISDN interface on the far end side:

```
Router# debug isdn event
Jan 3 11:29:52.559: ISDN BR0: RX <- DISCONNECT pd = 8 callref = 0x81
Jan 3 11:29:52.563: Cause i = 0x8090 - Normal call clearing
```

The following is sample output from the `debug isdn event` command of a call teardown event for a call that has not passed call screening and has been rejected by the ISDN interface on the router side:

```
Router# debug isdn event
Jan 3 11:32:03.263: ISDN BR0: RX <- DISCONNECT pd = 8 callref = 0x85
Jan 3 11:32:03.267: Cause i = 0x8095 - Call rejected
```

The following is sample output from the `debug isdn event` command of a call teardown event for an outgoing call that uses a dialer subaddress:

```
Router# debug isdn event
Jan 3 11:41:48.483: ISDN BR0: Event: Call to 61885:1212 at 64 Kb/s
Jan 3 11:41:48.495: ISDN BR0: TX -> SETUP pd = 8 callref = 0x04
Jan 3 11:41:48.495: Bearer Capability i = 0x8890
Jan 3 11:41:48.499: Channel ID i = 0x83
Jan 3 11:41:48.503: Called Party Number i = 0x80, '61885'
```
The output is similar to the output of `debug isdn q931`. Refer to the `debug isdn q931` command for detailed field descriptions.

The following is sample output from the `debug isdn event` command of call setup events for a successful callback for legacy DDR:

```
Router# debug isdn event
BRI0: Caller id Callback server starting to spanky 81012345678902
: Callback timer expired
BRI0: beginning callback to spanky 81012345678902
BRI0: Attempting to dial 81012345678902
```

The following is sample output from the `debug isdn event` command for a callback that was unsuccessful because the router had no dialer map for the calling number:

```
Router# debug isdn event
BRI0: Caller id 81012345678902 callback - no matching map
```

The table below describes the significant fields shown in the display.

```
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BRI0: Caller id Callback server starting to ...</td>
<td>Caller ID callback has started, plus host name and number called. The callback enable timer starts now.</td>
</tr>
<tr>
<td>: Callback timer expired</td>
<td>Callback timer has expired; callback can proceed.</td>
</tr>
<tr>
<td>BRI0: beginning callback to ... BRI0: Attempting to dial ...</td>
<td>Actions proceeding after the callback timer expired, plus host name and number called.</td>
</tr>
</tbody>
</table>
```

The following is sample output from the `debug isdn event` command for a callback that was successful when the dialer profiles DDR feature is configured:

```
*Mar 1 00:46:51.827: BR0:1: Caller id 81012345678901 matched to profile delorean
*Mar 1 00:46:51.827: Dialer1: Caller id Callback server starting to delorean 81012345678901
*Mar 1 00:46:54.155: : Callback timer expired
*Mar 1 00:46:54.151: Dialer1: beginning callback to delorean 81012345678901
*Mar 1 00:46:54.155: Freeing callback to delorean 81012345678901
```
The following example provides information about accepting X.25 calls on the ISDN D channel (for purpose of example, bold type indicates messages of interest in the following output):

```
Router# debug isdn event
*Sep 28 12:34:29.747: ISDN BR1/1 EVENTd: isdn_host_packet_mode_events: Host packet call received call id 0xB
```

The table below describes significant fields of call setup events for a successful callback for the sample output from the `debug isdn event` command when the dialer profiles DDR feature is configured.

### Table 87: `debug isdn event` Field Descriptions for Caller ID Callback and Dialer Profiles

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BR0:1:Caller id ... matched to profile ...</td>
<td>Interface, channel number, caller ID that are matched, and the profile to bind to the interface.</td>
</tr>
<tr>
<td>: Callback timer expired</td>
<td>Callback timer has expired; callback can proceed.</td>
</tr>
<tr>
<td>Dialer1:beginning callback to...</td>
<td>Callback process is beginning to the specified number.</td>
</tr>
<tr>
<td>Freeing callback to...</td>
<td>Callback has been started to the specified number, and the number has been removed from the callback list.</td>
</tr>
<tr>
<td>BRI0: Dialing cause Callback return call BRI0: Attempting to dial</td>
<td>The reason for the call and the number being dialed.</td>
</tr>
<tr>
<td>%LINK-3-UPDOWN: Interface BRI0:2, changed state to up</td>
<td>Interface status: up.</td>
</tr>
<tr>
<td>%DIALER-6-BIND: Interface BRI0:2 bound to profile Dialer1</td>
<td>Profile bound to the interface.</td>
</tr>
<tr>
<td>%LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:2, changed state to up</td>
<td>Line protocol status: up.</td>
</tr>
<tr>
<td>%ISDN-6-CONNECT: Interface BRI0:2 is now connected to ...</td>
<td>Interface is now connected to the specified host and number.</td>
</tr>
<tr>
<td>isdn_host_packet_mode_events: Host packet call received call id 0xB</td>
<td>Host is accepting incoming X.25 call using ITU Q.931 SAPI value 0 procedures.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug isdn q931</code></td>
<td>Displays call setup and teardown information of ISDN Layer 3 network connections.</td>
</tr>
</tbody>
</table>
**debug isdn q921**

To display data link layer (Layer 2) access procedures that are taking place at the router on the D channel (Link Access Procedure or LAPD) of its ISDN interface, use the `debug isdn q921` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
d debug isdn q921 [{detail | frame | interface [bri number]}]
no debug isdn q921 [{detail | frame | interface}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>detail</code></td>
<td>(Optional) Displays ISDN Q.921 packet detail.</td>
</tr>
<tr>
<td><code>frame</code></td>
<td>(Optional) Displays ISDN Q.921 frame contents.</td>
</tr>
<tr>
<td><code>interface</code></td>
<td>(Optional) Specifies an interface for debugging.</td>
</tr>
<tr>
<td><code>bri number</code></td>
<td>(Optional) Specifies the BRI interface and selects the interface number.</td>
</tr>
<tr>
<td></td>
<td>Valid values are from 0 to 6.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)ZJ</td>
<td>The <code>detail</code> and <code>frame</code> keywords were added.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The ISDN data link layer interface provided by the router conforms to the user interface specification defined by ITU-T recommendation Q.921. The `debug isdn q921` command output is limited to commands and responses exchanged during peer-to-peer communication carried over the D channel. This debug information does not include data transmitted over the B channels that are also part of the router ISDN interface. The peers (data link layer entities and layer management entities on the routers) communicate with each other with an ISDN switch over the D channel.

**Note**

The ISDN switch provides the network interface defined by Q.921. This debug command does not display data link layer access procedures taking place within the ISDN network (that is, procedures taking place on the network side of the ISDN connection). Refer to Appendix B, “ISDN Switch Types, Codes, and Values,” in the *ISDN Switch Types, Codes, and Values* document on Cisco.com for a list of the supported ISDN switch types.
A router can be the calling or called party of the ISDN Q.921 data link layer access procedures. If the router is the calling party, the command displays information about an outgoing call. If the router is the called party, the command displays information about an incoming call and the keepalives.

The `debug isdn q921` command can be used with the `debug isdn event`, `debug isdn q931`, `debug isdn q921 frame`, and `debug isdn q921 detail` commands at the same time. The displays are intermingled.

Use the `service timestamps debug datetime msec` global configuration command to include the time with each message.

**Examples**

The following is example output for a single active data link connection (DLC). The debugs turned on are `debug isdn q921`, `debug isdn q921 frame`, and `debug isdn q921 detail`. In the debugs below, “Q921” followed by a colon (:) indicates that `debug isdn q921` has been entered. “Q921” followed by the letter “f” indicates that `debug isdn q921 frame` has been entered. “Q921” followed by the letter “d” indicates that `debug isdn q921 detail` has been entered.

The following output shows that the L2 frame is received. The first two octets form the address field; the third octet forms the control field. The address field identifies the originator of a frame and whether it is a command or a response. The second octet of the address field identifies the DLC with which the frame is associated. The control field (third octet) contains the frame type code and sequence number information.

```
00:12:10:ISDN Q921d:isdn_from_driver_process:QUEUE_EVENT
00:12:10:ISDN Se1:15 Q921f:PBXb RX <- 0x0E03EF
```

The following output interprets the octet information. String “PBXb” indicates that the side receiving (RX) this frame is acting as a PBXb (as opposed to PBXa, which is the other possibility). This example also gives information about the type of frame received (SABMR), the associated DLC (1), the frame type code received from the control field (cntl=SABMR), and the sequence number (indicated by nbit, which is 0 in this case).

```
00:12:10:ISDN Se1:15 Q921:PBXb RX <- SABMR dlci=1 cntl=SABMR nbit=0
```

The following output shows information received from the driver (source_id of x200) showing an L2 frame (event x141). This results from the SABMR frame that was received from the peer PBX (v_bit and chan do not have any significance in this case).

```
00:12:10:ISDN Se1:15 Q921d:process_rxdata:Frame sent to L2
00:12:10:ISDN Q921d:isdn_from_driver_process:event_count 3
00:12:10:ISDN Se1:15 Q921d:dpnss_l2_main:source_id x200 event x141 v_bit x0 chan x0
```

The following output shows that DPNSS L2 for DLC 1 (chan 1) has received an SABMR frame (event x0) in the IDLE state (s_dpnss_idle):

```
00:12:10:ISDN Se1:15 Q921d:s_dpnss_idle:event x0 chan 1
```

The following output shows that for DLC 1 (chan 1 above), a UA frame (event x1) needs to be sent to the driver (dest x200):

```
00:12:10:ISDN Se1:15 Q921d:dpnss_l2_mail:dest x200 event x1 v_bit 1 chan 1 out_pkt x630531A4
```

The following output shows that for DLC 1, a DL_EST_IND (event x201) needs to be sent to L3 (DUA in this case because of the backhauling) indicating that this DLC is now up (in RESET COMPLETE state):
The following output shows that the L2 frame is transmitted (TX):

```
00:12:10:ISDN Se1:15 Q921d:dnss_l2_mail:dest x300 event x201 v_bit 1 chan 1 out_pkt x0
```

The following output shows that string “PBXb” is the side transmitting (TX) and that this frame is acting as PBX B. This example also gives information about the associated DLC (1), the frame type code transmitted from the control field (cntl=UA), and the sequence number (indicated by nbit, which is 0 in this case).

```
00:12:10:ISDN Se1:15 Q921:PBXb TX -> UA dlci=1 cntl=UA nbit=0
```

The following is complete debugging output from a DPNSS call:

```
Jan 8 17:24:43.499:ISDN Q921d:isdn_l2d_srq_process:QUEUE_EVENT
Jan 8 17:24:43.499:ISDN Se2/0:15 Q921f:PBXa TX -> UI(R) dlci=1 cntl=UI nbit=0
Jan 8 17:24:43.499:ISDN Q921d:isdn_l2d_srq_process:event_count 1
Jan 8 17:24:43.503:ISDN Q921d:isdn_from_driver_process:QUEUE_EVENT
Jan 8 17:24:43.507:ISDN Se2/0:15 Q921:PBXa RX <- 0x44030300102A34232A35302A33333330
Jan 8 17:24:43.507:ISDN Se2/0:15 Q921:PBXa RX <- i=0x00102A34232A35302A3333333030303031234343434343030303031
Jan 8 17:24:43.507:ISDN Q921d:dpnss_l2_main:source_id x200 event x2 chan 1
Jan 8 17:24:43.507:ISDN Se2/0:15 Q921d:dpnss_l2_main:source_id x200 event x200 event x3 v_bit 1 chan 1 out_pkt x63F183D4
Jan 8 17:24:43.507:ISDN Q921d:isdn_l2d_srq_process:QUEUE_EVENT
Jan 8 17:24:43.507:ISDN Se2/0:15 Q921f:PBXa TX -> 0x44030300102A34232A35302A33333330
Jan 8 17:24:43.507:ISDN Se2/0:15 Q921:PBXa RX <- UI(C) dlci=1 cntl=UI nbit=0
Jan 8 17:24:43.507:ISDN Q921d:isdn_l2d_srq_process:event_count 1
Jan 8 17:24:43.515:ISDN Q921d:isdn_from_driver_process:QUEUE_EVENT
Jan 8 17:24:43.515:ISDN Q921d:dpnss_l2_main:source_id x200 event x200 event x3 v_bit 1 chan 1 out_pkt x63F183D4
Jan 8 17:24:43.515:ISDN Se2/1:15 Q921d:dpnss_l2_main:source_id x4 event x240 v_bit 0 chan x2
Jan 8 17:24:43.519:ISDN Se2/1:15 Q921d:dpnss_l2_main:source_id x240 event x240 chan 1
Jan 8 17:24:43.519:ISDN Se2/1:15 Q921d:dpnss_l2_main:dest x200 event x2
```
v_bit 1 chan 1 out_pkt x63EE5780
Jan 8 17:24:43.599:ISDN Se2/1:15 LIFd:LIF_StartTimer:timer (0x63E569A8),
ticks (500), event (0x1201)
Jan 8 17:24:43.599:ISDN Q921d:isdn_l2d_srq_process:QUEUE_EVENT
Jan 8 17:24:43.599:ISDN Se2/1:15 Q921f:PBXa TX ->
0x46030300102A31232A35302A33333330
Jan 8 17:24:43.599:ISDN Se2/1:15 Q921f:PBXa RX <= 0x460303123A33333330303030303031
Jan 8 17:24:43.599:ISDN Q921d:isdn_l2d_srq_process:QUEUE_EVENT
Jan 8 17:24:43.623:ISDN Se2/1:15 Q921f:PBXa RX <= 0x460303
Jan 8 17:24:43.623:ISDN Se2/1:15 Q921f:PBXa RX <= UI(R) dlci=1 cntl=UI nbit=1
Jan 8 17:24:43.623:ISDN Se2/1:15 Q921d:process_rxdata:Frame sent to L2
Jan 8 17:24:43.623:ISDN Se2/1:15 Q921d:dpnss_l2_mail:dest x200 event
x141 v_bit x0 chan x0
Jan 8 17:24:43.627:ISDN Se2/1:15 Q921d:dpnss_l2_main:source_id x200 event
x141 v_bit x0 chan x0
Jan 8 17:24:43.627:ISDN Q921d:isdn_l2d_srq_process:QUEUE_EVENT
Jan 8 17:24:43.719:ISDN Q921d:isdn_l2d_srq_process:QUEUE_EVENT
Jan 8 17:24:43.719:ISDN Se2/1:15 Q921f:PBXa RX <= 0x440313092A34232A35302A3333333030303030
Jan 8 17:24:43.719:ISDN Se2/1:15 Q921f:PBXa RX <= UI(C) dlci=1 cntl=UI nbit=1
Jan 8 17:24:43.719:ISDN Se2/1:15 Q921d:process_rxdata:Frame sent to L2
Jan 8 17:24:43.719:ISDN Se2/1:15 Q921d:dpnss_l2_main:source_id x200 event
x141 v_bit x0 chan x0
Jan 8 17:24:43.719:ISDN Q921d:isdn_l2d_srq_process:QUEUE_EVENT
Jan 8 17:24:43.723:ISDN Q921d:isdn_l2d_srq_process:QUEUE_EVENT
Jan 8 17:24:43.723:ISDN Se2/1:15 Q921f:PBXa RX <= 0x4403132A35302A33333330303030303030303031
Jan 8 17:24:43.723:ISDN Se2/1:15 Q921f:PBXa RX <= UI(R) dlci=1 cntl=UI nbit=1
Jan 8 17:24:43.723:ISDN Se2/1:15 Q921d:process_rxdata:Frame sent to L2
Jan 8 17:24:43.727:ISDN Se2/1:15 Q921f:PBXa RX <= 0x440313092A34232A35302A33333330303030303030303031
Jan 8 17:24:43.727:ISDN Se2/1:15 Q921f:PBXa RX <= UI(C) dlci=1 cntl=UI nbit=1
Jan 8 17:24:43.727:ISDN Se2/1:15 Q921d:process_rxdata:Frame sent to L2
Jan 8 17:24:43.727:ISDN Se2/1:15 Q921d:dpnss_l2_mail:dest x200 event
x141 v_bit x0 chan x0
Jan 8 17:24:43.731:ISDN Q921d:isdn_l2d_srq_process:QUEUE_EVENT
Jan 8 17:24:43.731:ISDN Se2/1:15 Q921d:dpnss_l2_main:source_id x200 event
x141 v_bit x0 chan x0
Jan 8 17:24:43.731:ISDN Q921d:isdn_l2d_srq_process:QUEUE_EVENT
Jan 8 17:24:43.731:ISDN Se2/1:15 Q921d:dpnss_l2_mail:dest x200 event x3
v_bit 1 chan 1 out_pkt x63EE57CC
Jan 8 17:24:43.731:ISDN Se2/1:15 Q921d:dpnss_l2_mail:dest x200 event x3
v_bit 1 chan 1 out_pkt x63EE57CC
Jan 8 17:24:43.731:ISDN Se2/1:15 Q921d:dpnss_l2_mail:dest x200 event x3
v_bit 1 chan 1 out_pkt x63EE57CC
Jan 8 17:24:43.731:ISDN Se2/1:15 Q921d:dpnss_l2_mail:dest x200 event x3
v_bit 1 chan 1 out_pkt x63EE57CC
Jan 8 17:24:43.731:ISDN Q921d:isdn_l2d_srq_process:QUEUE_EVENT
Jan 8 17:24:43.731:ISDN Se2/1:15 Q921d:isdn_l2d_srq_process:QUEUE_EVENT
Jan 8 17:24:43.731:ISDN Se2/1:15 Q921d:isdn_l2d_srq_process:QUEUE_EVENT
Jan 8 17:24:43.731:ISDN Q921d:isdn_l2d_srq_process:QUEUE_EVENT
Jan 8 17:24:43.739:ISDN Se2/1:15 Q921:PBXa RX <- UI(C) dlci=1 cntl=UI nbit=1 i=0x092A34232A35302A3434343030303031232A31382A33312A33312A3332
Jan 8 17:24:43.739:ISDN Se2/1:15 Q921d:process_rxdata:Frame sent to L2
Jan 8 17:24:43.739:ISDN Q921d:isdn_from_driver_process:event_count 1
Jan 8 17:24:43.739:ISDN Se2/1:15 Q921d:dpnss_l2_main:source_id x200 event x141 v_bit x0 chan x0
Jan 8 17:24:43.739:ISDN Se2/1:15 Q921d:s_dpnss_information_transfer:event x200 chan 1
Jan 8 17:24:43.739:ISDN Se2/1:15 Q921d:dpnss_l2_mail:dest x200 event x141 v_bit 1 chan 1 source_id x200 event x3
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921d:process_rxdata:Frame sent to L2
Jan 8 17:24:43.739:ISDN Q921d:isdn_from_driver_process:event_count 1
Jan 8 17:24:43.739:ISDN Q921d:isdn_l2d_srq_process:QUEUE_EVENT
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921f:PBXa TX -> 0x440313
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921:PBXa TX -> UI(R) dlci=1 cntl=UI nbit=1
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921d:dpnss_l2_main:source_id x200 event x400 v_bit x0 chan x2
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921d:s_dpnss_information_transfer:event x200 chan 1
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921d:dpnss_l2_mail:dest x200 event x3 v_bit 1 chan 1 out_pkt x63EE57CC
Jan 8 17:24:43.739:ISDN Q921d:isdn_l2d_srq_process:event_count 1
Jan 8 17:24:43.739:ISDN Q921d:isdn_from_driver_process:QUEUE_EVENT
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921f:PBXa RX <- 0x460313092A31232A35302A343434303030303123
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921:PBXa RX <- UI(R) dlci=1 cntl=UI nbit=1
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921d:dpnss_l2_main:source_id x200 event x4 event x240 v_bit x0 chan x2
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921d:s_dpnss_information_transfer:event x240 chan 1
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921d:dpnss_l2_mail:dest x200 event x2 v_bit 1 chan 1 out_pkt x636B1B64
Jan 8 17:24:43.739:ISDN Q921d:isdn_l2d_srq_process:event_count 1
Jan 8 17:24:43.739:ISDN Q921d:isdn_from_driver_process:QUEUE_EVENT
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921f:PBXa TX -> 0x460313092A31232A35302A343434303030303123
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921:PBXa TX -> UI(C) dlci=1 cntl=UI nbit=0
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921d:dpnss_l2_main:source_id x200 event x3 v_bit 1 chan 1 source_id x200 event x3
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921d:dpnss_l2_mail:dest x200 event x2 v_bit 1 chan 1 out_pkt x30631BCC
Jan 8 17:24:43.739:ISDN Q921d:process_rxdata:Frame sent to L2
Jan 8 17:24:43.739:ISDN Q921d:isdn_from_driver_process:event_count 1
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921f:PBXa RX <- 0x460313092A31232A35302A343434303030303123
Jan 8 17:24:43.739:ISDN Se2/0:15 Q921:PBXa RX <- UI(R) dlci=1 cntl=UI nbit=1
The following output shows details of the preceding debugging events.

The first two octets (0x4403) form the address field, while the third octet (0x03) is the control field. All the octets starting from the fourth constitute DPNSS L3 information, which needs to be backhauled to the Cisco PGW2200.

All of the octets following “i=” constitute DPNSS L3 information received from the peer.

In the INFORMATION TRANSFER state, DLC 1 received a UI(C) frame (event x2) from the peer carrying DPNSS L3 information:

Information is sent to the driver (dest x200), which is then sent to the peer: An Unnumbered Information--Response [UI(R)] (event x3) acknowledges the received Unnumbered Information--Command [UI(C)].

The following is sample output from the `debug isdn q921` command for an outgoing call:
The following lines indicate a Layer 2 link establishment.

The following lines indicate the message exchanges between the data link layer entity on the local router (user side) and the assignment source point (ASP) on the network side during the TEI assignment procedure. This assumes that the link is down and no TEI currently exists.

At 14:47:30.171, the local router data link layer entity sent an Identity Request message to the network data link layer entity to request a TEI value that can be used in subsequent communication between the peer data link layer entities. The request includes a randomly generated reference number (31815) to differentiate among user devices that request automatic TEI assignment and an action indicator of 127 to indicate that the ASP can assign any TEI value available. The ISDN user interface on the router uses automatic TEI assignment.
At 14:47:30.219, the network data link entity responds to the Identity Request message with an Identity Assigned message. The response includes the reference number (31815) previously sent in the request and TEI value (64) assigned by the ASP.

The following lines indicate the message exchanges between the layer management entity on the network and the layer management entity on the local router (user side) during the TEI check procedure:

Jan 3 14:47:30.227: ISDN BR0: RX <- IDCKRQ ri = 0 ai = 127
Jan 3 14:47:30.235: ISDN BR0: TX -> IDCKRP ri = 16568 ai = 64

At 14:47:30.227, the layer management entity on the network sends the Identity Check Request message to the layer management entity on the local router to check whether a TEI is in use. The message includes a reference number that is always 0 and the TEI value to check. In this case, an ai value of 127 indicates that all TEI values should be checked. At 14:47:30.227, the layer management entity on the local router responds with an Identity Check Response message indicating that TEI value 64 is currently in use.

The following lines indicate the messages exchanged between the data link layer entity on the local router (user side) and the data link layer on the network side to place the network side into modulo 128 multiple frame acknowledged operation. Note that the data link layer entity on the network side also can initiate the exchange.

Jan 3 14:47:30.223: ISDN BR0: TX -> SABMEp sapi = 0 tei = 64
Jan 3 14:47:30.239: ISDN BR0: RX <- UAf sapi = 0 tei = 64

At 14:47:30.223, the data link layer entity on the local router sends the SABME command with a SAPI of 0 (call control procedure) for TEI 64. At 14:47:30.239, the first opportunity, the data link layer entity on the network responds with a UA response. This response indicates acceptance of the command. The data link layer entity sending the SABME command may need to send it more than once before receiving a UA response.

The following lines indicate the status of the data link layer entities. Both are ready to receive I frames.

Jan 3 14:47:43.815: ISDN BR0: RX <- RRp sapi = 0 tei = 64 nr = 2
Jan 3 14:47:43.819: ISDN BR0: TX -> RRf sapi = 0 tei = 64 nr = 0

These I-frames are typically exchanged every 10 seconds (T203 timer).

The following is sample output from the `debug isdn q921` command for an incoming call. It is an incoming SETUP message that assumes that the Layer 2 link is already established to the other side.
The table below describes the significant fields shown in the display.

**Table 88: debug isdn q921 Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 3 14:49:47.391</td>
<td>Indicates the date and time at which the frame was sent from or received by the data link layer entity on the router. The time is maintained by an internal clock.</td>
</tr>
<tr>
<td>TX</td>
<td>Indicates that this frame is being sent from the ISDN interface on the local router (user side).</td>
</tr>
<tr>
<td>RX</td>
<td>Indicates that this frame is being received by the ISDN interface on the local router from the peer (network side).</td>
</tr>
<tr>
<td>IDREQ</td>
<td>Indicates the Identity Request message type sent from the local router to the network (ASP) during the automatic TEI assignment procedure. This message is sent in a UI command frame. The SAPI value for this message type is always 63 (indicating that it is a Layer 2 management procedure) but it is not displayed. The TEI value for this message type is 127 (indicating that it is a broadcast operation).</td>
</tr>
<tr>
<td>ri = 31815</td>
<td>Indicates the Reference number used to differentiate between user devices requesting TEI assignment. This value is a randomly generated number from 0 to 65535. The same ri value sent in the IDREQ message should be returned in the corresponding IDASSN message. Note that a Reference number of 0 indicates that the message is sent from the network side management layer entity and a reference number has not been generated.</td>
</tr>
<tr>
<td>ai = 127</td>
<td>Indicates the Action indicator used to request that the ASP assign any TEI value. It is always 127 for the broadcast TEI. Note that in some message types, such as IDREM, a specific TEI value is indicated.</td>
</tr>
<tr>
<td>IDREM</td>
<td>Indicates the Identity Remove message type sent from the ASP to the user side layer management entity during the TEI removal procedure. This message is sent in a UI command frame. The message includes a reference number that is always 0, because it is not responding to a request from the local router. The ASP sends the Identity Remove message twice to avoid message loss.</td>
</tr>
<tr>
<td>IDASSN</td>
<td>Indicates the Identity Assigned message type sent from the ISDN service provider on the network to the local router during the automatic TEI assignment procedure. This message is sent in a UI command frame. The SAPI value for this message type is always 63 (indicating that it is a Layer 2 management procedure). The TEI value for this message type is 127 (indicating it is a broadcast operation).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>ai = 64</td>
<td>Indicates the TEI value automatically assigned by the ASP. This TEI value is used by data link layer entities on the local router in subsequent communication with the network. The valid values are in the range from 64 to 126.</td>
</tr>
<tr>
<td>SABME</td>
<td>Indicates the set asynchronous balanced mode extended command. This command places the recipient into modulo 128 multiple frame acknowledged operation. This command also indicates that all exception conditions have been cleared. The SABME command is sent once a second for N200 times (typically three times) until its acceptance is confirmed with a UA response. For a list and brief description of other commands and responses that can be exchanged between the data link layer entities on the local router and the network, see ITU-T Recommendation Q.921.</td>
</tr>
<tr>
<td>sapi = 0</td>
<td>Identifies the service access point at which the data link layer entity provides services to Layer 3 or to the management layer. A SAPI with the value 0 indicates it is a call control procedure. Note that the Layer 2 management procedures such as TEI assignment, TEI removal, and TEI checking, which are tracked with the debug isdn q921 command, do not display the corresponding SAPI value; it is implicit. If the SAPI value were displayed, it would be 63.</td>
</tr>
<tr>
<td>tei = 64</td>
<td>Indicates the TEI value automatically assigned by the ASP. This TEI value will be used by data link layer entities on the local router in subsequent communication with the network. The valid values are in the range from 64 to 126.</td>
</tr>
<tr>
<td>IDCKRQ</td>
<td>Indicates the Identity Check Request message type sent from the ISDN service provider on the network to the local router during the TEI check procedure. This message is sent in a UI command frame. The ri field is always 0. The ai field for this message contains either a specific TEI value for the local router to check or 127, which indicates that the local router should check all TEI values. For a list and brief description of other message types that can be exchanged between the local router and the ISDN service provider on the network, see Appendix B, “ISDN Switch Types, Codes, and Values.”</td>
</tr>
<tr>
<td>IDCKRP</td>
<td>Indicates the Identity Check Response message type sent from the local router to the ISDN service provider on the network during the TEI check procedure. This message is sent in a UI command frame in response to the IDCKRQ message. The ri field is a randomly generated number from 0 to 65535. The ai field for this message contains the specific TEI value that has been checked.</td>
</tr>
<tr>
<td>UAf</td>
<td>Confirms that the network side has accepted the SABME command previously sent by the local router. The final bit is set to 1.</td>
</tr>
<tr>
<td>INFOc</td>
<td>Indicates that this is an Information command. It is used to transfer sequentially numbered frames containing information fields that are provided by Layer 3. The information is transferred across a data-link connection.</td>
</tr>
</tbody>
</table>
### Field Description

| INFORMATION pd = 8 callref = (null) | Indicates the information fields provided by Layer 3. The information is sent one frame at a time. If multiple frames need to be sent, several Information commands are sent. The pd value is the protocol discriminator. The value 8 indicates it is call control information. The call reference number is always null for SPID information. |
| SPID information i = 0x3431353930333833636031 | Indicates the SPID. The local router sends this information to the ISDN switch to indicate the services to which it subscribes. SPIIDs are assigned by the service provider and are usually 10-digit telephone numbers followed by optional numbers. Currently, only the DMS-100 switch supports SPIIDs, one for each B channel. If SPID information is sent to a switch type other than DMS-100, an error may be displayed in the debug information. |
| ns = 0 | Indicates the send sequence number of sent I frames. |
| nr = 0 | Indicates the expected send sequence number of the next received I frame. At time of transmission, this value should be equal to the value of ns. The value of nr is used to determine whether frames need to be re-sent for recovery. |
| RRR | Indicates the Receive Ready response for unacknowledged information transfer. The RRR is a response to an INFOc. |
| RRp | Indicates the Receive Ready command with the poll bit set. The data link layer entity on the user side uses the poll bit in the frame to solicit a response from the peer on the network side. |
| RRF | Indicates the Receive Ready response with the final bit set. The data link layer entity on the network side uses the final bit in the frame to indicate a response to the poll. |
| SAPI | Indicates the service access point identifier. The SAPI is the point at which data link services are provided to a network layer or management entity. Currently, this field can have the value 0 (for call control procedure) or 63 (for Layer 2 management procedures). |
| TEI | Indicates the terminal endpoint identifier (TEI) that has been assigned automatically by the assignment source point (ASP) (also called the layer management entity on the network side). The valid range is from 64 to 126. The value 127 indicates a broadcast. |

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug isdn event</td>
<td>Displays ISDN events occurring on the user side (on the router) of the ISDN interface.</td>
</tr>
<tr>
<td>debug isdn q931</td>
<td>Displays information about call setup and teardown of ISDN network connections (Layer 3) between the local router (user side) and the network.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>service timestamps debug datetime msec</td>
<td>Includes the time with each debug message.</td>
</tr>
</tbody>
</table>
debug isdn q931

To display information about call setup and teardown of ISDN network connections (Layer 3) between the local router (user side) and the network, use the `debug isdn q931` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug isdn q931 [asn1 | detail | interface [bri number]]
no debug isdn q931
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>asn1</code></td>
<td>(Optional) Displays ISDN Q.931 Abstract Syntax Notation number one (ASN.1) details.</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>(Optional) Displays ISDN Q.931 packet details.</td>
</tr>
<tr>
<td><code>interface</code></td>
<td>(Optional) Specifies an interface for debugging.</td>
</tr>
<tr>
<td><code>bri number</code></td>
<td>(Optional) Specifies the BRI interface and selects the interface number. Valid values are from 0 to 6.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>The <code>debug isdn</code> command was introduced.</td>
</tr>
<tr>
<td>12.3(11)T</td>
<td>This command was enhanced to display the contents of the Facility Information Element (IE) in textual format.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>asn1</code>, <code>detail</code>, <code>interface</code>, and <code>bri number</code> keywords and argument were added.</td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>This command was enhanced to display reports about SAPI 0 procedures that accept X.25 calls on the BRI D channel.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The ISDN network layer interface provided by the router conforms to the user interface specification defined by ITU-T recommendation Q.931 and to other specifications (for example, switch type VN4). The router only tracks activities that occur on the user side, not on the network side, of the network connection. The `debug isdn q931` command output is limited to commands and responses exchanged during peer-to-peer communication carried over the D channel. This debug information does not include data sent over B channels, which are also part of the router’s ISDN interface. The peers (network layers) communicate with each other via an ISDN switch over the D channel.

A router can be the calling or the called party of the ISDN Q.931 network connection call setup and teardown procedures. If the router is the calling party, the command displays information about an outgoing call. If the router is the called party, the command displays information about an incoming call.

This command decodes parameters of the Facility IE and displays them as text, with parameter values as they are applicable and relevant to the operation. In addition, the ASN.1 encoded Notification structure of the Notification-Indicator IE is also decoded.
You can use the `debug isdn q931` command with the `debug isdn event` and the `debug isdn q921` commands at the same time. The displays will be intermingled. Use the `service timestamps debug datetime msec` global configuration command to include the time with each message.

**Examples**

The following is sample output from the `debug isdn q931` command of a call setup procedure for an outgoing call:

```
Router# debug isdn q931
TX -> SETUP pd = 8 callref = 0x04
   Bearer Capability i = 0x8890
   Channel ID i = 0x83
   Called Party Number i = 0x80, '415555121202'
RX <- CALL_PROC pd = 8 callref = 0x84
   Channel ID i = 0x89
RX <- CONNECT pd = 8 callref = 0x84
TX -> CONNECT_ACK pd = 8 callref = 0x04....
Success rate is 0 percent (0/5)
```

The following is sample output from the `debug isdn q931` command of a call setup procedure for an incoming call:

```
Router# debug isdn q931
RX <- SETUP pd = 8 callref = 0x06
   Bearer Capability i = 0x8890
   Channel ID i = 0x89
   Calling Party Number i = 0x0083, '81012345678902'
TX -> CONNECT pd = 8 callref = 0x86
RX <- CONNECT_ACK pd = 8 callref = 0x06
```

The following is sample output from the `debug isdn q931` command that shows the contents of the Facility IE. The following example uses the supplementary service Malicious Call Identification (MCID). In this service, the router sends out the Facility IE.

```
Router# debug isdn q931
Sep 20 04:09:38.335 UTC: ISDN Se7/1:23 Q931: TX -> DISCONNECT pd = 8 callref = 0x0007
   Cause i = 0x8290 - Normal call clearing
   Facility i = 0x91A106020107020103
      Protocol Profile = Remote Operations Protocol 0xA106020107020103
      Component = Invoke component
      Invoke Id = 7 <MCID>
      Operation = MCIDRequest
```

The following is sample output from the `debug isdn q931` command of a call teardown procedure from the network:

```
Router# debug isdn q931
RX <- DISCONNECT pd = 8 callref = 0x84
   Cause i = 0x8790
   Looking Shift to Codeset 6
   Codeset 6 IE 0x1 1 0x82 '10'
TX -> RELEASE pd = 8 callref = 0x04
   Cause i = 0x8090
RX <- RELEASE_COMP pd = 8 callref = 0x84
```

The following example shows how to turn on the `debug isdn q931 asn1` capability and how to use the `show debug` command to display the results of the debug:
Router# debug isdn q931 asn1
debug isdn asn1 is ON.
Router# show debug

The following ISDN debugs are enabled on all DSLs:
debug isdn error is ON.
debug isdn event is ON.
debug isdn q931 is ON.
debug isdn asn1 is ON.
DEBUGS with ASN1 enabled:
    ice call = 0x1
00:08:49: Sub Msg = CDAPI_MSG_SUBTYPE_TBCT_REQ
00:08:49: Call Type = VOICE
00:08:49: B Channel = 0
00:08:49: Cause = 0
00:08:49: ISDN ASN1: isdnAsn1Component
00:08:49: ISDN ASN1: isdnAsn1Invoke
00:08:49: ISDN ASN1: isdnAsn1InvTBCT
00:08:49: ISDN ASN1: op Invoke TBCT
00:08:49: ISDN Se0:23 Q931: TX -> FACILITY pd = 8 callref = 0x8001
Facility i = 0x91A11102010506072A8648CE1500083003020101
*Jun 15 06:27:51.547: %ISDN-6-CONNECT: Interface Serial0:0 is now connected to 1 1111
00:08:51: ISDN Se0:23 Q931: RX <- FACILITY pd = 8 callref = 0x01
Facility i = 0x91A203020105A11302010180010506072A8648CE1500083003020164
00:08:51: ISDN ASN1: isdnAsn1Component
00:08:51: ISDN ASN1: isdnAsn1Res
00:08:51: ISDN ASN1: isdnAsn1ResTbct

The table below describes the significant fields shown in the displays, in alphabetical order.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bearer Capability</td>
<td>Indicates the requested bearer service to be provided by the network.</td>
</tr>
<tr>
<td>CALL_PROC</td>
<td>Indicates the CALL PROCEEDING message; the requested call setup has begun, and no more call setup information will be accepted.</td>
</tr>
<tr>
<td>Called Party Number</td>
<td>Identifies the called party. This field is present only in outgoing SETUP messages. Note that this field can be replaced by the Keypad facility field. This field uses the IA5 character set.</td>
</tr>
<tr>
<td>Calling Party Number</td>
<td>Identifies the origin of the call. This field is present only in incoming SETUP messages. This field uses the IA5 character set.</td>
</tr>
<tr>
<td>callref</td>
<td>Indicates the call reference number in hexadecimal notation. The value of this field indicates the number of calls made from either the router (outgoing calls) or the network (incoming calls).</td>
</tr>
<tr>
<td></td>
<td>Note that the originator of the SETUP message sets the high-order bit of the call reference number to 0.</td>
</tr>
<tr>
<td></td>
<td>The destination of the connection sets the high-order bit to 1 in subsequent call control messages, such as the CONNECT message.</td>
</tr>
<tr>
<td></td>
<td>For example, callref = 0x04 in the request becomes callref = 0x84 in the response.</td>
</tr>
<tr>
<td>Cause</td>
<td>Indicates the cause of the disconnect.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Channel ID</td>
<td>Indicates the channel identifier. The value 83 indicates any channel, 89 indicates the B1 channel, and 8A indicates the B2 channel. For more information about the channel identifier, see ITU-T Recommendation Q.931.</td>
</tr>
<tr>
<td>Codeset 6 IE 0x1 i = 0x82, ‘10’</td>
<td>Indicates charging information. This information is specific to the NTT switch type and may not be sent by other switch types.</td>
</tr>
<tr>
<td>CONNECT</td>
<td>Indicates that the called user has accepted the call.</td>
</tr>
<tr>
<td>CONNECT_ACK</td>
<td>Indicates that the calling user acknowledges the called user’s acceptance of the call.</td>
</tr>
<tr>
<td>DISCONNECT</td>
<td>Indicates either that the user side has requested the network to clear an end-to-end connection or that the network has cleared the end-to-end connection.</td>
</tr>
<tr>
<td>i =</td>
<td>Indicates the information element identifier. The value depends on the field with which the identifier is associated. See the ITU-T Q.931 specification for details about the possible values associated with each field for which this identifier is relevant.</td>
</tr>
<tr>
<td>Looking Shift to Codeset 6</td>
<td>Indicates that the next information elements will be interpreted according to information element identifiers assigned in codeset 6. Codeset 6 means that the information elements are specific to the local network.</td>
</tr>
<tr>
<td>pd</td>
<td>Indicates the protocol discriminator that distinguishes messages for call control over the user-network ISDN interface from other ITU-T-defined messages, including other Q.931 messages. The protocol discriminator is 8 for call control messages, such as SETUP. For basic-Tr6, the protocol discriminator is 65.</td>
</tr>
<tr>
<td>Protocol Profile</td>
<td>Remote operations protocol, which contains networking extensions for other services. This profile determines which protocol should be used to decode the rest of a Facility IE message. A Facility IE can contain multiple components. Each component displays a hexadecimal code followed by the code contents in text. In the example that included encoded ISDN Facility IE message output, 0xA106020107020103 is the hexadecimal code and represents the Facility IE Component, Invoke Id, and Operation. The Operation portion of the IE corresponds to the supplementary service that the component represents.</td>
</tr>
<tr>
<td>RELEASE</td>
<td>Indicates that the sending equipment will release the channel and call reference. The recipient of this message should prepare to release the call reference and channel.</td>
</tr>
<tr>
<td>RELEASE.Comp</td>
<td>Indicates that the sending equipment has received a RELEASE message and has now released the call reference and channel.</td>
</tr>
<tr>
<td>RX &lt;-&gt;</td>
<td>Indicates that this message is being received by the user side of the ISDN interface from the network side.</td>
</tr>
<tr>
<td>SETUP</td>
<td>Indicates that the SETUP message type has been sent to initiate call establishment between peer network layers. This message can be sent from either the local router or the network.</td>
</tr>
</tbody>
</table>
Indicates that this message is being sent from the local router (user side) to the network side of the ISDN interface.

Text in bold in the following example indicates the acceptance of an incoming X.25 call on the ISDN D channel, per ITU Q.931 SAPI value 0 procedures:

```
Router# debug isdn q931
*Sep 28 12:34:29.739: ISDN BR1/1 Q931: RX <- SETUP pd = 8  callref = 0x5C (re-assembled)
  Bearer Capability i = 0x88C0C2E6
  Standard = CCITT
  Transfer Capability = Unrestricted Digital
  Transfer Mode = Packet
  Transfer Rate = Packet - not specified
  User Info L2 Protocol = Recommendation Q921/I.441
  User Info L3 Protocol = Recommendation X.25, Packet Layer

  Channel ID i = 0x8C
    Exclusive, No B-channel

  Information Rate i = 0x8888
  Packet Layer Binary Params i = 0x80
  Packet Layer Window Size i = 0x8282
  Packet Size i = 0x8888
  Calling Party Number i = 0x0083, '144014384106'
    Plan:Unknown, Type:Unknown
  User-User i = 0x02CC000000
```

The command output is intermingled with information from the `debug isdn events` command; see the description for the `debug isdn events` command to understand significant fields displayed in this report.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug isdn events</td>
<td>Displays ISDN events occurring on the router (user side) of the ISDN interface.</td>
</tr>
<tr>
<td>debug isdn q921</td>
<td>Displays Layer 2 access procedures that are taking place at the router on the D channel of the ISDN interface.</td>
</tr>
<tr>
<td>service timestamps</td>
<td>Configure a time stamp on debugging or system logging messages.</td>
</tr>
</tbody>
</table>
debug isdn tgrm

To view ISDN trunk group resource manager information, use the `debug isdn tgrm` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```bash
default isdn tgrm
no default isdn tgrm
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Disable console logging and use buffered logging before using the `debug isdn tgrm` command. Using the `debug isdn tgrm` command generates a large volume of debugs, which can affect router performance.

**Examples**

Sample output from the `debug isdn tgrm` command is shown below.

The output shows that the channel used (bchan) is 1, service state is 0 (in-service), call_state is 2 (busy), “false busy” is 0, and DSL is 2. The output also shows that the B channel is 1, the channel is available, and the call state is transitioned from 0 (idle) to 2 (busy).

The last two lines of output shows that bchan is 1, call state is 1 (busy), call type is 2 (voice), and call direction is 1 (incoming).

```
00:26:31:ISDN:get_tgrm_avail_state:idb 0x64229380 bchan 1 service_state 0 call_state 2 false
busy 0x0 dsl 2
00:26:31:ISDN:update_tgrm_call_status:idb 0x64229380 bchan 1 availability state 1 call
state(prev,new) (0,2), dsl 2
00:26:31:ISDN:Calling TGRM with tgrm_call_isdn_update:idb 0x64229380 bchan 1 call state 1
call type 2 call dir 1
```

The table below provides an alphabetical listing of the fields shown in the `debug isdn tgrm` command output and a description of each field.

**Table 90: debug isdn tgrm Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>availability state</td>
<td>Indicates whether the channel is available:</td>
</tr>
<tr>
<td></td>
<td>0 = Not available 1 = Available</td>
</tr>
<tr>
<td>bchan</td>
<td>Bearer channel used for this call.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| call dir          | Direction of the call:  
0 = Incoming 1 = Outgoing                                                   |
| call_state        | State of the call. It has different values depending on whether it is from ISDN perspective or TGRM perspective.  
When printed from get_tgrm_avail_state(), it is the state value from ISDN perspective:  
0 = Idle 1 = Negotiate 2 = Busy 3 = Reserved 4 = Restart pending 5 = Maintenance pend 6 = Reassigned  
When printed from tgrm_call_isdn_update(), it is the state value from TGRM perspective:  
0 = Idle 1 = Busy 2 = Pending 3 = Reject                                           |
| call state (prev, new) | Indicates the state transition of the call. The state values are as shown in call_state from the ISDN perspective. |
| call type         | Type of call:  
0 = Invalid 1 = Data 2 = Voice 3 = Modem 4 = None                           |
| dsl               | Internal interface identifier.                                              |
| false busy        | Bit map of all the channels on the interface indicating their soft busy status. |
| idb               | Address of the interface descriptor block (IDB) for the interface.          |
| service_state     | Service state:  
0 = In-service 1 = Maintenance 2 = Out of service                           |

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show trunk group</td>
<td>Displays the configuration of the trunk group.</td>
</tr>
<tr>
<td>translation-profile (voice service POTS)</td>
<td>Assigns a translation profile to the interface.</td>
</tr>
<tr>
<td>trunk-group (interface)</td>
<td>Assigns a trunk group to the interface.</td>
</tr>
</tbody>
</table>
debug isis adj packets

To display information on all adjacency-related activity such as hello packets sent and received and Intermediate System-to-Intermediate System (IS-IS) adjacencies going up and down, use the `debug isis adj packets` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
display isis adj packets [interface]
do debug isis adj packets [interface]
```

**Syntax Description**

- `interface` (Optional) Interface or subinterface name.

**Command Modes**

Privileged EXEC

**Examples**

The following is sample output from the `debug isis adj packets` command:

```
Router# debug isis adj packets
ISIS-Adj: Rec L1 IIH from 0000.0c00.40af (Ethernet0), cir type 3, cir id BBBB.BBBB.BBBB.01
ISIS-Adj: Rec L2 IIH from 0000.0c00.40af (Ethernet0), cir type 3, cir id BBBB.BBBB.BBBB.01
ISIS-Adj: Rec L1 IIH from 0000.0c00.0c36 (Ethernet1), cir type 3, cir id CCCC.CCCC.CCCC.03
ISIS-Adj: Area mismatch, level 1 IIH on Ethernet1
ISIS-Adj: Sending L1 IIH on Ethernet1
ISIS-Adj: Sending L2 IIH on Ethernet1
ISIS-Adj: Rec L2 IIH from 0000.0c00.0c36 (Ethernet1), cir type 3, cir id BBBB.BBBB.BBBB.03
```

The following line indicates that the router received an IS-IS hello packet (IIH) on Ethernet interface 0 from the Level 1 router (L1) at MAC address 0000.0c00.40af. The circuit type is the interface type:

```
1--Level 1 only; 2--Level 2 only; 3--Level 1/2
```

The circuit ID is what the neighbor interprets as the designated router for the interface.

```
ISIS-Adj: Rec L1 IIH from 0000.0c00.40af (Ethernet0), cir type 3, cir id BBBB.BBBB.BBBB.01
```

The following line indicates that the router (configured as a Level 1 router) received on Ethernet interface 1 is an IS-IS hello packet from a Level 1 router in another area, thereby declaring an area mismatch:

```
ISIS-Adj: Area mismatch, level 1 IIH on Ethernet1
```

The following lines indicates that the router (configured as a Level 1/Level 2 router) sent on Ethernet interface 1 is a Level 1 IS-IS hello packet, and then a Level 2 IS-IS packet:

```
ISIS-Adj: Sending L1 IIH on Ethernet1
ISIS-Adj: Sending L2 IIH on Ethernet1
```
**debug isis authentication**

To enable debugging of Intermediate System-to-Intermediate System (IS-IS) authentication, use the `debug isis authentication` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug isis authentication information
no debug isis authentication information
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>information</code></td>
<td>Required keyword that specifies IS-IS authentication information.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(21)ST</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug isis authentication` command with the `information` keyword:

```
Router# debug isis authentication information
3d03h:ISIS-AuthInfo:No auth TLV found in received packet
3d03h:ISIS-AuthInfo:No auth TLV found in received packet
```

The sample output indicates that the router has been running for 3 days and 3 hours. Debugging output is about IS-IS authentication information. The local router is configured for authentication, but it received a packet that does not contain authentication data; the remote router does not have authentication configured.
debug isis ipv6 rib

To display debugging information for Integrated Intermediate System-to-Intermediate System (IS-IS) IPv6 Version 6 routes in the global or local Routing Information Base (RIB), use the debug isis rib command in privileged EXEC mode. To disable the debugging of IS-IS IPv6 routes, use the no form of this command.

```
debug isis ipv6 rib [{global | local [{access-list-number | terse]}]}
no debug isis ipv6 rib [{global | local}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>global</td>
<td>(Optional) Displays debugging information for IS-IS IP Version 4 routes in the global RIB.</td>
</tr>
<tr>
<td>local</td>
<td>(Optional) Displays debugging information for IS-IS IP Version 4 routes in the IS-IS local RIB.</td>
</tr>
<tr>
<td>access-list-number</td>
<td>(Optional) Number of an access list. This is a decimal number from 100 to 199 or from 2000 to 2699.</td>
</tr>
<tr>
<td>terse</td>
<td>(Optional) Will not display debug information if the IS-IS IP Version 4 IS-IS local RIB has not changed.</td>
</tr>
</tbody>
</table>

### Command Default

Debugging of IS-IS IPv6 routes is disabled.

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.6S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The following is sample output from the `debug isis ipv6 rib` command shows shows an IPv6 prefix tag.

The table below describes the significant fields shown in the display.

```
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>isis ipv6 tag</td>
<td>Configures an administrative tag value to be associated with an IPv6 address prefix.</td>
</tr>
</tbody>
</table>
debug isis mpls traffic-eng advertisements

To print information about traffic engineering advertisements in Intermediate System-to-Intermediate System (IS-IS) link-state advertisement (LSA) messages, use the `debug isis mpls traffic-eng advertisements` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
display isis mpls traffic-eng advertisements
```

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)ST</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(3)T</td>
<td>This command was integrated into Cisco IOS Release 12.1(3)T.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(22)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

Examples

In the following example, information about traffic engineering advertisements is printed in IS-IS LSA messages:

```
Router# debug isis mpls traffic-eng advertisements
System ID:Router1.00
Router ID:10.106.0.6
Link Count:1
    Neighbor System ID:Router2.00 (P2P link)
    Interface IP address:10.42.0.6
    Neighbor IP Address:10.42.0.10
    Admin. Weight:10
    Physical BW:155520000 bits/sec
    Reservable BW:500000 bits/sec
    BW unreserved[0]:2000000 bits/sec, BW unreserved[1]:1000000 bits/sec
    BW unreserved[2]:1000000 bits/sec, BW unreserved[3]:1000000 bits/sec
    BW unreserved[4]:1000000 bits/sec, BW unreserved[5]:1000000 bits/sec
    BW unreserved[6]:1000000 bits/sec, BW unreserved[7]:0 bits/sec
    Affinity Bits:0x00000000
```

The table below describes the significant fields shown in the display.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System ID</td>
<td>Identification value for the local system in the area.</td>
</tr>
<tr>
<td>Router ID</td>
<td>Multiprotocol Label Switching traffic engineering router ID.</td>
</tr>
<tr>
<td>Link Count</td>
<td>Number of links that MPLS traffic engineering advertised.</td>
</tr>
<tr>
<td>Neighbor System ID</td>
<td>Identification value for the remote system in an area.</td>
</tr>
<tr>
<td>Interface IP address</td>
<td>IPv4 address of the interface.</td>
</tr>
<tr>
<td>Neighbor IP Address</td>
<td>IPv4 address of the neighbor.</td>
</tr>
<tr>
<td>Admin. Weight</td>
<td>Administrative weight associated with this link.</td>
</tr>
<tr>
<td>Physical BW</td>
<td>Bandwidth capacity of the link (in bits per second).</td>
</tr>
<tr>
<td>Reservable BW</td>
<td>Amount of reservable bandwidth on this link.</td>
</tr>
<tr>
<td>BW unreserved</td>
<td>Amount of bandwidth that is available for reservation.</td>
</tr>
<tr>
<td>Affinity Bits</td>
<td>Attribute flags of the link that are being flooded.</td>
</tr>
</tbody>
</table>
**debug isis mpls traffic-eng events**

To print information about traffic engineering-related Intermediate System-to-Intermediate System (IS-IS) events, use the **debug isis mpls traffic-eng events** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```plaintext
debug isis mpls traffic-eng events
no debug isis mpls traffic-eng events
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)ST</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(3)T</td>
<td>This command was integrated into Cisco IOS Release 12.1(3)T.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(22)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, information is printed about traffic engineering-related IS-IS events:

```plaintext
Router# debug isis mpls traffic-eng events
ISIS-RRR:Send MPLS TE Et4/0/1 Router1.02 adjacency down:address 0.0.0.0
ISIS-RRR:Found interface address 10.1.0.6 Router1.02, building subtlv... 58 bytes
ISIS-RRR:Found interface address 10.42.0.6 Router2.00, building subtlv... 64 bytes
ISIS-RRR:Interface address 0.0.0.0 Router1.00 not found, not building subtlv
ISIS-RRR:LSP Router1.02 changed from 0x606BCD30
ISIS-RRR:Mark LSP Router1.02 changed because TLV contents different, code 16
ISIS-RRR:Received 1 MPLS TE links flood info for system id Router1.00
```
debug isis nsf

To display information about the Intermediate System-to-Intermediate System (IS-IS) state during a Cisco nonstop forwarding (NSF) restart, use the debug isis nsf command in privileged EXEC mode. To disable debugging output, use the no form of this command.

debug isis nsf [detail]
no debug isis nsf [detail]

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(Optional) Provides detailed debugging information.</td>
</tr>
</tbody>
</table>

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(22)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.2(20)S</td>
<td>Support for the Cisco 7304 router was added.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the debug isis nsf command to display basic information about the IS-IS state during an NSF restart. Use the debug isis nsf detail command to display additional IS-IS state detail during an NSF restart.

Examples

The following example displays IS-IS state information during an NSF restart:

```
router# debug isis nsf
IS-IS NSF events debugging is on

cisco@router# debug isis nsf detail
```

The following example displays detailed IS-IS state information during an NSF restart:

```
router# debug isis nsf detail
IS-IS NSF events (detailed) debugging is on
router# Jan 24 20:04:54.090:%CLNS-5-ADJCHANGE:ISIS:Adjacency to gsr1 (GigabitEthernet2/0/0) Up, Standby adjacency
Jan 24 20:04:54.090:ISIS-NSF:ADJ:000C.0000.0000 (Gi2/0/0), type 8/1, cnt 0/1, ht 10 (NEW)
Jan 24 20:04:54.142:ISIS-NSF:Rcv LSP - L2 000B.0000.0000.00-00, seq 251, csum B0DC, ht 120, len 123 (local)
Jan 24 20:04:55.510:ISIS-NSF:Rcv LSP - L1 000B.0000.0000.00-00, seq 23E, csum D20D, ht 120, len 58 (local)
Jan 24 20:04:56.494:ISIS-NSF:ADJ:000C.0000.0000 (Gi2/0/0), type 8/0, cnt 0/1, ht 10, len 123 (local)
Jan 24 20:04:56.494:ISIS-NSF:ADJ:000C.0000.0000 (Gi2/0/0), type 8/0, cnt 0/1, ht 30
Jan 24 20:04:56.502:ISIS-NSF:Rcv LSP - L1 000B.0000.0000.01-00, seq 21C, csum E197, ht 120, len 58 (local)
Jan 24 20:04:58.230:ISIS-NSF:Rcv LSP - L2 000C.0000.0000.00-00, seq 11A, csum E197, ht 1194,
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nsf (IS-IS)</td>
<td>Configures NSF operations for IS-IS.</td>
</tr>
<tr>
<td>nsf interface wait</td>
<td>Specifies how long an NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart.</td>
</tr>
<tr>
<td>nsf interval</td>
<td>Specifies the minimum time between NSF restart attempts.</td>
</tr>
<tr>
<td>nsf t3</td>
<td>Specifies the methodology used to determine how long IETF NSF will wait for the LSP database to synchronize before generating overloaded link state information for itself and flooding that information out to its neighbors.</td>
</tr>
<tr>
<td>show clns neighbors</td>
<td>Displays both ES and IS neighbors.</td>
</tr>
<tr>
<td>show isis nsf</td>
<td>Displays current state information regarding IS-IS NSF.</td>
</tr>
</tbody>
</table>
**debug isis rib**

To display debugging information for Integrated Intermediate System-to-Intermediate System (IS-IS) IP Version 4 routes in the global or local Routing Information Base (RIB), use the `debug isis rib` command in privileged EXEC mode. To disable the debugging of IS-IS IP Version 4 routes, use the `no` form of this command.

```
debug isis rib [{global | local [{access-list-number | terse}]}]
no debug isis rib [{global | local}]
```

**Syntax Description**
- **global** (Optional) Displays debugging information for IS-IS IP Version 4 routes in the global RIB.
- **local** (Optional) Displays debugging information for IS-IS IP Version 4 routes in the IS-IS local RIB.
- **access-list-number** (Optional) Number of an access list. This is a decimal number from 100 to 199 or from 2000 to 2699.
- **terse** (Optional) Will not display debug information if the IS-IS IP Version 4 IS-IS local RIB has not changed.

**Command Default**
Debugging of IS-IS IP Version 4 routes is disabled.

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(26)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXE.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `debug isis rib` command to verify if an IP prefix has been installed or removed. To monitor updates from the IS-IS database to the IS-IS local RIB, use the `local` keyword, and to monitor updates from the IS-IS database to the global RIB, use the `global` keyword.

It is highly recommended that you limit the debugging output to information specific to the IP prefix that is associated with a specific access list by entering the `access-list-number` argument.

**Examples**

The following is sample output from the `debug isis rib` command after the `ip route priority high` command was used to give high priority to IS-IS IP prefixes for the configured access list...
access-list1. The debug output shows that the route 10.1.1.0/24 has been removed from the IS-IS local RIB.

Router# show running-config include access-list 1
access-list 1 permit 10.1.1.0 0.0.0.255
! access-list 1 is configured
Router# debug isis rib local terse 1
00:07:07: ISIS-LR: 10.1.1.0/24 aged out in LSP[10/(7->8)].
! The route 10.1.1.0/24 is removed from the IS-IS local RIB LSP[10/(7->8)].
00:07:07: ISIS-LR: rem path: [115/80/20] via 10.2.2.2(Et2) from 10.22.22.22 tg 0 LSP[10/7] from active chain (add to deleted chain)
! The remote path [115/80/20] is removed from the active chain.
00:07:07: ISIS-LR: Enqueued to updateQ[2] for 10.1.1.0/24
! Q[2] is marked to be the update.
00:07:07: ISIS-LR: rem path: [115/80/20] via 10.2.2.2(Et2) from 10.22.22.22 tg 0 LSP[10/7] from deleted chain
00:07:07: ISIS-LR: Rem RT 10.1.1.0/24
! The remote route [115/80/20] is removed from the deleted chain.

The table below describes the significant fields shown in the display.

Table 93: debug isis rib Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISIS-LR</td>
<td>IS-IS local route debugger.</td>
</tr>
<tr>
<td>10.1.1.0/24</td>
<td>IP prefix.</td>
</tr>
<tr>
<td>rem path:</td>
<td>Indicates the removal or insertion of a routing path—in this instance, it is a removal.</td>
</tr>
<tr>
<td>[115/80/20]</td>
<td>Administrative instance/type/metric for the routing path that has been removed or inserted.</td>
</tr>
<tr>
<td>via 10.2.2.2(Et2)</td>
<td>IP address of the next hop of the router, in this instance, Ethernet2.</td>
</tr>
<tr>
<td>from 10.22.22.22</td>
<td>IP address to advertise the route path.</td>
</tr>
<tr>
<td>tg 0</td>
<td>Priority of the IP prefix. All prefixes have a tag 0 priority unless otherwise configured.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip route priority high</td>
<td>Assigns a high priority to an IS-IS IP prefix.</td>
</tr>
<tr>
<td>show isis rib</td>
<td>Displays paths for routes in the IP Version 4 IS-IS local RIB.</td>
</tr>
</tbody>
</table>
debug isis rib redistribution

To debug the events that update the Intermediate System-to-Intermediate System (IS-IS) redistribution cache, use the `debug isis rib redistribution` command in privileged EXEC mode. To turn off debugging, use the `no` form of this command.

```
debug isis rib redistribution [{level-1 | level-2}] [access-list]
no debug isis rib redistribution [{level-1 | level-2}] [access-list]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>(Optional) Displays debug information for level 1 redistribution cache.</td>
</tr>
<tr>
<td>level-2</td>
<td>(Optional) Displays debug information for level 2 redistribution cache.</td>
</tr>
<tr>
<td>access-list</td>
<td>(Optional) An access list number from 1 to 199 or from 1300 to 2699.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(27)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(7)T.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXE.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

We recommend that you use this command only when a Cisco Technical Assistance Center representative requests you to do so to gather information for a troubleshooting purpose.

**Examples**

In the following example, the `debug isis rib redistribution` command is used to display information about events that update the IS-IS redistribution cache. The output is self-explanatory.

```
Router# debug isis rib redistribution level-1 123
IS-IS IPv4 redistribution RIB debugging is on for access list 123 for L1
Router# router isis
Router(config-router)# redistribute connected level-1
Router(config)# access-list 123 permit ip 10.0.0.0 0.255.255.255 any
Router(config)# interface Loopback123
Router(config-if)# ip address 10.123.123.3 255.255.255.255
Nov 25 00:33:46.532: ISIS-RR: 10.123.123.3/32: Up event, from 0x6D7CA60
Nov 25 00:33:46.532: ISIS-RR: looking at L1 redist RIB
Nov 25 00:33:46.532: ISIS-RR: redistributed to ISIS
Nov 25 00:33:46.532: ISIS-RR: added 10.123.123.3/32 to L1 redist RIB: [Connected/0] tag 0 external
Nov 25 00:33:47.532: ISIS-RR: Scanning L1 redist RIB
Nov 25 00:33:47.532: ISIS-RR: adv 10.123.123.3/32 as L1 redist route
Nov 25 00:33:47.532: ISIS-RR: End of scanningL1 redist RIB
```
The following line indicates that the connected route 10.123.123.3/32 was added to the IS-IS level 1 local redistribution cache with cost 0, metric type external, and administrative tag of 0:

Nov 25 00:33:47.532: ISIS-RR: added 10.123.123.3/32 to L1 redist RIB: [Connected/0] tag 0 external

The following line indicates that the redistributed route 10.123.123.3/32 was advertised in an IS-IS link-state packet (LSP) as a level 1 redistributed route:

Nov 25 00:33:47.532: ISIS-RR: adv 10.123.123.3/32 as L1 redist rout

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear isis rib redistribution</td>
<td>Clears some or all prefixes in the local redistribution cache.</td>
</tr>
<tr>
<td>show isis rib redistribution</td>
<td>Displays the prefixes in the IS-IS redistribution cache.</td>
</tr>
</tbody>
</table>
debug isis spf statistics

To display statistical information about building routes between intermediate systems (ISs), use the `debug isis spf statistics` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
default router# debug isis spf statistics
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

The Intermediate System-to-Intermediate System (IS-IS) Interdomain Routing Protocol (IDRP) provides routing between ISs by flooding the network with link-state information. IS-IS provides routing at two levels, intra-area (Level 1) and intra-domain (Level 2). Level 1 routing allows Level 1 ISs to communicate with other Level 1 ISs in the same area. Level 2 routing allows Level 2 ISs to build an interdomain backbone between Level 1 areas by traversing only Level 2 ISs. Level 1 ISs only need to know the path to the nearest Level 2 IS in order to take advantage of the interdomain backbone created by the Level 2 ISs.

The IS-IS protocol uses the shortest-path first (SPF) routing algorithm to build Level 1 and Level 2 routes. The `debug isis spf statistics` command provides information for determining the time required to place a Level 1 IS or Level 2 IS on the shortest path tree (SPT) using the IS-IS protocol.

**Note**

The SPF algorithm is also called the Dijkstra algorithm, after the creator of the algorithm.

**Examples**

The following is sample output from the `debug isis spf statistics` command:

```
default router# debug isis spf statistics
ISIS-Stats: Compute L1 SPT, Timestamp 2780.328 seconds
ISIS-Stats: Complete L1 SPT, Compute time 0.004, 1 nodes on SPT
ISIS-Stats: Compute L2 SPT, Timestamp 2780.3336 seconds
ISIS-Stats: Complete L2 SPT, Compute time 0.056, 12 nodes on SPT
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute L1 SPT</td>
<td>Indicates that Level 1 ISs are to be added to a Level 1 area.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Indicates the time at which the SPF algorithm was applied. The time is expressed as the number of seconds elapsed since the system was up and configured.</td>
</tr>
<tr>
<td>Complete L1 SPT</td>
<td>Indicates that the algorithm has completed for Level 1 routing.</td>
</tr>
<tr>
<td>Compute time</td>
<td>Indicates the time required to place the ISs on the SPT.</td>
</tr>
</tbody>
</table>
The following lines show the statistical information available for Level 1 ISs:

ISIS-Stats: Compute L1 SPT, Timestamp 2780.328 seconds
ISIS-Stats: Complete L1 SPT, Compute time 0.004, 1 nodes on SPT

The output indicates that the SPF algorithm was applied 2780.328 seconds after the system was up and configured. Given the existing intra-area topology, 4 milliseconds were required to place one Level 1 IS on the SPT.

The following lines show the statistical information available for Level 2 ISs:

ISIS-Stats: Compute L2 SPT, Timestamp 2780.3336 seconds
ISIS-Stats: Complete L2 SPT, Compute time 0.056, 12 nodes on SPT

This output indicates that the SPF algorithm was applied 2780.3336 seconds after the system was up and configured. Given the existing intradomain topology, 56 milliseconds were required to place 12 Level 2 ISs on the SPT.
debug isis spf-events

To display a log of significant events during an Intermediate System-to-Intermediate System (IS-IS) shortest-path first (SPF) computation, use the `debug isis spf-events` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debbug isis spf-events
no debug isis spf-events
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>Support for IPv6 was added.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>Support for IPv6 was added.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>Support for IPv6 was added.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.6</td>
<td>This command was introduced on Cisco ASR 1000 series routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays information about significant events that occur during SPF-related processing.

**Examples**

The following example displays significant events during an IS-IS SPF computation:

```
Router# debug isis spf-events
ISIS-Spf: Compute L2 IPv6 SPT
ISIS-Spf: Move 0000.0000.1111.00-00 to PATHS, metric 0
ISIS-Spf: Add 0000.0000.2222.01-00 to TENT, metric 10
ISIS-Spf: Move 0000.0000.2222.01-00 to PATHS, metric 10
ISIS-Spf: considering adj to 0000.0000.2222 (Ethernet3/1) metric 10, level 2, circuit 3, adj 3
ISIS-Spf:   (accepted)
ISIS-Spf: Add 0000.0000.2222.00-00 to TENT, metric 10
ISIS-Spf:   Next hop 0000.0000.2222 (Ethernet3/1)
ISIS-Spf: Move 0000.0000.2222.00-00 to PATHS, metric 10
ISIS-Spf: Add 0000.0000.2222.02-00 to TENT, metric 20
ISIS-Spf:   Next hop 0000.0000.2222 (Ethernet3/1)
ISIS-Spf: Move 0000.0000.2222.02-00 to PATHS, metric 20
ISIS-Spf: Add 0000.0000.3333.00-00 to TENT, metric 20
ISIS-Spf:   Next hop 0000.0000.3333 (Ethernet3/1)
ISIS-Spf: Move 0000.0000.3333.00-00 to PATHS, metric 20
```
**debug isis update-packets**

To display various sequence number protocol data units (PDUs) and link-state packets that are detected by a router, use the `debug isis update-packets` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
deploy isis update packets
no deploy isis update packets
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Examples**

This router has been configured for IS-IS routing. The following is sample output from the `debug isis update-packets` command:

```
Router# debug isis update-packets
ISIS-Update: Sending L1 CSNP on Ethernet0
ISIS-Update: Sending L2 CSNP on Ethernet0
ISIS-Update: Sending L2 CSNP on Tunnel0
ISIS-Update: Delete link 888.8800.0181.00 from L2 LSP 1600.8906.4022.00-00, seq E
ISIS-Update: Sending L1 LSP
ISIS-Update: Sending L1 CSNP on Ethernet0
ISIS-Update: Sending L2 CSNP on Ethernet0
ISIS-Update: Add link 888.8800.0181.00 to L2 LSP 1600.8906.4022.00-00, new seq 10, len 91
ISIS-Update: Sending L2 LSP 1600.8906.4022.00-00, seq 10, ht 1198 on Tunnel0
ISIS-Update: Sending L2 CSNP on Tunnel0
ISIS-Update: Sending L2 CSNP on Tunnel1
ISIS-Update: Updating L1 LSP
ISIS-Update: Rate limiting L1 LSP 1600.8906.4022.00-00, seq 11 (Tunnel0)
ISIS-Update: Sending L1 LSP
ISIS-Update: Rec L2 LSP 888.8800.0181.00.00-00 (Tunnel0)
ISIS-Update: PSNP entry 1600.8906.4022.00-00, seq 10, ht 1196
```

The following lines indicate that the router has sent a periodic Level 1 and Level 2 complete sequence number PDU on Ethernet interface 0:

```
ISIS-Update: Sending L1 CSNP on Ethernet0
ISIS-Update: Sending L2 CSNP on Ethernet0
```

The following lines indicate that the network service access point (NSAP) identified as 8888.8800.0181.00 was deleted from the Level 2 LSP 1600.8906.4022.00-00. The sequence number associated with this LSP is 0xE.

```
ISIS-Update: Updating L2 LSP
ISIS-Update: Delete link 888.8800.0181.00 from L2 LSP 1600.8906.4022.00-00, seq E
```

The following lines indicate that the NSAP identified as 8888.8800.0181.00 was added to the Level 2 LSP 1600.8906.4022.00-00. The new sequence number associated with this LSP is 0x10.

```
ISIS-Update: Updating L1 LSP
ISIS-Update: Sending L1 CSNP on Ethernet0
ISIS-Update: Sending L2 CSNP on Ethernet0
```
ISIS-Update: Add link 8888.8800.0181.00 to L2 LSP 1600.8906.4022.00-00, new seq 10, len 91

The following line indicates that the router sent Level 2 LSP 1600.8906.4022.00-00 with sequence number 0x10 on tunnel 0 interface:

ISIS-Update: Sending L2 LSP 1600.8906.4022.00-00, seq 10, ht 1198 on Tunnel0

The following lines indicates that a Level 2 LSP could not be transmitted because it was recently sent:

ISIS-Update: Sending L2 CSNP on Tunnel0
ISIS-Update: Updating L2 LSP
ISIS-Update: Rate limiting L2 LSP 1600.8906.4022.00-00, seq 11 (Tunnel0)

The following lines indicate that a Level 2 partial sequence number PDU (PSNP) has been received on tunnel 0 interface:

ISIS-Update: Updating L1 LSP
ISIS-Update: Rec L2 PSNP from 8888.8800.0181.00 (Tunnel0)

The following line indicates that a Level 2 PSNP with an entry for Level 2 LSP 1600.8906.4022.00-00 has been received. This output is an acknowledgment that a previously sent LSP was received without an error.

ISIS-Update: PSNP entry 1600.8906.4022.00-00, seq 10, ht 1196
debug iua as

To display debugging messages for the ISDN User Adaptation Layer (IUA) application server (AS), use the `debug iua as` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug iua as {user | state} {all | name as-name}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>Displays information about the use of application programming interfaces (APIs) and events between the ISDN layer and IUA.</td>
</tr>
<tr>
<td>state</td>
<td>Displays information about AS state transitions.</td>
</tr>
<tr>
<td>all</td>
<td>Enables debug for all the configured ASs.</td>
</tr>
<tr>
<td>name as-name</td>
<td>Defines the name of the AS.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows debugging output when an ISDN backhaul connection is initially established. The output shows that state debugging is turned on for all ASs and that the AS is active.

```
Router# debug iua as state all
IUA :state debug turned ON for ALL AS
00:11:52:IUA:AS as1 number of ASPs up is 1
00:11:57:IUA:AS as1 xsition AS-Up --> AS-Active, cause - ASP as1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug iua asp</td>
<td>Displays debugging messages for the IUA ASP.</td>
</tr>
</tbody>
</table>
debug iua asp

To display debugging messages for the IDSN User Adaptation Layer (IUA) application server process (ASP), use the `debug iua asp` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debbug iua asp {pak | peer-msg | sctp-sig | state} {all | name asp-name}
no debug iua asp
```

### Syntax Description

- **pak**
  - Displays information about all packets.
- **peer-msg**
  - Displays information about IUA peer-to-peer messages.
- **sctp-sig**
  - Displays information about the signals being sent by the Stream Control Transmission Protocol (SCTP) layer.
- **state**
  - Displays information about ASP state transition.
- **all**
  - Enables debugging output for all configured ASPs.
- **name asp-name**
  - Defines the name of the ASP.

### Command Default

No default behavior or values

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows debugging output when an ISDN backhaul connection is initially established. The output shows that peer message debugging is turned on for all ASPs and that the ASP is active.

```
Router# debug iua asp peer-msg all
IUA: peer message debug turned ON for ALL ASPs
00:04:58:IUA: received ASP_UP message on ASP asp1
00:04:58:IUA:ASP asp1 xsitIon ASP-Down -- ASP-Up, cause - rcv peer msg
ASP-UP
00:04:58:IUA: sending ACK of type 0x304 to asp asp1
00:05:03:IUA:recv ASP_ACTIVE message for ASP asp1
00:05:03:IUA:ASP asp1 xsitIon ASP-Up -- ASP-Active, cause - rcv peer msg
ASP-Active
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug iua as</code></td>
<td>Displays debugging messages for the IUA AS.</td>
</tr>
</tbody>
</table>
debug kerberos

To display information associated with the Kerberos Authentication Subsystem, use the `debug kerberos` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug kerberos
no debug kerberos
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

Kerberos is a security system that authenticates users and services without passing a cleartext password over the network. Cisco supports Kerberos under the authentication, authorization, and accounting (AAA) security system.

Use the `debug aaa authentication` command to get a high-level view of login activity. When Kerberos is used on the router, you can use the `debug kerberos` command for more detailed debugging information.

**Examples**

The following is part of the sample output from the `debug aaa authentication` command for a Kerberos login attempt that failed. The information indicates that Kerberos is the authentication method used.

```
Router# debug aaa authentication
AAA/AUTHEN/START (116852612): Method=KRB5
AAA/AUTHEN (116852612): status = GETUSER
AAA/AUTHEN/CONT (116852612): continue_login
AAA/AUTHEN (116852612): Method=KRB5
AAA/AUTHEN (116852612): status = GETPASS
AAA/AUTHEN/CONT (116852612): continue_login
AAA/AUTHEN (116852612): Method=KRB5
AAA/AUTHEN (116852612): status = GETPASS
AAA/AUTHEN (116852612): password incorrect
AAA/AUTHEN (116852612): status = FAIL
```

The following is sample output from the `debug kerberos` command for a login attempt that was successful. The information indicates that the router sent a request to the key distribution center (KDC) and received a valid credential.

```
Router# debug kerberos
Kerberos: Requesting TGT with expiration date of 820911631
Kerberos: Sent TGT request to KDC
Kerberos: Received TGT reply from KDC
Kerberos: Received valid credential with endtime of 820911631
```

The following is sample output from the `debug kerberos` command for a login attempt that failed. The information indicates that the router sent a request to the KDC and received a reply, but the reply did not contain a valid credential.

```
Router# debug kerberos
Kerberos: Requesting TGT with expiration date of 820911731
Kerberos: Sent TGT request to KDC
```
Kerberos: Received TGT reply from KDC
Kerberos: Received invalid credential.
AAA/AUTHEN (425003829): password incorrect

The following output shows other failure messages you might see that indicate a configuration problem. The first message indicates that the router failed to find the default Kerberos realm, therefore the process failed to build a message to send to the KDC. The second message indicates that the router failed to retrieve its own IP address. The third message indicates that the router failed to retrieve the current time. The fourth message indicates the router failed to find or create a credentials cache for a user, which is usually caused by low memory availability.

Router# debug kerberos
Kerberos: authentication failed when parsing name
Kerberos: authentication failed while getting my address
Kerberos: authentication failed while getting time of day
Kerberos: authentication failed while allocating credentials cache

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug aaa authentication</td>
<td>Displays information on accountable events as they occur.</td>
</tr>
</tbody>
</table>
debug kpml

To enable Keypad Markup Language (KPML) parser and builder debugs, use the `debug kpml` command to specify the debug option.

To disable KPML parser and builder debugs, use the `no` form of this command (you must enter one option).

```
dump kpml [{all | parser | builder | error}]
nodump kpml [{all | parser | builder | error}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enables all kpml debug tracing.</td>
</tr>
<tr>
<td>parser</td>
<td>Enables kpml parser tracing.</td>
</tr>
<tr>
<td>builder</td>
<td>Enables kpml builder tracing.</td>
</tr>
<tr>
<td>error</td>
<td>Enables kpml error tracing.</td>
</tr>
</tbody>
</table>

### Command Default

`no debug kpml all`

### Command Modes

Privileged EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

For incoming dial peers if you configure multiple DTMF negotiation methods, the first configure value takes precedence, then the second, then the third.

For incoming dial peers, the first out-of-band negotiation method takes precedence over other DTMF negotiation methods, except when rtp-nte has precedence; in this case, sip-kpml takes precedence over other out-of-band negotiation methods.

For incoming dial peers, if both sip-kpml and rtp-nte notification mechanisms are enabled and negotiated, the gateway relies on RFC 2833 notification to receive digits and a SUBSCRIBE for KPML is not initiated.

SIP KPML support complies to the IETF draft “draft-ietf-sIPPING-kpml-04.txt” with the following limitations:

- The SIP gateway always initiates SUBSCRIBE in the context of an established INVITE dialog. The gateway supports receiving SUBSCRIBE in the context of an established INVITE dialog, as well as out-of-call context requests with a leg parameter in the Event header. If the request code does not match an existing INVITE dialog, the gateway sends a NOTIFY with KPML status-code 481 and sets Subscription-State to terminated.

- The gateway does not support the Globally Routable User Agent (GRUU) requirement. The Contact header in the INVITE/200 OK message generates locally from the gateway’s contact information.

- The gateway always initiates persistent subscriptions, but it receives and processes persistent and one-shot subscriptions.
• The gateway supports only single-digit reporting. There is no need for inter-digit timer support. The only regular expressions supported are those which match to a single digit. For example:
  - `<regex>x</regex>` -- Matches to any digit 0 through 9
  - `<regex>1</regex>` -- Matches digit 1
  - `<regex>[x#*ABCD]</regex>` -- Matches to any digit 0 through 9, # (the pound sign), * (an asterisk), or A, B, C, or D
  - `<regex>[24]</regex>` -- Matches digits 2 or 4
  - `<regex>[2-9]</regex>` -- Matches any digit 2 through 9
  - `<regex>^[2-9]$</regex>` -- Matches digits 0 or 1

• The gateway does not support long key presses. Long key presses are detected and reported as a single digit press.

• Digit suppression is not supported (pre tag for suppressing inband digits).

• Individual stream selection is not supported. A SUBSCRIBE request for KPML applies to all audio streams in the dialog (stream element and reverse not supported).

You can configure support only on a SIP VoIP dial peer.

**Examples**

The following is output from the `debug kpml` command:

```
SIP call is established. DTMF sip-kpml was negotiated.
...
//-1/xxxxxxxxxxxxx/KPML/Parser/kpml_init:
//-1/xxxxxxxxxxxxx/KPML/Builder/kpml_encode: encode_data=0x64E25B48
//-1/xxxxxxxxxxxxx/KPML/Builder/kpml_encode_context_create: chunk_size=2k, max_allowed=16k
//-1/xxxxxxxxxxxxx/KPML/Builder/kpml_encode_context_create: context=0x6488C0AC, mp=0x6488B89C
//-1/xxxxxxxxxxxxx/KPML/Builder/kpml_build_request:
//-1/xxxxxxxxxxxxx/KPML/Builder/kpml_build_pattern:
//-1/xxxxxxxxxxxxx/KPML/Builder/kpml_build_regex_list:
//-1/xxxxxxxxxxxxx/KPML/Builder/kpml_build_regex_list:
//-1/xxxxxxxxxxxxx/KPML/Builder/kpml_build_request: length=289, buffp=0x645E9251
//-1/xxxxxxxxxxxxx/KPML/Builder/kpml_build_request: length=289, buffp=0x645E9251
.Safe: SUBSCRIBE sip:8888@172.18.193.250:5060 SIP/2.0
Via: SIP/2.0/UDP 172.18.193.251:5060;branch=z9hG4bKFF36
From: <sip:172.18.193.251>;tag=EA330-F6
To: <sip:8888@172.18.193.250>;tag=39497C-2EA
Call-ID: 57633F68-2BE011D6-8013D46B-B4F9B5F6@172.18.193.251
CSeq: 103 SUBSCRIBE
Max-Forwards: 70
Date: Fri, 01 Mar 2002 00:16:15 GMT
User-Agent: Cisco-SIPGateway/IOS-12.x
Event: kpml
Expires: 7200
Contact: <sip:172.18.193.251:5060>
```
Content-Type: application/kpml-request+xml
Content-Length: 327
<?xml version="1.0" encoding="UTF-8"?>
<kpml-request xmlns="urn:ietf:params:xml:ns:kpml-request"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:kpml-request kpml-request.xsd"
version="1.0">  
<pattern persist="persist"><regex tag="dtmf">[x*#ABCD]</regex></pattern>
</kpml-request>

SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.18.193.251:5060;branch=z9hG4bKFF36
From: <sip:8888@172.18.193.250>;tag=39497C-2EA
To: <sip:172.18.193.251>;tag=EA330-F6
Call-ID: 57633F68-2BE011DE-8015D46B-B4F9B5F6@172.18.193.251
CSeq: 101 SUBSCRIBE
Max-Forwards: 70
Date: Fri, 01 Mar 2002 01:02:51 GMT
User-Agent: Cisco-SIPGateway/IOS-12.x
Event: kpml
Expires: 7200
Contact: <sip:172.18.193.250:5060>
Content-Type: application/kpml-request+xml
Content-Length: 327
<?xml version="1.0" encoding="UTF-8"?>
<kpml-request xmlns="urn:ietf:params:xml:ns:kpml-request"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:kpml-request kpml-request.xsd"
version="1.0">  
<pattern persist="persist"><regex tag="dtmf">[x*#ABCD]</regex></pattern>
</kpml-request>

Cisco IOS Debug Command Reference - Commands I through L
570
CSeq: 103 SUBSCRIBE
Content-Length: 0
Expires: 7200
Via: SIP/2.0/UDP 172.18.193.250:5060;branch=z9hG4bK5FE3
From: <sip:8888@172.18.193.250>;tag=39497C-2EA
To: <sip:172.18.193.251>;tag=EA330-F6
Date: Fri, 01 Mar 2002 00:16:24 GMT
Call-ID: 57633F68-2BE011D6-8013D46B-B4F9B5F6@172.18.193.251
CSeq: 101 SUBSCRIBE
Content-Length: 0
Contact: <sip:172.18.193.250:5060>
Expires: 7200
Via: SIP/2.0/UDP 172.18.193.251:5060;branch=z9hG4bK101EA4
From: <sip:172.18.193.251>;tag=EA330-F6
To: <sip:8888@172.18.193.250>;tag=39497C-2EA
Date: Fri, 01 Mar 2002 00:16:24 GMT
Call-ID: 57633F68-2BE011D6-8013D46B-B4F9B5F6@172.18.193.251
CSeq: 102 NOTIFY
Max-Forwards: 70
Date: Fri, 01 Mar 2002 00:16:24 GMT
User-Agent: Cisco-SIPGateway/IOS-12.x
Event: kpml
Subscription-State: active
Contact: <sip:172.18.193.251:5060>
Content-Length: 0
Expires: 7200
Via: SIP/2.0/UDP 172.18.193.251:5060;branch=z9hG4bK6111
From: <sip:172.18.193.251>;tag=EA330-F6
To: <sip:8888@172.18.193.250>;tag=39497C-2EA
Date: Fri, 01 Mar 2002 01:02:51 GMT
User-Agent: Cisco-SIPGateway/IOS-12.x
Event: kpml
Subscription-State: active
Contact: <sip:172.18.193.250:5060>
Content-Length: 0
Max-Forwards: 70
Date: Fri, 01 Mar 2002 01:02:51 GMT
User-Agent: Cisco-SIPGateway/IOS-12.x
Event: kpml
Subscription-State: active
Contact: <sip:172.18.193.250:5060>
Content-Length: 0
...
Call-ID: 57633F68-2BE011D6-8013D46B-B4F9B5F6@172.18.193.251
CSeq: 105 NOTIFY
Max-Forwards: 70
Date: Fri, 01 Mar 2002 00:37:33 GMT
User-Agent: Cisco-SIPGateway/IOS-12.x
Event: kpml
Subscription-State: active
Contact: <sip:172.18.193.251:5060>
Content-Type: application/kpml-response+xml
Content-Length: 113
<?xml version="1.0" encoding="UTF-8"?>
<kpml-response version="1.0" code="200" text="OK" digits="1" tag="dtmf"/>

Sent:
NOTIFY sip:172.18.193.250:5060 SIP/2.0
Via: SIP/2.0/UDP 172.18.193.251:5060;branch=z9hG4bK1117DE
From: <sip:172.18.193.251>;tag=EA330-F6
To: <sip:8888@172.18.193.250>;tag=39497C-2EA
Date: Fri, 01 Mar 2002 01:24:08 GMT
Call-ID: 57633F68-2BE011D6-8013D46B-B4F9B5F6@172.18.193.251
CSeq: 105 NOTIFY
Content-Length: 0
<?xml version="1.0" encoding="UTF-8"?>
<kpml-response version="1.0" code="200" text="OK" digits="2" tag="dtmf"/>

Sent:
NOTIFY sip:172.18.193.250:5060 SIP/2.0
Via: SIP/2.0/UDP 172.18.193.251:5060;branch=z9hG4bK12339
From: <sip:172.18.193.251>;tag=EA330-F6
To: <sip:8888@172.18.193.250>;tag=39497C-2EA
Date: Fri, 01 Mar 2002 00:37:44 GMT
Call-ID: 57633F68-2BE011D6-8013D46B-B4F9B5F6@172.18.193.251
CSeq: 106 NOTIFY
Max-Forwards: 70
Date: Fri, 01 Mar 2002 00:37:44 GMT
User-Agent: Cisco-SIPGateway/IOS-12.x
Event: kpml
Subscription-State: active
Contact: <sip:172.18.193.251:5060>
Content-Type: application/kpml-response+xml
Content-Length: 113
<?xml version="1.0" encoding="UTF-8"?>
<kpml-response version="1.0" code="200" text="OK" digits="3" tag="dtmf"/>

Received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.18.193.251:5060;branch=z9hG4bK1117DE
From: <sip:172.18.193.251>;tag=EA330-F6
To: <sip:8888@172.18.193.250>;tag=39497C-2EA
Date: Fri, 01 Mar 2002 00:37:33 GMT
Call-ID: 57633F68-2BE011D6-8013D46B-B4F9B5F6@172.18.193.251
CSeq: 105 NOTIFY
Content-Length: 113
<?xml version="1.0" encoding="UTF-8"?>
<kpml-response version="1.0" code="200" text="OK" digits="2" tag="dtmf"/>
SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.18.193.251:5060;branch=z9hG4bK12339
From: <sip:172.18.193.251>;tag=EA330-F6
To: <sip:8888@172.18.193.250>;tag=39497C-2EA
Date: Fri, 01 Mar 2002 01:24:20 GMT
Call-ID: 57633F68-2BE011D6-8013D46B-B4F9B5F6@172.18.193.251
CSeq: 106 NOTIFY
Content-Length: 0

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show sip-ua calls</td>
<td>Verifies that the DTMF method is SIP-KPML.</td>
</tr>
</tbody>
</table>
debug kron

To display debugging messages about Command Scheduler policies or occurrences, use the debug kron command in privileged EXEC mode. To disable debugging output, use the no form of this command.

```
debug kron {all | exec-cli | info | major}
no debug kron {all | exec-cli | info | major}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>Displays all debugging output about Command Scheduler policy lists or occurrences.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exec-cli</td>
<td>Displays detailed debugging output about Command Scheduler policy list command-line interface (CLI) commands.</td>
</tr>
<tr>
<td></td>
<td>info</td>
<td>Displays debugging output about Command Scheduler policy lists, occurrence warnings, or progress information.</td>
</tr>
<tr>
<td></td>
<td>major</td>
<td>Displays debugging output about Command Scheduler policy list or occurrence failures.</td>
</tr>
</tbody>
</table>

**Command Default**

If no keyword is specified, all debugging messages are displayed.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(1)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the debug kron command to display the output of a scheduled EXEC show command on the console.

**Examples**

The following example shows debugging messages for the EXEC CLI show version after the CLI was run at a scheduled interval:

```
Router# debug kron exec-cli
Kron cli occurrence messages debugging is on
2w6d: Call parse_cmd 'show version'
2w6d: Kron CLI return 0
**CLI 'show version':
Cisco Internetwork Operating System Software IOS (tm) C2600 Software (C2600-I-M
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show kron schedule</strong></td>
<td>Displays the status and schedule information for Command Scheduler occurrences.</td>
</tr>
</tbody>
</table>
debug l2ctrl

To enable debugging for Layer 2 Control (L2CTRL), use the `debug l2ctrl` command in privileged EXEC mode. To disable debugging for L2CTRL, use the `no` form of this command.

```plaintext
debug l2ctrl {all | evc | pm | registry}
no debug l2ctrl {all | evc | pm | registry}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>Displays all L2CTRL debugging messages.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>evc</td>
<td>Displays Ethernet virtual circuit (EVC) and L2CTRL messages.</td>
</tr>
<tr>
<td></td>
<td>pm</td>
<td>Displays switch PM and L2CTRL messages.</td>
</tr>
<tr>
<td></td>
<td>registry</td>
<td>Displays L2CTRL registries.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRD</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable debugging of all L2CTRL related events:

```plaintext
Router# debug l2ctrl all
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ethernet l2ctrl</td>
<td>Enables Ethernet L2CTRL debugging messages.</td>
</tr>
</tbody>
</table>
debug l2fib

To enable the logging of Layer 2 Forwarding Information Base (L2FIB) debug messages, use the `debug l2fib` command in privileged EXEC mode. To disable the debugging, use the `no` form of this command.

```
ddebug l2fib {addr [unicast | multicast] | all | bridge-domain [port] | event | error | ha | l2port | mlrib | olist | otv tunnel [decap | encap]}
no debug l2fib {addr [unicast | multicast] | all | bridge-domain [port] | event | error | ha | l2port | mlrib | olist | otv tunnel [decap | encap]}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>addr</code></td>
<td>Enables logging of unicast or multicast object-specific debug messages.</td>
</tr>
<tr>
<td><code>unicast</code></td>
<td>(Optional) Enables logging of unicast object-specific debug messages.</td>
</tr>
<tr>
<td><code>multicast</code></td>
<td>(Optional) Enables logging of multicast object-specific debug messages.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Enables logging of all L2FIB debug messages.</td>
</tr>
<tr>
<td><code>bridge-domain</code></td>
<td>Enables logging of bridge-domain object-specific debug messages.</td>
</tr>
<tr>
<td><code>port</code></td>
<td>Enables logging of bridge-domain port object-specific debug messages.</td>
</tr>
<tr>
<td><code>event</code></td>
<td>Enables logging of event debug messages.</td>
</tr>
<tr>
<td><code>error</code></td>
<td>Enables logging of the error debug messages.</td>
</tr>
<tr>
<td><code>ha</code></td>
<td>Enables logging of high availability (HA) events.</td>
</tr>
<tr>
<td><code>l2port</code></td>
<td>Enables logging of Layer 2 port object-specific debug messages.</td>
</tr>
<tr>
<td><code>mlrib</code></td>
<td>Enables logging of Multilayer Routing Information Base (MLRIB) interactions.</td>
</tr>
<tr>
<td><code>olist</code></td>
<td>Enables logging of output list object-specific debug messages.</td>
</tr>
<tr>
<td><code>otv tunnel</code></td>
<td>Enables logging of Overlay Transport Virtualization (OTV) tunnel object-specific debug messages.</td>
</tr>
<tr>
<td><code>decap</code></td>
<td>Enables logging of OTV tunnel decap object-specific debug messages.</td>
</tr>
<tr>
<td><code>encap</code></td>
<td>Enables logging of OTV tunnel encap object-specific debug messages.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.5S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug l2fib all` command:

```
Router# debug l2fib all
```
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show l2fib</td>
<td>Displays information about L2FIB.</td>
</tr>
</tbody>
</table>
**debug l2relay events**

To start debugging of Layer 2 Relay events, use the `debug l2relay events` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command (SGSN D-node only).

```
deploy l2relay events
no debug l2relay events
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(1)GA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(3)T</td>
<td>This command was integrated into Cisco IOS Release 12.1(3)T.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The SGSN module uses the proprietary Layer 2 Relay protocol in conjunction with the intra-Serving GPRS Support Node (iSGSN) protocol for communication between the SGSN-datacom (SGSN-D) and SGSN-telecom (SGSN-T) units that comprise the SGSN.

For debugging purposes, it might also be useful to trace Layer 2 Relay packets. To display information about Layer 2 Relay packets, use the `debug l2relay packets` command.

Normally you will not need to use the `debug l2relay events` or `debug l2relay packets` commands. If problems with the SGSN are encountered, Cisco technical support personnel may request that issue the command.

**Caution**

Because the `debug l2relay events` command generates a substantial amount of output, use it only when traffic on the GPRS network is low, so other activity on the system is not adversely affected.

**Examples**

The following example enables the display of Layer 2 Relay events:

```
Router# debug l2relay events
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug l2relay packets</code></td>
<td>Displays Layer 2 Relay packets (SGSN D-node only).</td>
</tr>
</tbody>
</table>
**debug l2relay packets**

To display information about Layer 2 Relay packets, use the `debug l2relay packets` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command (SGSN D-node only).

```plaintext
debug l2relay packets
no debug l2relay packets
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.1(1)GA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td></td>
<td>12.1(3)T</td>
<td>This command was integrated into Cisco IOS Release 12.1(3)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug l2relay packets` command to display information about Layer 2 Relay packets.

The SGSN module uses the proprietary Layer 2 Relay protocol in conjunction with the intra-Serving GPRS Support Node (iSGSN) protocol for communication between the SGSN-datacom (SGSN-D) and SGSN-telecom (SGSN-T) units that comprise the SGSN.

For debugging purposes, it might also be useful to trace Layer 2 Relay events. To display information about Layer 2 Relay events, use the `debug l2relay events` command.

Normally you will not need to use the `debug l2relay packets` or `debug l2relay events` command. If problems with the SGSN are encountered, Cisco technical support personnel may request that you issue the command.

⚠️ **Caution**

Because the `debug l2relay packets` command generates a significant amount of output, use it only when traffic on the GPRS network is low, so other activity on the system is not adversely affected.

**Examples**

The following example enables the display of Layer 2 Relay packets:

```plaintext
Router# debug l2relay packets
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip igmp</td>
<td>Displays Layer 2 Relay events (SGSN D-node only).</td>
</tr>
</tbody>
</table>
**debug l2tp**

To enable debugging of Layer 2 Tunneling Protocol (L2TP) information, use the `debug l2tp` command in privileged EXEC mode. To disable L2TP debugging, use the `no` form of this command.

```
debug l2tp {all | application | brief | db {error | event | lookup} | error | event | export | l2tun | packet {brief | detail | error | event} | route | seq {brief | snmp | timer}}
no debug l2tp {all | application | brief | db {error | event | lookup} | error | event | export | l2tun | packet {brief | detail | error | event} | route | seq {brief | snmp | timer}}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enables the most commonly used L2TP debugs.</td>
</tr>
<tr>
<td>application</td>
<td>Enables L2TP application information debugs.</td>
</tr>
<tr>
<td>brief</td>
<td>Enables L2TP debug information in a single line.</td>
</tr>
<tr>
<td>db</td>
<td>Enables L2TP database debugs.</td>
</tr>
<tr>
<td>error</td>
<td>Enables L2TP error debugs.</td>
</tr>
<tr>
<td>event</td>
<td>Enables L2TP event debugs.</td>
</tr>
<tr>
<td>lookup</td>
<td>Enables L2TP database lookup.</td>
</tr>
<tr>
<td>export</td>
<td>Enables L2TP external data and command-line interface (CLI) debugs.</td>
</tr>
<tr>
<td>l2tun</td>
<td>Enables Layer 2 tunnel (L2Tun) socket application programming interface (API) debugs.</td>
</tr>
<tr>
<td>packet</td>
<td>Enables L2TP packet information debugs.</td>
</tr>
<tr>
<td>detail</td>
<td>Enables L2TP packet dump details debugs.</td>
</tr>
<tr>
<td>route</td>
<td>Enables L2TP route watch debugs.</td>
</tr>
<tr>
<td>seq</td>
<td>Enables extra sequencing debugs.</td>
</tr>
<tr>
<td>brief</td>
<td>(Optional) Enables L2TP one-line sequencing debugs.</td>
</tr>
<tr>
<td>snmp</td>
<td>Enables L2TP Simple Network Management Protocol (SNMP) event debugs.</td>
</tr>
<tr>
<td>timer</td>
<td>Enables L2TP timer debugs.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRB.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB.</td>
</tr>
</tbody>
</table>
Modification
This command was modified. The **application** and **brief** keywords were added.

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was modified. The <strong>application</strong> and <strong>brief</strong> keywords were added.</td>
</tr>
<tr>
<td>15.0(1)S</td>
<td>This command was modified. The <strong>snmp</strong> and <strong>route</strong> keywords were added.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the `debug l2tp` command to troubleshoot L2TP operations.

Examples

The following example shows how to enable L2TP debugging:

```
Router> enable
Router# debug l2tp all
L2TP most commonly used debugs debugging is on
Router# debug l2tp application
L2TP application debugs debugging is on
Router# debug l2tp brief
L2TP brief, one line debugs debugging is on
Router# debug l2tp db lookup
L2TP database lookups debugging is on
Router# debug l2tp error
L2TP errors debugging is on
Router# debug l2tp seq
L2TP sequencing debugging is on
Router# debug l2tp snmp
L2TP SNMP events debugging is on
```

The following sample output of the `show debugging` command displays the debugs enabled for L2TP. The field descriptions are self-explanatory.

```
Router# show debugging

L2TP:
  L2TP packet events debugging is on
  L2TP packet errors debugging is on
  L2TP packet detail debugging is on
  L2TP errors debugging is on
  L2TP events debugging is on
  L2TP L2TUN socket API debugging is on
  L2TP sequencing debugging is on
  L2TP export data to applications and cli debugging is on
  L2TP route watch debugging is on
  L2TP timers debugging is on
  L2TP brief, one line debugs debugging is on
  L2TP application debugs debugging is on
  L2TP database lookups debugging is on
  L2TP SNMP events debugging is on
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show debugging</td>
<td>Displays information about the types of debugging that are enabled for your router.</td>
</tr>
</tbody>
</table>
debug l2tp redundancy

To enable the display of information on Layer 2 Tunneling Protocol (L2TP) sessions that contain redundancy status, use the `debug l2tp redundancy` command in user or privileged EXEC mode. To disable this debugging, use the `no` form of this command.

```
default l2tp redundancy  { cf | detail | error | event | fsm | resync | rf }
no default l2tp redundancy
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cf</code></td>
<td>Displays L2TP redundancy-facility (cf) events.</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>Displays L2TP redundancy details.</td>
</tr>
<tr>
<td><code>error</code></td>
<td>Displays L2TP redundancy errors.</td>
</tr>
<tr>
<td><code>event</code></td>
<td>Displays L2TP redundancy events.</td>
</tr>
<tr>
<td><code>fsm</code></td>
<td>Displays L2TP redundancy forwarding-service manager (fsm) events.</td>
</tr>
<tr>
<td><code>resync</code></td>
<td>Displays L2TP redundancy resynchronizations.</td>
</tr>
<tr>
<td><code>rf</code></td>
<td>Displays L2TP redundancy-facility (rf) events.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>)
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.2</td>
<td>This command was introduced in Cisco IOS XE Release 2.2.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `debug l2tp redundancy` command in privileged EXEC mode to display a list of redundancy events and errors.

Use the `show l2tp redundancy` command in privileged EXEC mode to display information on the state of the Layer 2 Tunneling Protocol (L2TP) or a specific L2TP session redundancy data.

**Examples**

The following example shows how to display a debug of redundancy events during the setup and termination of an L2TP High Availability (HA) tunnel for a L2TP Network Server (LNS) active Route Processor (RP):

```
LNS1> debug enable
LNS1# debug l2tp redundancy cf
L2TP redundancy cf debugging is on
LNS1# debug l2tp redundancy
```
debug ipv6 inspect through debug local-ack state
debug l2tp redundancy

detail
L2TP redundancy details debugging is on
LNS1# debug
l2tp
redundancy
error
L2TP redundancy errors debugging is on
LNS1# debug
l2tp
redundancy
event
L2TP redundancy events debugging is on
LNS1# debug
l2tp
redundancy
fsm
L2TP redundancy fsm debugging is on
LNS1# debug
l2tp
redundancy
resync
L2TP redundancy resync debugging is on
LNS1# debug
l2tp
redundancy
rf
L2TP redundancy rf debugging is on
LNS1#
*Aug 26 18:00:00.467: %SYS-5-CONFIG_I: Configured from console by console
LNS1#
*Aug 26 18:00:45.631: L2TP tnl
01000:________: CCM initialized CCM session
*Aug 26 18:00:45.631: : L2TP HA:CC playback chkpt skipped, CC not doing HA
*Aug 26 18:00:45.711: : L2TP HA FSM:Receive proto FSM event 19
*Aug 26 18:00:45.711: : L2TP HA FSM:Receive RxSCCRQ
*Aug 26 18:00:45.711: : L2TP HA:lcm_cc alloc: l2tp_cc 070B45B8, lcm_cc 02FE55E8
*Aug 26 18:00:45.711: : L2TP HA FSM:FSM-CC ev Rx-SCCRQ
*Aug 26 18:00:45.711: : L2TP HA FSM:FSM-CC
Idle->Wt-ChkptSidRmt
*Aug 26 18:00:45.711: : L2TP HA FSM:FSM-CC do Block-Tx-AckSCCRQ
*Aug 26 18:00:45.711: : L2TP HA FSM:Checkpoint Two Cc IDs
*Aug 26 18:00:45.711: L2TP HA CF: Chkpt send: s/c id 0/52631, BothCcId, seq 0, ns/nr 0/0,
rid 51583, len 52; flush = 1, ctr 1
*Aug 26 18:00:45.711: 01000:0000CD97: L2TP HA:Enqueue peer Ns 0 to ns_q, seq 1 (q sz 0)
*Aug 26 18:00:45.711: L2TP tnl
01000:0000CD97: Encoding SCCRQ-IN CHKPT
*Aug 26 18:00:45.711: L2TP tnl
01000:0000CD97: Tx CHKPT
*Aug 26 18:00:45.739: L2TP tnl
01000:0000CD97: Encoding SCCRP-OUT CHKPT
*Aug 26 18:00:45.739: L2TP tnl
01000:0000CD97: Tx CHKPT
*Aug 26 18:00:45.739: : L2TP HA:Adjust local window size to 10
*Aug 26 18:00:45.739: 01000:0000CD97: L2TP HA FSM:Receive proto TxCM event SCCRP
*Aug 26 18:00:45.739: : L2TP HA FSM:Receive TxSCCRP
LNS1#
*Aug 26 18:00:45.739: : L2TP HA FSM:FSM-CC ev Tx-SCCRP
*Aug 26 18:00:45.739: : L2TP HA FSM:FSM-CC
Wt-ChkptSidRmt->WtCcIdRmt2
*Aug 26 18:00:45.739: : L2TP HA FSM:FSM-CC do Block-Tx-SCCRP
*Aug 26 18:00:45.739: 01000:0000CD97: L2TP HA FSM:Found blocked RxSCCRQ, seq_num 1
*Aug 26 18:00:45.739: 01000:0000CD97: L2TP HA FSM:Queued SCCRP to CC hold_q
*Aug 26 18:00:46.863: : L2TP HA FSM:CHKPT status callback: status 0, len 56
*Aug 26 18:00:46.863: : L2TP HA FSM:Context s/c id 0/52631, BothCcId, seq 1, ns/nr 0/0, rid
51583, len 52
*Aug 26 18:00:46.863: L2TP HA CF: Rcvd status s/c id 0/52631, BothCcId, seq 1, ns/nr 0/0,
rid 51583, len 52
*Aug 26 18:00:46.863: L2TP HA CF: Rcvd status 0: len 56
*Aug 26 18:00:46.863: L2TP HA CF: Status content s/c id 0/52631, BothCcId, seq 1, ns/nr
0/0, rid 51583, len 52

Cisco IOS Debug Command Reference - Commands I through L
584


Aug 26 18:00:46.863: 01000:0000CD97: L2TP HA FSM:Receive chkpt ack: s/c id 0/52631, BothCcId, seq 1, ns/nr 0/0, rid 51583, len 52
Aug 26 18:00:46.863: 01000:0000CD97: L2TP HA FSM:Receive CC-ChkptAck
Aug 26 18:00:46.863: 01000:0000CD97: L2TP HA FSM:CC send all unblocked if can LNS1#
Aug 26 18:00:46.863: 01000:0000CD97: L2TP HA:Ns entry to remove: found (current Ns 1)
Aug 26 18:00:46.863: 01000:0000CD97: L2TP HA:Advance peer Nr to 1 (ns_q sz 0)
Aug 26 18:00:48.095: L2TP HA CF: Chkpt send: s/c id 14072/52631, BothSesId, seq 0, ns/nr 2/1, rid 40276, len 52; flush = 1, ctr 3
Aug 26 18:00:48.095: L2TP HA CF: Enqueue peer Nr 2 to ns_q, seq 3 (q sz 0)
Aug 26 18:00:48.131: L2TP HA: Try to buffer sock msg type 19
Aug 26 18:00:48.131: L2TP HA: Buffering skipped
Aug 26 18:00:48.131: L2TP HA: Try to buffer sock msg type 23
Aug 26 18:00:48.131: CC not in resync state, buffering skipped
Aug 26 18:00:49.115: L2TP HA FSM: Check for Ns/Nr update 2, peer 1
Aug 26 18:00:49.115: L2TP HA FSM: Receive peer Ns/Nr update (2,2/1,1, int 3, rx 1, 3) (ns_q sz 1)
Aug 26 18:00:49.211: L2TP HA FSM: CHKPT status callback: status 0, len 56
Aug 26 18:00:49.211: Context s/c id 0/52631, CcUp, seq 2, ns/nr 1/1, rid 0, len 52
Aug 26 18:00:49.211: L2TP HA FSM: CHKPT status callback: status 0, len 56
Aug 26 18:00:49.211: Context s/c id 14072/52631, BothSesId, seq 3, ns/nr 1/2, rid 40276, len 52
Aug 26 18:00:49.211: L2TP HA CF: Rcvd status s/c id 0/52631, CcUp, seq 2, ns/nr 1/1, rid 0, len 52
Aug 26 18:00:49.211: L2TP HA CF: Rcvd status 0: len 56
Aug 26 18:00:49.211: L2TP HA CF: Status content s/c id 0/52631, CcUp, seq 2, ns/nr 1/1, rid 0, len 52
Aug 26 18:00:49.211: L2TP HA CF: Status content s/c id 14072/52631, BothSesId, seq 3, ns/nr 1/2, rid 40276, len 52
Aug 26 18:00:49.211: L2TP HA CB: Rcvd status 0: len 56
Aug 26 18:00:49.211: L2TP HA CF: Status content s/c id 14072/52631, BothSesId, seq 3, ns/nr 1/2, rid 40276, len 52
Aug 26 18:00:49.211: L2TP HA CF: Status content s/c id 14072/52631, BothSesId, seq 3, ns/nr 1/2, rid 40276, len 52
Aug 26 18:00:49.211: L2TP HA CF: Status content s/c id 14072/52631, BothSesId, seq 3, ns/nr 1/2, rid 40276, len 52
Aug 26 18:00:49.211: L2TP HA: Try to remove from CC's ns_q: seq num 3 (current Ns 3)
Aug 26 18:00:49.211: L2TP HA: NS entry to remove: found (current Ns 3)
Aug 26 18:00:49.211: L2TP HA: Advance peer Nr to 3 (ns_q sz 0)
Aug 26 18:00:49.211: L2TP HA: Session send all unblocked
Aug 26 18:00:49.211: L2TP HA: CC send if can (ICRP): ns 1 (1, 1), nr 3 (3)
Aug 26 18:00:49.211: L2TP HA CF: 0 ICRP 51583/40276 ns/nr 1/3
Aug 26 18:00:49.211: L2TP HA: Try to remove from CC's ns_q: seq num 3 (current Ns 3)
Aug 26 18:00:49.211: L2TP HA: NS entry to remove: found (current Ns 3)
Aug 26 18:00:49.211: L2TP HA: Advance peer Nr to 3 (ns_q sz 0)
Proceed with clearing all tunnels? [confirm]
Aug 26 18:01:21.271: 01000:0000CD97: L2TP HA FSM:Queued STOPCCN to cc hold_q
Aug 26 18:01:22.423: : L2TP HA FSM:CHKPT status callback: status 0, len 56
Aug 26 18:01:22.423: : L2TP HA FSM:Context s/c id 0/52631, CcDwn, seq 5, ns/nr 2/3, rid 0, len 52
Aug 26 18:01:22.423: : L2TP HA CF: Rcvd status s/c id 0/52631, CcDwn, seq 5, ns/nr 2/3, rid 0, len 52
Aug 26 18:01:22.423: : L2TP HA CF: Status content s/c id 0/52631, CcDwn, seq 5, ns/nr 2/3, rid 0, len 52
Aug 26 18:01:22.423: : L2TP HA FSM:Recv chkpt ack: s/c id 0/52631, CcDwn, seq 5, ns/nr 2/3, rid 0, len 52
Aug 26 18:01:22.423: : L2TP HA:Try to remove from CC's ns_q: seq num 5 (current Ns 4)
Aug 26 18:01:22.423: : L2TP HA:Ns entry to remove: not found (current Ns 4)
Aug 26 18:01:22.423: : L2TP HA:CC send all unblocked if can
Aug 26 18:01:22.423: : L2TP HA:CC send one blocked CM (SCCRP): ns 2 (2), nr 4
Aug 26 18:01:22.451: : L2TP HA:CC ns_q cleanup: overall head Ns old/new = 4/4 (Q sz 0)
Aug 26 18:01:22.451: : L2TP HA FSM:Check for Ns/Nr update 4, peer 3
Aug 26 18:01:22.451: : L2TP HA FSM:Receive peer Ns/Nr update (4,3/3, int 4, rx 3, 4) (ns_q sz 0)
Aug 26 18:01:22.451: : L2TP HA:CC destruction after Tx/Rx StopCCN LNS1#
Table 95: debug l2tp redundancy Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cf</td>
<td>Number of L2TP checkpointing-facility events (cf-events).</td>
</tr>
<tr>
<td>error</td>
<td>Number of L2TP checkpointing errors.</td>
</tr>
<tr>
<td>event</td>
<td>Number of L2TP checkpointing events.</td>
</tr>
<tr>
<td>fsm</td>
<td>Number of L2TP checkpointing fsm events.</td>
</tr>
<tr>
<td>resync</td>
<td>Number of L2TP checkpointing resynchronized events.</td>
</tr>
<tr>
<td>rf</td>
<td>Number of L2TP checkpointing redundancy-facility events (rf-events).</td>
</tr>
</tbody>
</table>

The table below describes the significant fields shown in the `debug l2tp redundancy` command output.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug vpdn redundancy</td>
<td>Displays information about VPDN sessions that have redundancy events and errors.</td>
</tr>
<tr>
<td>l2tp sso enable</td>
<td>Enables L2TP HA.</td>
</tr>
<tr>
<td>l2tp tunnel resync</td>
<td>Specifies the number of packets sent before waiting for an acknowledgment message.</td>
</tr>
<tr>
<td>show l2tp redundancy</td>
<td>Displays L2TP sessions containing redundancy data.</td>
</tr>
<tr>
<td>show vpdn redundancy</td>
<td>Displays VPDN sessions containing redundancy data.</td>
</tr>
<tr>
<td>sso enable</td>
<td>Enables L2TP HA session for VPDN groups.</td>
</tr>
</tbody>
</table>
debug l2vpn acircuit

To debug errors and events that occur on the Layer 2 VPN (L2VPN) attachment circuits (the circuits between the provider edge [PE] and customer edge [CE] devices), use the `debug l2vpn acircuit` command in privileged EXEC mode. To disable debugging, use the `no` form of this command.

```
debug l2vpn acircuit {error | event | event-trace number [{preserve}]}
no debug l2vpn acircuit {error | event | event-trace number [{preserve}]}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Displays errors that occur in attachment circuits.</td>
</tr>
<tr>
<td>event</td>
<td>Displays events that occur in attachment circuits.</td>
</tr>
<tr>
<td>event-trace</td>
<td>Displays event trace logs.</td>
</tr>
<tr>
<td>number</td>
<td>Number of event trace logs to be stored per context.</td>
</tr>
<tr>
<td>preserve</td>
<td>Specifies that the event trace logs should not be removed.</td>
</tr>
</tbody>
</table>

### Command Modes

- **Privileged EXEC (#)**

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the <code>debug acircuit</code> command in future releases.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated in Cisco IOS Release 15.3(1)S.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `debug l2vpn acircuit` command to identify provisioning events, setup failures, circuit up and down events, and configuration failures on attachment circuits.

An attachment circuit connects a PE device to a CE device. A device can have many attachment circuits. The attachment circuit manager controls all attachment circuits from one central location. Therefore, when you enable debug messages for an attachment circuit, you receive information about all attachment circuits.

### Examples

The following is sample output from the `debug acircuit event` command when an interface is enabled:

```
Device# debug l2vpn acircuit event

*Jan 28 15:19:03.070: ACLIB: ac_cstate() Handling circuit UP for interface Se2/0
*Jan 28 15:19:03.070: ACLIB [10.0.1.1, 200]: pthru_intf_handle_circuit_up() calling acmgr_circuit_up
*Jan 28 15:19:03.070: ACLIB [10.0.1.1, 200]: Setting new AC state to Ac-Connecting
*Jan 28 15:19:03.070: ACMGR: Receive <Circuit Up> msg
*Jan 28 15:19:03.070: Se2/0 ACMGR: circuit up event, SIP state chg down to connecting, action is service request
*Jan 28 15:19:03.070: Se2/0 ACMGR: Sent a sip service request
*Jan 28 15:19:03.070: ACLIB [10.0.1.1, 200]: AC updating switch context.
*Jan 28 15:19:03.070: Se2/0 ACMGR: Rcv SIP msg: resp connect forwarded, hdl 9500001D, l2ss_hdl 700001E
*Jan 28 15:19:03.070: Se2/0 ACMGR: service connected event, SIP state chg connecting to
```
connected, action is respond forwarded
*Jan 28 15:19:03.070: ACLIB: pthru_intf_response hdl is 9500001D, response is 1
*Jan 28 15:19:03.070: ACLIB [10.0.1.1, 200]: Setting new AC state to Ac-Connected

The following is sample output from the **debug l2vpn acircuit event** command when an interface is disabled:

Device# debug l2vpn acircuit event

*Jan 28 15:25:57.014: ACLIB: SW AC interface INTF-DOWN for interface Se2/0
*Jan 28 15:25:57.014: ACLIB [10.0.1.1, 200]: Setting new AC state to Ac-Idle
*Jan 28 15:25:57.014: Se2/0 ACMGR: Receive <Circuit Down> msg
*Jan 28 15:25:57.014: Se2/0 ACMGR: circuit down event, SIP state chg connected to end, action is service disconnect
*Jan 28 15:25:57.014: Se2/0 ACMGR: Sent a sip service disconnect
*Jan 28 15:25:59.014: %LINK-5-CHANGED: Interface Serial2/0, changed state to administratively down
*Jan 28 15:25:59.014: ACLIB: ac_cstate() Handling circuit DOWN for interface Se2/0
*Jan 28 15:26:00.014:%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down

The following example shows output from the **debug l2vpn acircuit** command for an xconnect session on a GigabitEthernet interface:

Device# debug l2vpn acircuit

23:28:35: ACLIB [10.0.3.201, 5]: SW AC interface UP for GigabitEthernet interface GE2/1/1
23:28:35: ACLIB [10.0.3.201, 5]: pthru_intf_handle_circuit_up() calling acmgr_circuit_up
23:28:35: ACLIB [10.0.3.201, 5]: Setting new AC state to Ac-Connecting
23:28:35: ACLIB [10.0.3.201, 5]: SW AC interface UP for GigabitEthernet interface GE2/1/1
23:28:35: ACLIB [10.0.3.201, 5]: pthru_intf_handle_circuit_up() ignoring up event. Already connected or connecting.
23:28:35: ACMGR: Receive <Circuit Up> msg
23:28:35: GE2/1/1 ACMGR: circuit up event, SIP state chg down to connecting, action is service request
23:28:35: GE2/1/1 ACMGR: Sent a sip service request
23:28:37: %LINK-3-UPDOWN: Interface GigabitEthernet2/1/1, changed state to up
23:28:38: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/1/1, changed state to up
23:28:53: GE2/1/1 ACMGR: Rcv SIP msg: resp connect forwarded, hdl D6000002, sss_hdl 9E00000F
23:28:53: GE2/1/1 ACMGR: service connected event, SIP state chg connecting to connected, action is respond forwarded
23:28:53: ACLIB: pthru_intf_response hdl is D6000002, response is 1
23:28:53: ACLIB [10.0.3.201, 5]: Setting new AC state to Ac-Connected

The command output is self-explanatory.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug acircuit</td>
<td>Debugs errors and events that occur on the attachment circuits.</td>
</tr>
<tr>
<td>debug vpdn</td>
<td>Debugs errors and events relating to L2TP configuration and the surrounding Layer 2 tunneling infrastructure.</td>
</tr>
<tr>
<td>debug xconnect</td>
<td>Debugs errors and events related to an xconnect configuration.</td>
</tr>
</tbody>
</table>
**debug l2vpn atom checkpoint**

To enable the debugging of Any Transport over MPLS (AToM) events when AToM is configured for nonstop forwarding/stateful switchover (NSF/SSO) and graceful restart, use the `debug l2vpn atom checkpoint` command in privileged EXEC mode. To disable the debugging of these messages, use the `no` form of this command.

```
debuge l2vpn atom checkpoint
no debug l2vpn atom checkpoint
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Debugging of the AToM NSF/SSO and graceful restart is disabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command will replace the <code>debug mpls l2transport checkpoint</code> command in future releases.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated in Cisco IOS Release 15.3(1)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Debug commands use a significant amount of CPU time and can affect system performance.

**Examples**

In the following example, the output shows that NSF/SSO and graceful restart synchronize the data between the active and backup Route Processors (RP) after an AToM virtual circuit (VC) is created. (Both `debug l2vpn atom checkpoint` and `debug l2vpn acircuit checkpoint` commands are enabled in this example.)

The `debug l2vpn atom checkpoint` command is enabled on the active RP:

```
Device# debug l2vpn atom checkpoint
Device# debug l2vpn acircuit checkpoint
```

**Example Output**

AToM HA:
AToM checkpointing events and errors debugging is on
AC HA:
Attachment Circuit Checkpoint debugging is on

AToM HA [10.55.5.2, 1002]: Build provision msg, SSM sw/seg 8192/8194 [0x2000/0x2002] PW id 9216 [0x2400] local label 21
AToM HA: CF sync send complete
AC HA CF: Sync send complete. Code:0

On the standby RP, the following messages indicate that it receives checkpointing data:

```
AC HA [10.55.5.2, 1002]: Add to WaitQ. Flags:1
AToM HA [105.55.5.2, 1002]: Received 32-byte provision version 1 CF message
```
During a switchover from the active to the backup RP, the following debug messages are displayed:

```
%HA-5-MODE: Operating mode is hsa, configured mode is sso.
AC HA RF: CId:83, Seq:710, Sta:RF_STATUS_OPER_REDUNDANCY_MODE_CHANGE, Opr:5, St:STANDBY HOT, PSt:ACTIVE
AToM HA: CID 84, Seq 715, Status RF_STATUS_OPER_REDUNDANCY_MODE_CHANGE, Op 5, State STANDBY HOT, Peer ACTIVE
AC HA RF: CId:83, Seq:710, Sta:RF_STATUS_PEER_PRESENCE, Opr:0, St:STANDBY HOT, PSt:DISABLED
AToM HA: CID 84, Seq 715, Status RF_STATUS_PEER_PRESENCE, Op 0, State STANDBY HOT, Peer DISABLED
%HA-2-CUTOVER_NOTICE: Cutover initiated. Cease all console activity until system restarts.
%HA-2-CUTOVER_NOTICE: Do not add/remove RSPs or line cards until switchover completes.
%HA-2-CUTOVER_NOTICE: Deinitializing subsystems...
%OIR-6-REMCARD: Card removed from slot 4, interfaces disabled
%OIR-6-REMCARD: Card removed from slot 5, interfaces disabled
%OIR-6-REMCARD: Card removed from slot 9, interfaces disabled
%HA-2-CUTOVER_NOTICE: Reinitializing subsystems...
%HA-2-CUTOVER_NOTICE: System preparing to restart...
%HA-5-NOTICE: Resuming initialization...
AC HA RF: CId:83, Seq:710, Sta:RF_STATUS_REDUNDANCY_MODE_CHANGE, Opr:7, St:STANDBY HOT, PSt:DISABLED
.
.
.
%LDP-5-GR: LDP restarting gracefully. Preserving forwarding state for 250 seconds.
AC HA RF: CId:83, Seq:710, Sta:RF_PROG_ACTIVE, Opr:0, St:ACTIVE, PSt:DISABLED
AToM HA: CID 84, Seq 715, Event RF_PROG_ACTIVE, Op 0, State ACTIVE, Peer DISABLED
AC HA: Switchover: Standby->Active
AC HA RF: Reconciling
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>debug l2vpn acircuit checkpoint</strong></td>
<td>Enables the debugging of AToM attachment circuit events when AToM is configured for NSF/SSO and graceful restart.</td>
</tr>
<tr>
<td><strong>debug mpls l2transport checkpoint</strong></td>
<td>Enables the debugging of AToM events when AToM is configured for NSF/SSO and graceful restart.</td>
</tr>
</tbody>
</table>
**debug l2vpn atom event-trace**

To enable debugging of event trace information for Layer 2 VPN (L2VPN) Any Transport over MPLS (AToM), use the `debug l2vpn atom event-trace` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug l2vpn atom {event-trace number [{preserve}]}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Number of event trace logs to be stored per context.</td>
</tr>
<tr>
<td><code>preserve</code></td>
<td>(Optional) Specifies that the event trace logs should not be removed.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the <code>debug mpls l2transport event-trace</code> command in future releases.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated in Cisco IOS Release 15.3(1)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug l2vpn atom event-trace` command does not produce any output of its own. Instead, it affects the size of the event-trace buffer for Any Transport over MPLS (AToM) events.

**Examples**

The following is sample output from the `debug l2vpn atom event-trace` command:

```
Device# debug l2vpn atom event-trace
AToM LDP event-trace debugging is on
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug mpls l2transport event-trace</code></td>
<td>Enables debugging of event trace information for MPLS Layer 2 transport events.</td>
</tr>
</tbody>
</table>
debug l2vpn atom fast-failure-detect

To enable the debugging of Layer 2 VPN (L2VPN) Any Transport over MPLS (AToM) fast failure detection, use the `debug l2vpn atom fast-failure-detect` command in privileged EXEC mode. To disable the debugging, use the `no` form of this command.

```
display l2vpn atom fast-failure-detect
no display l2vpn atom fast-failure-detect
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Debugging of L2VPN fast failure detection is disabled.

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the <code>debug mpls l2transport fast-failure-detect</code> command in future releases.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated in Cisco IOS Release 15.3(1)S.</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to enable L2VPN AToM fast failure detection:

```
Device# debug l2vpn atom fast-failure-detect
--------- Line Card (Slot 3) ---------
AToM fast failure detect debugging is on
00:03:28: AToM FFD[10.1.1.2]: Sending type: BFD, adjacency: DOWN, local: 10.1.1.1
00:03:28: AToM FFD[10.1.1.2]: ADJ_DOWN, local: 10.1.1.1
00:03:28: AToM FFD[10.1.1.2, 100]: ADJ_DOWN
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug mpls l2transport fast-failure-detection</code></td>
<td>Enables the debugging of fast failure detection.</td>
</tr>
</tbody>
</table>
**debug l2vpn atom signaling**

To enable debugging of Layer 2 VPN (L2VPN) Any Transport over MPLS (AToM) signaling protocol information, use the `debug l2vpn atom signaling` command in privileged EXEC mode. To disable debugging, use the `no` form of this command.

```
debug l2vpn atom signaling {event | message | fsm}
no debug l2vpn atom signaling {event | message | fsm}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>event</code></td>
<td>Enables debugging of protocol events.</td>
</tr>
<tr>
<td><code>message</code></td>
<td>Enables debugging of protocol messages.</td>
</tr>
<tr>
<td><code>fsm</code></td>
<td>Enables debugging of finite state machine (FSM).</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the <code>debug mpls l2transport signaling</code> command in future releases.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated in Cisco IOS Release 15.3(1)S.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug l2vpn atom signaling` command:

```
Device# debug l2vpn atom signaling event
AToM LDP event debugging is on

Device# debug l2vpn atom signaling message
AToM LDP message debugging is on

AToM:
  AToM LDP event debugging is on
  AToM LDP message debugging is on
  *Mar 24 23:10:55.611: AToM LDP [10.9.9.9]: Allocate LDP instance
  *Mar 24 23:10:55.611: AToM LDP [10.9.9.9]: Opening session, 1 clients
  *Mar 24 23:10:56.063: %SYS-5-CONFIG_I: Configured from console by console
  *Mar 24 23:10:56.583: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up
  *Mar 24 23:11:00.539: AToM LDP [10.9.9.9]: Session is up
  *Mar 24 23:11:00.539: AToM LDP [10.9.9.9]: Peer address change, add 10.1.1.100
  *Mar 24 23:11:00.539: AToM LDP [10.9.9.9]: Peer address change, add 10.1.1.6
  *Mar 24 23:11:00.539: AToM LDP [10.9.9.9]: Sending label mapping msg
    vc type 7, cbit 1, vc id 50, group id 6, vc label 21, status 0, mtu 1500
  *Mar 24 23:11:00.539: AToM LDP [10.9.9.9]: Received label mapping msg, id 113
    vc type 7, cbit 1, vc id 50, group id 6, vc label 21, status 0, mtu 1500
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>debug mpls l2transport signaling</code></td>
<td>Displays information about the AToM signaling protocol.</td>
</tr>
</tbody>
</table>
debug l2vpn atom static-oam

To enable the debugging of messages related to static operations administrative and management (OAM), use the `debug l2vpn atom static-oam` command in privileged EXEC mode. To disable the debugging of these messages, use the `no` form of this command.

```
debug l2vpn atom static-oam [elog | error | event | fsm]
no debug l2vpn atom static-oam [{elog | error | event | fsm}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>elog</code></td>
<td>Displays logging messages for static pseudowire OAM.</td>
</tr>
<tr>
<td><code>error</code></td>
<td>Displays error messages for static pseudowire OAM.</td>
</tr>
<tr>
<td><code>event</code></td>
<td>Displays event messages for static pseudowire OAM.</td>
</tr>
<tr>
<td><code>fsm</code></td>
<td>Displays finite state machine (FSM) messages for static pseudowire OAM.</td>
</tr>
</tbody>
</table>

### Command Default

Display of static pseudowire messages is not disabled.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command will replace the <code>debug mpls l2transport static-oam</code> command in future releases.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated in Cisco IOS Release 15.3(1)S.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `debug l2vpn atom static-oam error` does not produce any output of its own. Instead, it affects the size of the event-trace buffer for Any Transport over MPLS (AToM) events.

### Examples

The following example enables the display of error messages for static pseudowire OAM:

```
Device# debug l2vpn atom static-oam error
Static PW OAM events debugging is on
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug mpls l2transport static-oam</code></td>
<td>Enables the debugging of messages related to static pseudowire operations OAM.</td>
</tr>
<tr>
<td><code>show l2vpn atom static-oam</code></td>
<td>Displays the status of static pseudowires.</td>
</tr>
</tbody>
</table>
debug l2vpn atom vc

To enable debugging of status of the Layer 2 VPN (L2VPN) Any Transport over MPLS (AToM) virtual circuits (VCs), use the `debug l2vpn atom vc` command in privileged EXEC mode. To disable debugging, use the `no` form of this command.

```
deploy debug l2vpn atom vc {event | fsm | ldp | subscriber | status} {event | fsm}
no deploy mpls l2transport vc {event | fsm | ldp | subscriber | status} {event | fsm}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>event</code></td>
<td>Displays AToM event messages about VCs.</td>
</tr>
<tr>
<td><code>fsm</code></td>
<td>Displays debug information related to the finite state machine (FSM).</td>
</tr>
<tr>
<td><code>ldp</code></td>
<td>Displays debug information related to the Label Distribution Protocol (LDP).</td>
</tr>
<tr>
<td><code>subscriber</code></td>
<td>Displays debug information related to the L2VPN subscriber.</td>
</tr>
<tr>
<td><code>status</code></td>
<td>Displays debug information related to the status of VCs.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the <code>debug mpls l2transport vc</code> command in future releases.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated in Cisco IOS Release 15.3(1)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can issue this command from the line card or the Route Processor (RP).

**Examples**

The following is sample output from the `debug l2vpn atom vc event` and `debug l2vpn atom vc fsm` commands:

```
Device# debug l2vpn atom vc event
AToM vc event debugging is on

Device# debug l2vpn atom vc fsm
AToM vc fsm debugging is on

AToM:
    AToM vc event debugging is on
    AToM vc fsm debugging is on
  *Mar 24 23:17:24.371: AToM MGR [10.9.9.9, 50]: Event provision, state changed from idle to provisioned
  *Mar 24 23:17:24.371: AToM SMGR [10.9.9.9, 50]: Requesting VC create, vc_handle 61A09930
  *Mar 24 23:17:24.371: AToM MGR [10.9.9.9, 50]: Local up, state changed from provisioned to local standby
  *Mar 24 23:17:24.371: AToM MGR [10.9.9.9, 50]: Update local vc label binding
  *Mar 24 23:17:24.371: AToM MGR [10.9.9.9, 50]: Successfully processed create request
```
The following is sample output of MPLS pseudowire status signaling messages from the `debug l2vpn atom vc status event` and `debug l2vpn atom vc status fsm` commands:

```
Device# debug l2vpn atom vc status event
Device# debug l2vpn atom vc status fsm

*Feb 26 14:03:42.543: AToM MGR [10.9.9.9, 100]: Receive SSS STATUS(UP)
*Feb 26 14:03:42.543: AToM MGR [10.9.9.9, 100]: AC status UP
*Feb 26 14:03:42.543: AToM MGR [10.9.9.9, 100]: S:Evt local up, LndRru->LnuRru
*Feb 26 14:03:42.543: AToM MGR [10.9.9.9, 100]: S:Evt local ready, LnuRru->LruRru
*Feb 26 14:03:42.543: AToM MGR [10.9.9.9, 100]: S:Act send label(UP)
*Feb 26 14:03:42.543: AToM MGR [10.9.9.9, 100]: Send label(UP)
*Feb 26 14:03:42.543: AToM MGR [10.9.9.9, 100]: Local AC : UP
*Feb 26 14:03:42.543: AToM MGR [10.9.9.9, 100]: Dataplane: no fault
*Feb 26 14:03:42.543: AToM MGR [10.9.9.9, 100]: Overall : no fault
*Feb 26 14:03:42.543: AToM MGR [10.9.9.9, 100]: Remote label is ready
*Feb 26 14:03:42.543: AToM MGR [10.9.9.9, 100]: S:Evt remote ready in LruRru
*Feb 26 14:03:42.543: AToM MGR [10.9.9.9, 100]: S:Evt remote up in LruRru
*Feb 26 14:03:42.543: AToM MGR [10.9.9.9, 100]: S:Evt dataplane clear fault in LruRru
*Feb 26 14:03:42.551: AToM MGR [10.9.9.9, 100]: S:Evt dataplane clear fault in LruRru
```

The status codes in the messages, such as S and LruRru, indicate the status of the local and remote devices. The following is the list status codes displayed in the output:

- **L**—local router
- **R**—remote router
- **r** or **n**—ready (r) or not ready (n)
- **u** or **d**—up (u) or down (d) status

The output also includes the following values:

- **D**—Dataplane
- **S**—Local shutdown

The status codes in the messages, such as **S** and **LruRru**, indicate the status of the local and remote devices. The following is the list status codes displayed in the output:

- **L**—local router
- **R**—remote router
- **r** or **n**—ready (r) or not ready (n)
- **u** or **d**—up (u) or down (d) status

The output also includes the following values:

- **D**—Dataplane
- **S**—Local shutdown
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>debug mpls l2transport vc</strong></td>
<td>Enables debugging of the AToM VCs.</td>
</tr>
</tbody>
</table>
**debug l2vpn atom vc vccv**

To enable Layer 2 VPN (L2VPN) Any Transport over MPLS (AToM) Virtual Circuit Connection Verification (VCCV) debugging, use the `debug l2vpn atom vc vccv` command in privileged EXEC mode. To disable debugging, use the `no` form of this command.

```
default l2vpn atom vc vccv [bfd] event
no default l2vpn atom vc vccv [bfd] event
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bfd</td>
<td>(Optional) Displays event messages when Bidirectional Forwarding Detection (BFD) sessions are created, when BFD sends dataplane fault notifications to L2VPN, and when L2VPN sends the attachment circuit (AC) signaling status to BFD.</td>
</tr>
<tr>
<td>event</td>
<td>Displays AToM event messages about the VCCV.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the <code>debug mpls l2transport vc vccv</code> command in future releases.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated in Cisco IOS Release 15.3(1)S.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to enable L2VPN AToM VCCV events and AToM VCCV BFD events debugging.

### Examples

The following example shows how to enable MPLS L2VPN virtual circuit (VC) VCCV BFD event debugging:

```
Device# debug l2vpn atom vc vccv bfd event
AToM VCCV BFD events debugging is on
Aug 10 16:55:41.493: AToM VCCV BFD[10.1.1.2, 1234000]: .. cc_type 1
Aug 10 16:55:41.493: AToM VCCV BFD[10.1.1.2, 1234000]: .. CC control word enabled
Aug 10 16:55:42.315: AToM VCCV BFD[10.1.1.2, 1234000]: session 00000001 ADJ UP
Aug 10 16:55:42.315: AToM VCCV BFD[10.1.1.2, 1234000]: inform BFD, status UP, event 1
Aug 10 16:55:42.315: AToM VCCV BFD[10.1.1.2, 1234000]: Start VCCV BFD status timer
Aug 10 16:55:45.374: AToM VCCV BFD[10.1.1.2, 1234000]: VCCV BFD status timer expired
Aug 10 16:55:45.374: AToM VCCV BFD[10.1.1.2, 1234000]: session 00000001 BFD STATUS UP
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>debug mpls l2transport vc vccv</code></td>
<td>Enables AToM VCCV debugging</td>
</tr>
<tr>
<td></td>
<td><code>show mpls l2transport vc</code></td>
<td>Displays information about the status of the AToM VCs.</td>
</tr>
</tbody>
</table>
**debug l2vpn pseudowire**

To enable debugging information for Layer 2 VPN (L2VPN) pseudowire configuration, use the `debug l2vpn pseudowire` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug l2vpn pseudowire {event | error}
no debug l2vpn pseudowire {event | error}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>event</code></td>
<td>Displays debugging information for L2VPN pseudowire events.</td>
</tr>
<tr>
<td><code>error</code></td>
<td>Displays debugging information for L2VPN pseudowire errors.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated into Cisco IOS release 15.3(1)S.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `debug l2vpn pseudowire event` command:

```
Device# debug l2vpn pseudowire event
L2VPN pseudowire events debugging is on.

*Aug 10 17:52:25.851: Pseudowire[pw1]: Pseudowire interface: peer id 10.0.0.0 not configured
*Aug 10 17:52:25.851: Pseudowire[pw1]: Pseudowire interface config still incomplete, skip update to xconnect db
*Aug 10 17:52:33.727: Pseudowire[pw1]: Pseudowire interface not yet associated with a L2VPN service
```
**debug l2vpn vfi**

To enable debugging layer 2 VPN (L2VPN) virtual forwarding instance (VFI) events and errors, use the `debug l2vpn vfi` command in privileged EXEC mode. To disable debugging of VFI events and errors, use the `no` form of this command.

```
debug l2vpn vfi [{fsm}] {error | event}
no debug l2vpn vfi [{fsm}] {error | event}
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced. This command will replace the <code>debug vfi</code> command in future releases.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated in Cisco IOS Release 15.3(1)S.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug l2vpn vfi` command:

```
Device# debug l2vpn vfi
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug vfi</td>
<td>Enables debugging VFI events and errors.</td>
</tr>
</tbody>
</table>
**debug l2vpn xconnect**

To enable the debugging information about a Layer 2 VPN (L2VPN) xconnect configuration, use the `debug l2vpn xconnect` command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug l2vpn xconnect [error | event | initialization | internal | monitor]
no debug l2vpn xconnect [error | event | initialization | internal | monitor]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>Displays errors related to an xconnect configuration.</td>
</tr>
<tr>
<td>event</td>
<td>Displays events related to an xconnect configuration.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays the xconnect detailed debugging information.</td>
</tr>
<tr>
<td>initialization</td>
<td>Displays information about xconnect initialization events.</td>
</tr>
<tr>
<td>internal</td>
<td>Displays information about xconnect internal events.</td>
</tr>
<tr>
<td>monitor</td>
<td>Displays debugging information about xconnect peer monitoring debugs.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.7S</td>
<td>This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the <code>debug xconnect</code> command in future releases.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated in Cisco IOS Release 15.3(1)S.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `debug l2vpn xconnect` command for an xconnect session on a Gigabit Ethernet interface:

```
Device# debug l2vpn xconnect event
00:01:16: XC AUTH [Gi2/1/1, 5]: Event: start xconnect authorization, state changed from IDLE to AUTHORIZING
00:01:16: XC AUTH [Gi2/1/1, 5]: Event: found xconnect authorization, state changed from AUTHORIZING to DONE
00:01:16: XC AUTH [Gi2/1/1, 5]: Event: free xconnect authorization request, state changed from DONE to END
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug xconnect</td>
<td>Enables the debugging information for an xconnect configuration.</td>
</tr>
</tbody>
</table>
**debug l3-mgr tunnel**

To enable debugging for interface, tunnel, or VLAN events for the Layer 3 manager infrastructure on RP of Cisco 7600 routers, use the `debug l3-mgr tunnel` command. To disable the debugging, use the `no` form of the command.

```plaintext
debug l3-mgr tunnel

no debug l3-mgr tunnel
```

**Syntax Description**

- **l3-mgr** Displays debugging output for the Layer 3 manager infrastructure on Cisco 7600 routers.
- **tunnel** Displays all tunnel related reserved VLAN events.

**Command Default**
None

**Command Modes**
Privileged EXEC

**Command History**

- **Release Modification**
  - 15.3(2)S This command was introduced on Cisco 7600 series routers.

**Usage Guidelines**
Use the debug command only to troubleshoot specific problems, or during troubleshooting sessions with Cisco technical support staff.

**Example Debugging Output**

The following shows sample output for the `debug l3-mgr tunnel` command:

```plaintext
CE1#debug l3-mgr tunnel
l3 mgr tunnel debugging is on
*Mar 1 09:50:53.431 IST: l3mgr_tunnel_checking_src_address:
  Tunnel[Tunnel56] src[64003801] tbl_id[0] state changed to DOWN
*Mar 1 09:50:53.431 IST: l3mgr_tunnel_checking_src_address:
  Checked Tunnel[Tunnel110] src[64006E01] if_up[UP] tbl_id[0]
  Checked Tunnel[Tunnel1109] src[64006D01] if_up[UP] tbl_id[0]
*Mar 1 09:50:53.431 IST: l3mgr_tunnel_checking_src_address:
  Checked Tunnel[Tunnel109] src[64006C01] if_up[UP] tbl_id[0]
  Checked Tunnel[Tunnel108] src[64006B01] if_up[UP] tbl_id[0]
*Mar 1 09:50:53.431 IST: l3mgr_tunnel_checking_src_address:
  Checked Tunnel[Tunnel107] src[64006A01] if_up[UP] tbl_id[0]
  Checked Tunnel[Tunnel106] src[64006901] if_up[UP] tbl_id[0]
  Checked Tunnel[Tunnel105] src[64006801] if_up[UP] tbl_id[0]
  Checked Tunnel[Tunnel104] src[64006701] if_up[UP] tbl_id[0]
  Checked Tunnel[Tunnel103] src[64006601] if_up[UP] tbl_id[0]
  Checked Tunnel[Tunnel102] src[64006501] if_up[UP] tbl_id[0]
  Checked Tunnel[Tunnel101] src[64006401] if_up[UP] tbl_id[0]
```
*Mar 1 09:50:53.435 IST: l3mgr_tunnel_checking_src_address:
Checked Tunnel[Tunnel100] src[64006401] if_up[UP] tbl_id[0]
**debug l4f**

To enable troubleshooting for Layer 4 Forwarding (L4F) flows, use the **debug l4f** command in privileged EXEC mode. To disable the troubleshooting, use the **no** form of this command.

```
debug l4f {api | flow-db | flows | packet {all | detail | injection | interception | proxying | spoofing} | test-app | trace-db-api | trace-db-flow | trace-engine}
no debug l4f {api | flow-db | flows | packet {all | detail | injection | interception | proxying | spoofing} | test-app | trace-db-api | trace-db-flow | trace-engine}
```

**Syntax Description**

- `api` Toggles L4F API debugging.
- `flow-db` Toggles L4F flow database debugging.
- `flows` Toggles L4F flows debugging.
- `packet` Toggles L4F packet debugging.
- `all` Toggles all L4F packet debugging.
- `detail` Toggles L4F packet detail debugging.
- `injection` Toggles L4F packet injection debugging.
- `interception` Toggles L4F packet interception debugging.
- `proxying` Toggles L4F packet proxying debugging.
- `spoofing` Toggles L4F packet spoofing debugging.
- `test-app` Toggles L4F test application debugging.
- `trace-db-api` Toggles L4F database API debugging.
- `trace-db-flow` Toggles L4F database flow debugging.
- `trace-engine` Toggles L4F API tracing debugging.

**Command Default**

L4F debugging is off.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to enable debugging for Layer 4 forwarding flows.

**Examples**

The following example shows how to enable debugging for L4F packets:
debug 14f

Router# debug 14f packet all

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show 14f</td>
<td>Displays the flow database for L4F.</td>
</tr>
</tbody>
</table>
debug lACP

To enable debugging of all Link Aggregation Control Protocol (LACP) activity, use the **debug lACP** command in privileged EXEC mode. To disable LACP debugging, use the **no** form of this command.

```
debug lACP [{all | event | fsm | misc | multi-chassis [{all | database | lACP-mgr | redundancy-group | user-interface}] | packet}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>(Optional) Activates debugging for all LACP operations.</td>
</tr>
<tr>
<td>event</td>
<td>(Optional) Activates debugging of events that occur within LACP.</td>
</tr>
<tr>
<td>fsm</td>
<td>(Optional) Activates debugging for changes within the LACP finite state machine.</td>
</tr>
<tr>
<td>misc</td>
<td>(Optional) Activates debugging for various operations that may be useful for monitoring the status of LACP.</td>
</tr>
<tr>
<td>multi-chassis</td>
<td>(Optional) Activates multi-chassis LACP (mLACP) debugging.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) Activates all mLACP debugging.</td>
</tr>
<tr>
<td>database</td>
<td>(Optional) Activates mLACP database debugging.</td>
</tr>
<tr>
<td>lACP-mgr</td>
<td>(Optional) Activates mLACP interface debugging.</td>
</tr>
<tr>
<td>redundancy-group</td>
<td>(Optional) Activates mLACP interchassis redundancy group debugging.</td>
</tr>
<tr>
<td>user-interface</td>
<td>(Optional) Activates mLACP interchassis user interface debugging.</td>
</tr>
<tr>
<td>packet</td>
<td>(Optional) Displays the receiving and transmitting LACP control packets.</td>
</tr>
</tbody>
</table>

**Command Default**

LACP debugging activity is disabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(13)EW</td>
<td>Support for this command was introduced on the Cisco Catalyst 4500 series switch.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.4</td>
<td>This command was integrated into Cisco IOS XE Release 2.4.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was modified. The following keywords were added: <strong>multi-chassis</strong>, <strong>all</strong>, <strong>database</strong>, <strong>lACP-mgr</strong>, <strong>redundancy-group</strong>, and <strong>user-interface</strong>.</td>
</tr>
</tbody>
</table>
Usage Guidelines

This command is useful for troubleshooting problems with LACP.

Examples

The following sample output from the `debug lacp all` command shows LACP activity on a port-channel member link Gigabit Ethernet 5/0/0:

```
Router# debug lacp all
Link Aggregation Control Protocol all debugging is on
Router1#
*Aug 20 17:21:51.685: LACP: Act: tlv:1, tlv-len:20, key:0x1, p-pri:0x8000, p:0x14, p-state:0x3C, s-pri:0xFFFF, s-mac:0011.2026.7300
*Aug 20 17:21:51.685: LACP: Part: tlv:2, tlv-len:20, key:0x5, p-pri:0x8000, p:0x42, p-state:0x3D, s-pri:0x8000, s-mac:0014.a93d.4a00
*Aug 20 17:21:51.685: LACP: G15/0/0 LACP packet received, processing
*Aug 20 17:21:51.685: lacp_rx Gi5: during state CURRENT, got event 5(recv_lacpdu)
*Aug 20 17:21:51.685: LACP: LACP packet received, processing
*Aug 20 17:21:51.685: lacp_rx Gi5: during state SLOW_PERIODIC, got event 3(pt_expired)
*Aug 20 17:21:51.685: lacp_ptx Gi5: SLOW_PERIODIC -> PERIODIC_TX
*Aug 20 17:21:51.685: LACP: Gi5/0/0 oper-key: 0x0
*Aug 20 17:21:51.685: LACP: lacp_hw_on: Gi5/0/0 is coming up
*Aug 20 17:22:19.989: LACP: timer lacp_t(Gi5/0/0) started with interval 1000.
```

Cisco IOS Debug Command Reference - Commands I through L
*Aug 20 17:22:23.413: LACP: Gi5/0/0 lacp_action_ptx_no_periodic entered
*Aug 20 17:22:23.413: LACP: lacp_p(Gi5/0/0) timer stopped
*Aug 20 17:22:24.153: %LINK-3-UPDOWN: Interface GigabitEthernet5/0/0, changed state to up
*Aug 20 17:22:24.153: LACP: lacp_hw_on: Gi5/0/0 is coming up
*Aug 20 17:22:24.153: lacp_ptx Gi5: during state FAST_PERIODIC, got event 0(no_periodic)
*Aug 20 17:22:24.153: LACP: lacp_p(Gi5/0/0) timer stopped
*Aug 20 17:22:24.153: LACP:
*Aug 20 17:22:25.021: LACP: lacp_p(Gi5/0/0) timer stopped
*Aug 20 17:22:25.021: LACP: lacp_p(Gi5/0/0) expired
*Aug 20 17:22:25.021: LACP: Gi5/0/0 lacp_action_ptx_fast_periodic_exit entered
*Aug 20 17:22:25.021: LACP: lacp_p(Gi5/0/0) timer stopped
*Aug 20 17:22:25.021: LACP: lacp_p(Gi5/0/0) expired
*Aug 20 17:22:25.917: lacp_ptx Gi5: during state FAST_PERIODIC, got event 3(pt_expired)
*Aug 20 17:22:25.917: @@@ lacp_ptx Gi5: FAST_PERIODIC -> PERIODIC_TX
*Aug 20 17:22:25.917: LACP: Gi5/0/0 lacp_action_ptx_fast_periodic_exit entered
*Aug 20 17:22:25.917: LACP: lacp_p(Gi5/0/0) timer stopped
Router1#
debug lane client

Effective with Cisco IOS Release 15.1M, the **debug lane client** command is not available in Cisco IOS software.

To display information about a LAN Emulation Client (LEC), use the **debug lane client** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug lane client {all | le-arp | mpoa | packet | signaling | state | topology} [interface interface]
no debug lane client {all | le-arp | mpoa | packet | signaling | state | topology} [interface interface]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all debug information related to the LEC.</td>
</tr>
<tr>
<td>le-arp</td>
<td>Displays debug information related to the LAN Emulation (LANE) Address Resolution Protocol (ARP) table.</td>
</tr>
<tr>
<td>mpoa</td>
<td>Displays debug information to track the following:</td>
</tr>
<tr>
<td></td>
<td>• MPOA specific TLV information in le-arp requests/responses</td>
</tr>
<tr>
<td></td>
<td>• Elan-id and local segment TLV in lane control frames</td>
</tr>
<tr>
<td></td>
<td>• When a LANE client is bound to an MPC/MPS</td>
</tr>
<tr>
<td>packet</td>
<td>Displays debug information about each packet.</td>
</tr>
<tr>
<td>signaling</td>
<td>Displays debug information related to client switched virtual circuits (SVCs).</td>
</tr>
<tr>
<td>state</td>
<td>Displays debug information when the state changes.</td>
</tr>
<tr>
<td>topology</td>
<td>Displays debug information related to the topology of the emulated LAN (ELAN).</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Limits the debugging output to messages that relate to a particular interface or subinterface. If you enter this command multiple times with different interfaces, the last interface entered will be the one used to filter the messages.</td>
</tr>
</tbody>
</table>

### Command Default

If the interface number is not specified, the default will be the number of all the **mpoa lane** clients.

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1M</td>
<td>This command was removed.</td>
</tr>
</tbody>
</table>
Usage Guidelines

The **debug lane client all** command can generate a large amount of output. Use a limiting keyword or specify a subinterface to decrease the amount of output and focus on the information you need.

Examples

The following example shows output for **debug lane client packet** and **debug lane client state** commands for an LEC joining an ELAN named elan1:

```
Router# debug lane client packet
Router# debug lane client state
```

The LEC listens for signaling calls to its ATM address (Initial State):

```
LEC ATM2/0.1: sending LISTEN
LEC ATM2/0.1: listen on 39.020304050607080910111213.00000CA05B40.01
LEC ATM2/0.1: received LISTEN
```

The LEC calls the LAN Emulation Configuration Server (LECS) and attempts to set up the Configure Direct VC (LECS Connect Phase):

```
LEC ATM2/0.1: sending SETUP
LEC ATM2/0.1: callid 0x6114D174
LEC ATM2/0.1: called party 39.020304050607080910111213.00000CA05B43.00
LEC ATM2/0.1: calling_party 39.020304050607080910111213.00000CA05B40.01
```

The LEC receives a CONNECT response from the LECS. The Configure Direct VC is established:

```
LEC ATM2/0.1: received CONNECT
LEC ATM2/0.1: callid 0x6114D174
LEC ATM2/0.1: vcd 148
```

The LEC sends a CONFIG REQUEST to the LECS on the Configure Direct VC (Configuration Phase):

```
LEC ATM2/0.1: sending LANE_CONFIG_REQ on VCD 148
LEC ATM2/0.1: SRC MAC address 0000.0ca0.5b40
LEC ATM2/0.1: SRC ATM address 39.020304050607080910111213.00000CA05B40.01
LEC ATM2/0.1: LAN Type 2
LEC ATM2/0.1: Frame size 2
LEC ATM2/0.1: LAN Name elan1
LEC ATM2/0.1: LAN Name size 5
```

The LEC receives a CONFIG RESPONSE from the LECS on the Configure Direct VC:

```
LEC ATM2/0.1: received LANE_CONFIG_RSP on VCD 148
LEC ATM2/0.1: SRC MAC address 0000.0ca0.5b40
LEC ATM2/0.1: SRC ATM address 39.020304050607080910111213.00000CA05B40.01
LEC ATM2/0.1: LAN Type 2
LEC ATM2/0.1: Frame size 2
LEC ATM2/0.1: LAN Name elan1
LEC ATM2/0.1: LAN Name size 5
```

The LEC releases the Configure Direct VC:

```
LEC ATM2/0.1: sending RELEASE
LEC ATM2/0.1: callid 0x6114D174
LEC ATM2/0.1: cause code 31
```

The LEC receives a RELEASE_COMPLETE from the LECS:
LEC ATM2/0.1: received RELEASE_COMPLETE
LEC ATM2/0.1: callid 0x6114D174
LEC ATM2/0.1: cause code 16

The LEC calls the LAN Emulation Server (LES) and attempts to set up the Control Direct VC (Join/Registration Phase):

LEC ATM2/0.1: sending SETUP
LEC ATM2/0.1: callid 0x61167110
LEC ATM2/0.1: called party 39.020304050607080910111213.00000CA05B41.01
LEC ATM2/0.1: calling_party 39.020304050607080910111213.00000CA05B40.01

The LEC receives a CONNECT response from the LES. The Control Direct VC is established:

LEC ATM2/0.1: received CONNECT
LEC ATM2/0.1: callid 0x61167110
LEC ATM2/0.1: vcd 150

The LEC sends a JOIN REQUEST to the LES on the Control Direct VC:

LEC ATM2/0.1: sending LANE_JOIN_REQ on VCD 150
LEC ATM2/0.1: Status 0
LEC ATM2/0.1: LECID 0
LEC ATM2/0.1: SRC MAC address 0000.0ca0.5b40
LEC ATM2/0.1: SRC ATM address 39.020304050607080910111213.00000CA05B40.01
LEC ATM2/0.1: LAN Type 2
LEC ATM2/0.1: Frame size 2
LEC ATM2/0.1: LAN Name elan1
LEC ATM2/0.1: LAN Name size 5

The LEC receives a SETUP request from the LES to set up the Control Distribute VC:

LEC ATM2/0.1: received SETUP
LEC ATM2/0.1: callid 0x6114D174
LEC ATM2/0.1: called party 39.020304050607080910111213.00000CA05B40.01
LEC ATM2/0.1: calling_party 39.020304050607080910111213.00000CA05B41.01

The LEC responds to the LES call setup with a CONNECT:

LEC ATM2/0.1: sending CONNECT
LEC ATM2/0.1: callid 0x6114D174
LEC ATM2/0.1: vcd 151

A CONNECT_ACK is received from the ATM switch. The Control Distribute VC is established:

LEC ATM2/0.1: received CONNECT_ACK
The LEC receives a JOIN response from the LES on the Control Direct VC.
LEC ATM2/0.1: received LANE_JOIN_RSP on VCD 150
LEC ATM2/0.1: Status 0
LEC ATM2/0.1: LECID 1
LEC ATM2/0.1: SRC MAC address 0000.0ca0.5b40
LEC ATM2/0.1: SRC ATM address 39.020304050607080910111213.00000CA05B40.01
LEC ATM2/0.1: LAN Type 2
LEC ATM2/0.1: Frame size 2
LEC ATM2/0.1: LAN Name elan1
LEC ATM2/0.1: LAN Name size 5

The LEC sends an LE ARP request to the LES to obtain the broadcast and unknown server (BUS) ATM NSAP address (BUS connect):
LEC ATM2/0.1: sending LANE_ARP_REQ on VCD 150
LEC ATM2/0.1: SRC MAC address 0000.0ca0.5b40
LEC ATM2/0.1: SRC ATM address 39.020304050607080910111213.00000CA05B40.01
LEC ATM2/0.1: TARGET MAC address ffff.ffff.ffff
LEC ATM2/0.1: TARGET ATM address 00.000000000000000000000000.0000000000.00

The LEC receives its own LE ARP request via the LES over the Control Distribute VC:

LEC ATM2/0.1: received LANE_ARP_RSP on VCD 151
LEC ATM2/0.1: SRC MAC address 0000.0ca0.5b40
LEC ATM2/0.1: SRC ATM address 39.020304050607080910111213.00000CA05B40.01
LEC ATM2/0.1: TARGET MAC address ffff.ffff.ffff
LEC ATM2/0.1: TARGET ATM address 39.020304050607080910111213.00000CA05B42.01

The LEC calls the BUS and attempts to set up the Multicast Send VC:

LEC ATM2/0.1: sending SETUP
LEC ATM2/0.1: callid 0x6114D354
LEC ATM2/0.1: called party 39.020304050607080910111213.00000CA05B42.01
LEC ATM2/0.1: calling_party 39.020304050607080910111213.00000CA05B40.01

The LEC receives a CONNECT response from the BUS. The Multicast Send VC is established:

LEC ATM2/0.1: received CONNECT
LEC ATM2/0.1: callid 0x6114D354
LEC ATM2/0.1: vcd 153

The LEC receives a SETUP request from the BUS to set up the Multicast Forward VC:

LEC ATM2/0.1: received SETUP
LEC ATM2/0.1: callid 0x610D4230
LEC ATM2/0.1: called party 39.020304050607080910111213.00000CA05B40.01
LEC ATM2/0.1: calling_party 39.020304050607080910111213.00000CA05B42.01

The LEC responds to the BUS call setup with a CONNECT:

LEC ATM2/0.1: sending CONNECT
LEC ATM2/0.1: callid 0x610D4230
LEC ATM2/0.1: vcd 154

A CONNECT_ACK is received from the ATM switch. The Multicast Forward VC is established:

LEC ATM2/0.1: received CONNECT_ACK
The LEC moves into the OPERATIONAL state.
%LANE-5-UPDOWN: ATM2/0.1 elan elan1: LE Client changed state to up

The following output is from the show lane client command after the LEC joins the emulated LAN as shown in the debug lane client output:
The following example shows **debug lane client** all command output when an interface with LECS, an LES/BUS, and an LEC is shut down:

Router# **debug lane client all**
LEC ATM1/0.2: received RELEASE_COMPLETE
LEC ATM1/0.2: callid 0x60E8B474
LEC ATM1/0.2: cause code 0
LEC ATM1/0.2: action A_PROCESS_REL_COMP
LEC ATM1/0.2: action A_TEARDOWN_LEC
LEC ATM1/0.2: sending RELEASE
LEC ATM1/0.2: callid 0x60EB6160
LEC ATM1/0.2: cause code 31
LEC ATM1/0.2: sending RELEASE
LEC ATM1/0.2: callid 0x60EB7548
LEC ATM1/0.2: cause code 31
LEC ATM1/0.2: sending RELEASE
LEC ATM1/0.2: callid 0x60EB9E48
LEC ATM1/0.2: cause code 31
LEC ATM1/0.2: sending CANCEL
LEC ATM1/0.2: ATM address 47.00918100000000613E5A2F01.006070174820.02
LEC ATM1/0.2: state ACTIVE event LEC_SIG_RELEASE_COMP => TERMINATING
LEC ATM1/0.3: received RELEASE_COMPLETE
LEC ATM1/0.3: callid 0x60EB6108
LEC ATM1/0.3: cause code 0
LEC ATM1/0.3: action A_PROCESS_REL_COMP
LEC ATM1/0.3: action A_TEARDOWN_LEC
LEC ATM1/0.3: sending RELEASE
LEC ATM1/0.3: callid 0x60EB66D4
LEC ATM1/0.3: cause code 31
LEC ATM1/0.3: sending RELEASE
LEC ATM1/0.3: callid 0x60EB7B8C
LEC ATM1/0.3: cause code 31
LEC ATM1/0.3: sending RELEASE
LEC ATM1/0.3: callid 0x60EBA3BC
LEC ATM1/0.3: cause code 31
LEC ATM1/0.3: sending CANCEL
LEC ATM1/0.3: ATM address 47.00918100000000613E5A2F01.006070174820.03
LEC ATM1/0.3: state ACTIVE event LEC_SIG_RELEASE_COMP => TERMINATING
LEC ATM1/0.2: received RELEASE_COMPLETE
LEC ATM1/0.2: callid 0x60EB7548
LEC ATM1/0.2: cause code 0
LEC ATM1/0.2: action A_PROCESS_TERM_REL_COMP
LEC ATM1/0.2: state TERMINATING event LEC_SIG_RELEASE_COMP => TERMINATING
LEC ATM1/0.3: received RELEASE_COMPLETE
LEC ATM1/0.3: callid 0x60EB7B8C
LEC ATM1/0.3: cause code 0
LEC ATM1/0.3: action A_PROCESS_TERM_REL_COMP
LEC ATM1/0.3: state TERMINATING event LEC_SIG_RELEASE_COMP => TERMINATING
LEC ATM1/0.1: received RELEASE_COMPLETE
LEC ATM1/0.1: callid 0x60EBC458
LEC ATM1/0.1: cause code 0
LEC ATM1/0.1: action A_PROCESS_REL_COMP
LEC ATM1/0.1: action A_TEARDOWN_LEC
LEC ATM1/0.1: sending RELEASE
LEC ATM1/0.1: callid 0x60EBD30C
LEC ATM1/0.1: cause code 31
LEC ATM1/0.1: sending RELEASE
LEC ATM1/0.1: callid 0x60EBDD28
LEC ATM1/0.1: cause code 31
LEC ATM1/0.1: sending RELEASE
LEC ATM1/0.1: callid 0x60EBF174
LEC ATM1/0.1: cause code 31
LEC ATM1/0.1: sending CANCEL
LEC ATM1/0.1: ATM address 47.009181000000061E5A2F01.006070174820.01
LEC ATM1/0.1: state ACTIVE event LEC_SIG_RELEASE_COMP => TERMINATING
LEC ATM1/0.1: received RELEASE_COMPLETE
LEC ATM1/0.1: callid 0x60EBDD28
LEC ATM1/0.1: cause code 0
LEC ATM1/0.1: action A_PROCESS_TERM_REL_COMP
LEC ATM1/0.1: state TERMINATING event LEC_SIG_RELEASE_COMP => TERMINATING
LEC ATM1/0.2: received RELEASE_COMPLETE
LEC ATM1/0.2: callid 0x60EB6160
LEC ATM1/0.2: cause code 0
LEC ATM1/0.2: action A_PROCESS_TERM_REL_COMP
LEC ATM1/0.2: state TERMINATING event LEC_SIG_RELEASE_COMP => TERMINATING
LEC ATM1/0.3: received RELEASE_COMPLETE
LEC ATM1/0.3: callid 0x60EB66D4
LEC ATM1/0.3: cause code 0
LEC ATM1/0.3: action A_PROCESS_TERM_REL_COMP
LEC ATM1/0.3: state TERMINATING event LEC_SIG_RELEASE_COMP => TERMINATING
LEC ATM1/0.2: received CANCEL
LEC ATM1/0.2: state IDLE event LEC_SIG_CANCEL => IDLE
LEC ATM1/0.3: received CANCEL
LEC ATM1/0.3: state IDLE event LEC_SIG_CANCEL => IDLE
LEC ATM1/0.1: received CANCEL
LEC ATM1/0.1: state IDLE event LEC_SIG_CANCEL => IDLE
LEC ATM1/0.1: action A_SHUTDOWN_LEC
LEC ATM1/0.1: sending CANCEL
LEC ATM1/0.1: ATM address 47.009181000000061E5A2F01.006070174820.02
LEC ATM1/0.3: action A_SHUTDOWN_LEC
LEC ATM1/0.3: sending CANCEL
LEC ATM1/0.3: ATM address 47.009181000000061E5A2F01.006070174820.03
LEC ATM1/0.1: state IDLE event LEC.Local deactivate => IDLE
LEC ATM1/0.2: state Idle event LEC.Local deactivate => IDLE
LEC ATM1/0.3: state Idle event LEC.Local deactivate => IDLE

The following output is from the debug lane client mpoa command when the lane interface is shut down:
The following output is from the **debug lane client mpoa** command when the **lane** interface is started (not shut down):

```
Router# debug lane client mpoa
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int atm 1/1/0.1
Router(config-subif)#shutdown
Router(config-subif)#
00:23:32:LANE-5-UPDOWN:ATM1/1/0.1 elan elan2:LE Client changed state to down
00:23:32:LEC ATM1/1/0.1:lec_inform_mpoa_state_chg:DOWN
00:23:32:LEC ATM1/1/0.1:lec_inform_mpoa_state_chg:DOWN
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#exit
Router(config)#exit
```

```
The following output is from the **debug lane client mpoa** command when the **lane** interface is started (not shut down):

```
Router# debug lane client mpoa
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int atm 1/1/0.1
Router(config-subif)#
00:23:39:LEC ATM1/1/0.1:lec_process_lane_tlv:msg LANE_CONFIG_RSP, num_tlvs 14
00:23:39:LEC ATM1/1/0.1:elan id from LECS set to 300
00:23:39:LEC ATM1/1/0.1:lec_process_lane_tlv:msg LANE_JOIN_RSP, num_tlvs 1
00:23:39:LEC ATM1/1/0.1:elan id from LES set to 300
00:23:39:LEC ATM1/1/0.1:lec_append_mpoa_dev_tlv:
00:23:39:LEC ATM1/1/0.1:got mpoa client addr 47.0091810000000050E2097801.0050A29AF42D.00
00:23:39:LANE-5-UPDOWN:ATM1/1/0.1 elan elan2:LE Client changed state to up
00:23:39:LEC ATM1/1/0.1:lec_inform_mpoa_state_chg:UP
00:25:57:LEC ATM1/1/0.1:lec_process_lane_tlv:msg LANE_ARP_REQ, num_tlvs 1
00:25:57:LEC ATM1/1/0.1:lec_process_dev_type_tlv: lec 47.0091810000000050E2097801.00500B306440.02
type MPS, mpc 0.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.
mpps 47.0091810000000050E2097801.00500B306444.00, num_mps_mac 1, mac 0050.0B30.6440
00:25:57:LEC ATM1/1/0.1:create mpoa_lec
00:25:57:LEC ATM1/1/0.1:new mpoa_lec 0x617E3118
00:25:57:LEC ATM1/1/0.1:lec_process_dev_type_tlv:type MPS, num_mps_mac 1
00:25:57:LEC ATM1/1/0.1:lec_add_mps:
remote lec 47.0091810000000050E2097801.00500B306440.02
mpoa nsap 47.0091810000000050E2097801.00500B306444.00, num_mps_mac 1, mac 0050.0B30.6440
00:25:57:LEC ATM1/1/0.1:lec_process_dev_type_tlv:remote lec 47.0091810000000050E2097801.00500B306440.02
mpoa nsap 47.0091810000000050E2097801.00500B306444.00, num_mps_mac 1, mac 0050.0B30.6440
00:25:57:LEC ATM1/1/0.1:lec_add_mps:
remote lec 47.0091810000000050E2097801.00500B306440.02
mpoa nsap 47.0091810000000050E2097801.00500B306444.00, num_mps_mac 1, mac 0050.0B30.6440
00:25:57:LEC ATM1/1/0.1:lec_process_dev_type_tlv:remote lec 47.0091810000000050E2097801.00500B306440.02
mpoa nsap 47.0091810000000050E2097801.00500B306444.00, num_mps_mac 1, mac 0050.0B30.6440
00:25:57:LEC ATM1/1/0.1:lec_add_mps:
remote lec 47.0091810000000050E2097801.00500B306440.02
mpoa nsap 47.0091810000000050E2097801.00500B306444.00, num_mps_mac 1, mac 0050.0B30.6440
00:25:57:LEC ATM1/1/0.1:lec_process_dev_type_tlv:
remote lec 47.0091810000000050E2097801.00500B306440.02
mpoa nsap 47.0091810000000050E2097801.00500B306444.00, num_mps_mac 1, mac 0050.0B30.6440
00:25:57:LEC ATM1/1/0.1:lec_process_dev_type_tlv:
remote lec 47.0091810000000050E2097801.00500B306440.02
mpoa nsap 47.0091810000000050E2097801.00500B306444.00, num_mps_mac 1, mac 0050.0B30.6440
00:25:57:LEC ATM1/1/0.1:lec_process_dev_type_tlv:
remote lec 47.0091810000000050E2097801.00500B306440.02
mpoa nsap 47.0091810000000050E2097801.00500B306444.00, num_mps_mac 1, mac 0050.0B30.6440
```

**Cisco IOS Debug Command Reference - Commands I through L**

620
The following output is from the **debug lane client mpoa** command when the ATM major interface is shut down:

```
Router# debug lane client mpoa
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# int atm 1/1/0
Router(config-if)# shutdown
Router(config-if)#
00:26:28:LANE ATM1/1/0:atm hardware reset
00:26:28:%LANE-5-UPDOWN:ATM1/1/0.1 elan elan2:LE Client changed state to down
00:26:28:LEC ATM1/1/0.1:lec_info_mpoa_state_chg:DOWN
00:26:28:LEC ATM1/1/0.1:lec_info_mpoa_state_chg:DOWN
00:26:28:%MPOA-5-UPDOWN:MPC mp2:state changed to down
00:26:28:LEC ATM1/1/0.1:mpoa_to_lec:appl 6, opcode 0
00:26:30:%LINK-5-CHANGED:Interface ATM1/1/0, changed state to administratively down
00:26:30:LANE ATM1/1/0:atm hardware reset
00:26:31:%LINEPROTO-5-UPDOWN:Line protocol on Interface ATM1/1/0, changed state to down
Router(config-if)#
00:26:32:LANE ATM1/1/0:atm hardware reset
00:26:32:LEC ATM1/1/0.1:mpoa_to_lec:appl 6, opcode 0
00:26:32:LANE ATM1/1/0:atm hardware reset
00:26:32:LEC ATM1/1/0.1:lec_info_mpoa_state_chg:DOWN
00:26:32:LEC ATM1/1/0.1:lec_info_mpoa_state_chg:DOWN
Router(config-if)# exit
Router(config)# exit
```

The following output is from the **debug lane client mpoa** command when the ATM major interface is started:

```
Router# debug lane client mpoa
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# int atm 1/1/0
Router(config-if)# no shutdown
Router(config-if)#
00:26:32:LANE ATM1/1/0:atm hardware reset
00:26:32:LEC ATM1/1/0.1:lec_info_mpoa_state_chg:DOWN
00:26:34:%LINK-3-UPDOWN:Interface ATM1/1/0, changed state to down
00:26:34:LANE ATM1/1/0:atm hardware reset
00:26:41:%LINK-3-UPDOWN:Interface ATM1/1/0, changed state to up
00:26:42:%LINEPROTO-5-UPDOWN:Line protocol on Interface ATM1/1/0, changed state to up
00:27:10:%LANE-6-INFO:ATM1/1/0:ILMI prefix add event received
00:27:10:LANE ATM1/1/0:prefix add event for 470091810000000050E2097801 ptr=0x617BFC0C len=13
00:27:10: the current first prefix is now:470091810000000050E2097801
00:27:10:%ATMSSCOP-5-SSCOPINIT:- Intf :ATM1/1/0, Event :Rcv End, State :Active.
00:27:10:%LANE-6-INFO:ATM1/1/0:ILMI prefix add event received
00:27:10:LANE ATM1/1/0:prefix add event for 470091810000000050E2097801 ptr=0x617BEE6C len=13
00:27:10: the current first prefix is now:470091810000000050E2097801
```
00:27:10:%LANE-5-UPDOWN:ATM1/1/0.1 elan elan2:LE Client changed state to down
00:27:10:LEC ATM1/1/0.1:lec_inform_mpoa_state_chg:DOWN
00:27:10:LEC ATM1/1/0.1:mpoa_to_lec:appl 6, opcode 0
00:27:10:%MPOA-5-UPDOWN:MPC mpc2:state changed to up
00:27:10:LEC ATM1/1/0.1:mpoa_to_lec:appl 6, opcode 1
00:27:12:LEC ATM1/1/0.1:lec_process_lane_tlv:msg LANE_CONFIG_RSP, num_tlvs 14
00:27:12:LEC ATM1/1/0.1:elan id from LECS set to 300
00:27:12:LEC ATM1/1/0.1:lec_process_lane_tlv:msg LANE_JOIN_RSP, num_tlvs 1
00:27:12:LEC ATM1/1/0.1:elan id from LES set to 300
00:27:12:LEC ATM1/1/0.1:lec_append_mpoa_dev_tlv:
00:27:12:LEC ATM1/1/0.1:got mpoa client addr 47.0091810000000050E2097801.0050A29AF42D.00
00:27:12:%LANE-5-UPDOWN:ATM1/1/0.1 elan elan2:LE Client changed state to up
00:27:12:LEC ATM1/1/0.1:lec_inform_mpoa_state_chg:UP
Router(config-if)#exit
Router(config)#exit

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug modem traffic</td>
<td>Displays MPC debug information.</td>
</tr>
<tr>
<td>debug mpoa server</td>
<td>Displays information about the MPOA server.</td>
</tr>
</tbody>
</table>
**debug lane config**

**Note**

Effective with Cisco IOS Release 15.1M, the `debug lane config` command is not available in Cisco IOS software.

To display information about a LAN Emulation (LANE) configuration server, use the `debug lane config` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug lane config {all | events | packets}
no debug lane config {all | events | packets}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all debugging messages related to the LANE configuration server. The output includes both the <code>events</code> and <code>packets</code> types of output.</td>
</tr>
<tr>
<td>events</td>
<td>Displays only messages related to significant LANE configuration server events.</td>
</tr>
<tr>
<td>packets</td>
<td>Displays information on each packet sent or received by the LANE configuration server.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1M</td>
<td>This command was removed.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug lane config` output is intended to be used primarily by a Cisco technical support representative.

**Examples**

The following is sample output from the `debug lane config all` command when an interface with LECS, an LES/BUS, and an LEC is shut down:

```
Router# debug lane config all
LECS EVENT ATMI/0: processing interface down transition
LECS EVENT ATMI/0: placed de-register address 0x60E8A824 (47.0091810000000613E5A2F01.006070174823.00) request with signalling
LECS EVENT ATMI/0: ilmiDeRegisterAddress: sendSetRequestToILMI failure; interface down ?
LECS EVENT ATMI/0: placed de-register address 0x60EC4F28 (47.00790000000000000000000000A03E000001.00) request with signalling
LECS EVENT ATMI/0: ilmiDeRegisterAddress: sendSetRequestToILMI failure; interface down ?
LECS EVENT ATMI/0: placed de-register address 0x60EC5C08 (47.0089100000000613E5A2F01.006070174823.99) request with signalling
LECS EVENT ATMI/0: ilmiDeRegisterAddress: sendSetRequestToILMI failure; interface down ?
LECS EVENT ATMI/0: tearing down all connexions
LECS EVENT ATMI/0: elan 'xxx' LES 47.0091810000000613E5A2F01.006070174821.01 callId 0x60CE0F58 deliberately being disconnected
LECS EVENT ATMI/0: sending RELEASE for call 0x60CE0F58 cause 31
LECS EVENT ATMI/0: elan 'yyy' LES 47.0091810000000613E5A2F01.006070174821.02 callId 0x60CE2104 deliberately being disconnected
LECS EVENT ATMI/0: sending RELEASE for call 0x60CE2104 cause 31
LECS EVENT ATMI/0: elan 'zzz' LES 47.0091810000000613E5A2F01.006070174821.03 callId
```

Cisco IOS Debug Command Reference - Commands I through L
0x60CE2DC8 deliberately being disconnected
LECS EVENT ATM1/0: sending RELEASE for call 0x60CE2DC8 cause 31
LECS EVENT ATM1/0: All calls to/from LECSs are being released
LECS EVENT ATM1/0: placed de-register address 0x60EC4F28
(47.007900000000000000000000.00A03E00001.00) request with signalling
LECS EVENT ATM1/0: ilmiDeRegisterAddress: sendSetRequestToILMI failure; interface down?
LECS EVENT ATM1/0: ATM_RELEASE_COMPLETE received: callId 0x60CE0F58 cause 0
LECS EVENT ATM1/0: call 0x60CE0F58 cleaned up
LECS EVENT ATM1/0: ATM_RELEASE_COMPLETE received: callId 0x60CE2104 cause 0
LECS EVENT ATM1/0: call 0x60CE2104 cleaned up
LECS EVENT ATM1/0: ATM_RELEASE_COMPLETE received: callId 0x60CE2DC8 cause 0
LECS EVENT ATM1/0: call 0x60CE2DC8 cleaned up
LECS EVENT ATM1/0: UNKNOWN/UNSET: signalling DE-registered
LECS EVENT: UNKNOWN/UNSET: signalling DE-registered
LECS EVENT ATM1/0: placed de-register address 0x60E8A824
(47.00918100000000613E5A2F1.006070174823.00) request with signalling
LECS EVENT ATM1/0: ilmiDeRegisterAddress: sendSetRequestToILMI failure; interface down?
LECS EVENT ATM1/0: placed de-register address 0x60EC5C08
(47.00918100000000613E5A2F1.006070174823.99) request with signalling
LECS EVENT ATM1/0: ilmiDeRegisterAddress: sendSetRequestToILMI failure; interface down?
LECS EVENT ATM1/0: tearing down all connexions
LECS EVENT ATM1/0: All calls to/from LECSs are being released
LECS EVENT: config server 56 killed
**debug lane finder**

**Note**

Effective with Cisco IOS Release 15.1M, the **debug lane finder** command is not available in Cisco IOS software.

To display information about the finder internal state machine, use the **debug lane finder** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug lane finder
no debug lane finder
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1M</td>
<td>This command was removed.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **debug lane finder** command output is intended to be used primarily by a Cisco technical support representative.

**Examples**

The following is sample output from the **debug lane finder** command when an interface with LECS, LES/BUS, and LEC is shut down:

```
Router# debug lane finder
LECS FINDER ATM1/0.3: user request 1819 of type GET_MASTER_LECS_ADDRESS queued up
LECS FINDER ATM1/0: finder state machine started
LECS FINDER ATM1/0: time to perform a getNext on the ILMI
LECS FINDER ATM1/0: LECS 47.00918100000000613E5A2F01.006070174823.00 deleted
LECS FINDER ATM1/0: ilmi_client_request failed, answering all users
LECS FINDER ATM1/0: answering all requests now
LECS FINDER ATM1/0: responded to user request 1819
LECS FINDER ATM1/0: number of remaining requests still to be processed: 0
LECS FINDER ATM1/0.2: user request 1820 of type GET_MASTER_LECS_ADDRESS queued up
LECS FINDER ATM1/0: finder state machine started
LECS FINDER ATM1/0: time to perform a getNext on the ILMI
LECS FINDER ATM1/0: ilmi_client_request failed, answering all users
LECS FINDER ATM1/0: answering all requests now
LECS FINDER ATM1/0: responded to user request 1820
LECS FINDER ATM1/0: number of remaining requests still to be processed: 0
LECS FINDER ATM1/0.1: user request 1821 of type GET_MASTER_LECS_ADDRESS queued up
LECS FINDER ATM1/0: finder state machine started
LECS FINDER ATM1/0: time to perform a getNext on the ILMI
LECS FINDER ATM1/0: ilmi_client_request failed, answering all users
LECS FINDER ATM1/0: answering all requests now
LECS FINDER ATM1/0: responded to user request 1821
LECS FINDER ATM1/0: number of remaining requests still to be processed: 0
```
debug lane server

**Note**
Effective with Cisco IOS Release 15.1M, the `debug lane server` command is not available in Cisco IOS software.

To display information about a LAN Emulation (LANE) server, use the `debug lane server` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
depth lane server [interface interface]
no debug lane server [interface interface]
```

**Syntax Description**

`interface interface` (Optional) Limits the debugging output to messages relating to a specific interface or subinterface. If you use this command multiple times with different interfaces, the last interface entered is the one used to filter debugging messages.

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1M</td>
<td>This command was removed.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug lane server` command output is intended to be used primarily by a Cisco technical support representative. The `debug lane server` command can generate a substantial amount of output. Specify a subinterface to decrease the amount of output and focus on the information you need.

**Examples**

The following is sample output from the `debug lane server` command when an interface with LECS, LES/BUS, and LEC is shut down:

```
Router# debug lane server
LES ATM1/0.1: lsv_lecsAccessSigCB called with callId 0x60CE124C, opcode ATM_RELEASE_COMPLETE
LES ATM1/0.1: disconnected from the master LECS
LES ATM1/0.1: should have been connected, will reconnect in 3 seconds
LES ATM1/0.2: lsv_lecsAccessSigCB called with callId 0x60CE29E0, opcode ATM_RELEASE_COMPLETE
LES ATM1/0.2: disconnected from the master LECS
LES ATM1/0.2: should have been connected, will reconnect in 3 seconds
LES ATM1/0.3: lsv_lecsAccessSigCB called with callId 0x60EB1940, opcode ATM_RELEASE_COMPLETE
LES ATM1/0.3: disconnected from the master LECS
LES ATM1/0.3: should have been connected, will reconnect in 3 seconds
LES ATM1/0.2: elan yyy client 1 lost control distribute
LES ATM1/0.2: elan yyy client 1 lost control distribute
LES ATM1/0.2: elan yyy client 1 lost control distribute
LES ATM1/0.2: elan yyy client 1 lost control distribute
LES ATM1/0.2: elan yyy client 1 lost control distribute
LES ATM1/0.2: elan yyy client 1 lost control distribute
LES ATM1/0.2: elan yyy client 1 lost control distribute
LES ATM1/0.2: elan yyy client 1 lost control distribute
LES ATM1/0.2: elan yyy client 1 lost control distribute
LES ATM1/0.2: elan yyy client 1 lost control distribute
```
LES ATM1/0.1: elan xxx client 1 lost control distribute
LES ATM1/0.1: elan xxx client 1: lsv_kill_client called
LES ATM1/0.1: elan xxx client 1 state change Oper -> Term
LES ATM1/0.1: elan xxx client 1 lost MC forward
LES ATM1/0.1: elan xxx client 1: lsv_kill_client called
LES ATM1/0.2: elan yyy client 1 released control direct
LES ATM1/0.2: elan yyy client 1: lsv_kill_client called
LES ATM1/0.3: elan zzz client 1 released control direct
LES ATM1/0.3: elan zzz client 1: lsv_kill_client called
LES ATM1/0.2: elan yyy client 1 MC forward released
LES ATM1/0.2: elan yyy client 1: lsv_kill_client called
LES ATM1/0.2: elan yyy client 1: freeing client structures
LES ATM1/0.3: elan zzz client 1 unregistered 0060.7017.4820
LES ATM1/0.3: elan zzz client 1: lsv_kill_client called
LES ATM1/0.3: elan zzz client 1: freeing client structures
LES ATM1/0.3: elan zzz client 1 unregistered 0060.7017.4820
LES ATM1/0.3: elan zzz client 1 destroyed
LES ATM1/0.1: elan xxx released control direct
LES ATM1/0.1: elan xxx: lsv_kill_client called
LES ATM1/0.1: elan xxx MC forward released
LES ATM1/0.1: elan xxx: lsv_kill_client called
LES ATM1/0.1: elan xxx: freeing client structures
LES ATM1/0.1: elan xxx: unregistered 0060.7017.4820
LES ATM1/0.1: elan xxx: destroyed
LES ATM1/0.1: elan xxx: major interface state change
LES ATM1/0.1: cleanupLecsAccess: discarding all validation requests
LES ATM1/0.1: shutting down
LES ATM1/0.1: elan xxx: lsv_kill_lesbus called
LES ATM1/0.1: elan xxx: LES/BUS state change operational -> terminating
LES ATM1/0.1: cleanupLecsAccess: discarding all validation requests
LES ATM1/0.2: elan yyy major interface state change
LES ATM1/0.2: cleanupLecsAccess: discarding all validation requests
LES ATM1/0.2: shutting down
LES ATM1/0.2: elan yyy: lsv_kill_lesbus called
LES ATM1/0.2: elan yyy: LES/BUS state change operational -> terminating
LES ATM1/0.2: cleanupLecsAccess: discarding all validation requests
LES ATM1/0.2: elan yyy: shutting down
LES ATM1/0.2: elan yyy: lsv_kill_lesbus called
LES ATM1/0.2: elan yyy: LES/BUS state change operational -> terminating
LES ATM1/0.2: cleanupLecsAccess: discarding all validation requests
LES ATM1/0.2: elan yyy: all clients killed
LES ATM1/0.2: elan yyy: stopping listening on addresses
LES ATM1/0.2: elan yyy: multicast groups killed
LES ATM1/0.3: elan zzz: addresses de-registered from ilmi
LES ATM1/0.3: elan zzz: LES/BUS state change terminating -> down
LES ATM1/0.3: elan zzz: administratively down
LES ATM1/0.3: elan zzz: lsv_kill_lesbus called
LES ATM1/0.3: cleanupLecsAccess: discarding all validation requests
LES ATM1/0.3: elan zzz: lsv_kill_lesbus called
LES ATM1/0.3: cleanupLecsAccess: discarding all validation requests
LES ATM1/0.3: elan zzz: all clients killed
LES ATM1/0.3: elan zzz: stopping listening on addresses
LES ATM1/0.3: elan zzz: multicast groups killed
LES ATM1/0.1: elan xxx: addresses de-registered from ilmi
LES ATM1/0.1: elan xxx: LES/BUS state change terminating -> down
LES ATM1/0.1: elan xxx: administratively down
LES ATM1/0.1: elan xxx: lsv_kill_lesbus called
LES ATM1/0.1: cleanupLecsAccess: discarding all validation requests
LES ATM1/0.1: elan xxx: stopping listening on addresses
LES ATM1/0.1: elan xxx: all clients killed
LES ATM1/0.1: elan xxx: multicast groups killed
LES ATM1/0.1: elan xxx: addresses de-registered from ilmi
LES ATM1/0.1: elan xxx: LES/BUS state change terminating -> down
LES ATM1/0.1: elan xxx: administratively down
LES ATM1/0.3: elan zzz: lsv_kill_lesbus called
LES ATM1/0.3: cleanupLecsAccess: discarding all validation requests
LES ATM1/0.3: elan zzz: lsv_kill_lesbus called
LES ATM1/0.3: cleanupLecsAccess: discarding all validation requests
LES ATM1/0.3: elan zzz: stopped listening on addresses
LES ATM1/0.3: elan zzz: all clients killed
LES ATM1/0.3: elan zzz: multicast groups killing
LES ATM1/0.3: elan zzz: addresses de-registered from ilmi
LES ATM1/0.3: elan zzz: LES/BUS state change terminating -> down
LES ATM1/0.3: elan zzz: administratively down
LES ATM1/0.3: cleanupLecsAccess: discarding all validation requests
LES ATM1/0.2: cleanupLecsAccess: discarding all validation requests
LES ATM1/0.1: cleanupLecsAccess: discarding all validation requests
**debug lane signaling**

**Note**
Effective with Cisco IOS Release 15.1M, the `debug lane signaling` command is not available in Cisco IOS software.

To display information about LANE Server (LES) and Broadcast and Unknown Server (BUS) switched virtual circuits (SVCs), use the `debug lane signaling` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug lane signaling [interface interface]
no debug lane signaling [interface interface]
```

**Syntax Description**
- `interface interface` (Optional) Limits the debugging output to messages relating to a specific interface or subinterface. If you use this command multiple times with different interfaces, the last interface entered is the one used to filter debugging messages.

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1M</td>
<td>This command was removed.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `debug lane signaling` command output is intended to be used primarily by a Cisco technical support representative. The `debug lane signaling` command can generate a substantial amount of output. Specify a subinterface to decrease the amount of output and focus on the information you need.

**Examples**
The following is sample output from the `debug lane signaling` command when a route with LECS, LES/BUS, and LEC is shut down:

```
Router# debug lane signaling
LANE SIG ATM1/0.2: received ATM_RELEASE_COMPLETE callid 0x60EB565C cause 0 lv 0x60E8D348 lvstate LANE_VCC_CONNECTED
LANE SIG ATM1/0.2: lane_sig_mc_release: breaking lv 0x60E8D348 from mcg 0x60E97E84
LANE SIG ATM1/0.2: timer for lv 0x60E8D348 stopped
LANE SIG ATM1/0.2: sent ATM_RELEASE request for lv 0x60E8D468 in state LANE_VCC_CONNECTED
LANE SIG ATM1/0.2: sent ATM_RELEASE request for lv 0x60E8D3D8 in state LANE_VCC_CONNECTED
LANE SIG ATM1/0.2: sent ATM_RELEASE request for lv 0x60E8D2B8 in state LANE_VCC_CONNECTED
LANE SIG ATM1/0.3: received ATM_RELEASE_COMPLETE callid 0x60EB5CA0 cause 0 lv 0x60E8BEF4 lvstate LANE_VCC_CONNECTED
LANE SIG ATM1/0.3: lane_sig_mc_release: breaking lv 0x60E8BEF4 from mcg 0x60E9A37C
LANE SIG ATM1/0.3: timer for lv 0x60E8BEF4 stopped
LANE SIG ATM1/0.3: sent ATM_RELEASE request for lv 0x60E8C014 in state LANE_VCC_CONNECTED
LANE SIG ATM1/0.3: sent ATM_RELEASE request for lv 0x60E8BBF84 in state LANE_VCC_CONNECTED
LANE SIG ATM1/0.3: sent ATM_RELEASE request for lv 0x60E8BE64 in state LANE_VCC_CONNECTED
LANE SIG ATM1/0.3: received ATM_RELEASE_COMPLETE callid 0x60EB9040 cause 0 lv 0x60E8D468 lvstate LANE_VCC.Drop_SENT
LANE SIG ATM1/0.2: lane_sig_mc_release: breaking lv 0x60E8D468 from mcg 0x60E97ECS
LANE SIG ATM1/0.2: timer for lv 0x60E8D468 stopped
```
LANE SIG ATM1/0.3: received ATM_RELEASE_COMPLETE callid 0x60EB97D4 cause 0 lv 0x60E8C014
lvstate LANE_VCC_DROP_SENT
LANE SIG ATM1/0.3: laneSig_mc_release: breaking lv 0x60E8C014 from mcg 0x60E9A3C0
LANE SIG ATM1/0.3: timer for lv 0x60E8C014 stopped
LANE SIG ATM1/0.1: received ATM_RELEASE_COMPLETE callid 0x60EBCEB8 cause 0 lv 0x60EBBAF0
lvstate LANE_VCC_CONNECTED
LANE SIG ATM1/0.1: laneSig_mc_release: breaking lv 0x60EBBAF0 from mcg 0x60E8F51C
LANE SIG ATM1/0.1: timer for lv 0x60EBBAF0 stopped
LANE SIG ATM1/0.1: sent ATM_RELEASE request for lv 0x60EBBB10 in state LANE_VCC_CONNECTED
LANE SIG ATM1/0.1: sent ATM_RELEASE request for lv 0x60EBBB80 in state LANE_VCC_CONNECTED
LANE SIG ATM1/0.1: sent ATM_RELEASE_COMPLETE callid 0x60EBBA60 cause 0 lv 0x60EBBC10
lvstate LANE_VCC_DROP_SENT
LANE SIG ATM1/0.1: laneSig_mc_release: breaking lv 0x60EBBC10 from mcg 0x60E8F560
LANE SIG ATM1/0.1: timer for lv 0x60EBBC10 stopped
LANE SIG ATM1/0.1: sent ATM_RELEASE_COMPLETE callid 0x60E8B174 cause 0 lv 0x60E8D2B8
lvstate LANE_VCC_RELEASE_SENT
LANE SIG ATM1/0.2: received ATM_RELEASE_COMPLETE callid 0x60EB97D4 cause 0 lv 0x60E8C014
lvstate LANE_VCC_RELEASE_SENT
LANE SIG ATM1/0.2: timer for lv 0x60E8C014 stopped
LANE SIG ATM1/0.2: sent ATM_RELEASE COMPLETE callid 0x60EBBAF0 cause 0 lv 0x60EBBB10
lvstate LANE_VCC_RELEASE_SENT
LANE SIG ATM1/0.2: timer for lv 0x60EBBAF0 stopped
LANE SIG ATM1/0.2: sent ATM_RELEASE COMPLETE callid 0x60EBBB80 cause 0 lv 0x60EBBB10
lvstate LANE_VCC_RELEASE_SENT
LANE SIG ATM1/0.2: timer for lv 0x60EBBB80 stopped
LANE SIG ATM1/0.2: sent ATM_RELEASE COMPLETE callid 0x60EBBB6D4 cause 0 lv 0x60EBBA60
lvstate LANE_VCC_RELEASE_SENT
LANE SIG ATM1/0.2: timer for lv 0x60EBBA60 stopped
LANE SIG ATM1/0.3: received ATM_RELEASE_COMPLETE callid 0x60EB97D4 cause 0 lv 0x60E8C014
lvstate LANE_VCC_RELEASE_SENT
LANE SIG ATM1/0.3: timer for lv 0x60E8C014 stopped
LANE SIG ATM1/0.3: sent ATM_RELEASE COMPLETE callid 0x60EBBAF0 cause 0 lv 0x60EBBB10
lvstate LANE_VCC_RELEASE_SENT
LANE SIG ATM1/0.3: timer for lv 0x60EBBAF0 stopped
LANE SIG ATM1/0.3: sent ATM_RELEASE COMPLETE callid 0x60EBBB80 cause 0 lv 0x60EBBB10
lvstate LANE_VCC_RELEASE_SENT
LANE SIG ATM1/0.3: timer for lv 0x60EBBB80 stopped
LANE SIG ATM1/0.3: sent ATM_CANCEL_NSAP request for lv 0x0 in state NULL_VCC_POINTER
LANE SIG ATM1/0.1: received ATM_CANCEL_NSAP for nsap 0.0.0.0
LANE SIG ATM1/0.1: sent ATM_CANCEL_NSAP request for lv 0x0 in state NULL_VCC_POINTER
LANE SIG ATM1/0.2: received ATM_CANCEL_NSAP request for lv 0x0 in state NULL_VCC_POINTER
LANE SIG ATM1/0.3: received ATM_CANCEL_NSAP for nsap 0.0.0.0
LANE SIG ATM1/0.1: sent ATM_CANCEL_NSAP request for lv 0x0 in state NULL_VCC_POINTER
LANE SIG ATM1/0.2: received ATM_CANCEL_NSAP request for lv 0x0 in state NULL_VCC_POINTER
LANE SIG ATM1/0.3: received ATM_CANCEL_NSAP for nsap 0.0.0.0
LANE SIG ATM1/0.1: sent ATM_CANCEL_NSAP request for lv 0x0 in state NULL_VCC_POINTER
LANE SIG ATM1/0.2: received ATM_CANCEL_NSAP request for lv 0x0 in state NULL_VCC_POINTER
LANE SIG ATM1/0.3: received ATM_CANCEL_NSAP for nsap 0.0.0.0
debug lapb

To display all traffic for interfaces using Link Access Procedure, Balanced (LAPB) encapsulation, use the `debug lapb` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug lapb
no debug lapb
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced prior to this release.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays information on the X.25 Layer 2 protocol. It is useful to users familiar with the LAPB protocol.

You can use the `debug lapb` command to determine why X.25 interfaces or LAPB connections are going up and down. It is also useful for identifying link problems, as evidenced when the `show interfaces` EXEC command displays a high number of rejects or frame errors over the X.25 link.

The `debug lapb` command can generate debugging messages of LAPB on all interfaces configured with the `encapsulation lapb` command or when X.25 traffic is present on interfaces configured with the `encapsulation x25` command. LAPB debugging produces a substantial amount of data and makes debugging very tedious. The problem becomes more severe if the network contains a large number of X.25 interfaces. Therefore the LAPB debugging should be available for individual interface.

⚠️ **Caution**

Because the `debug lapb` command generates a substantial amount of output, use it when the aggregate of all LAPB traffic on X.25 and LAPB interfaces is fewer than five frames per second.

**Examples**

The following is sample output from the `debug lapb` command (the numbers 1 through 7 at the top of the display have been added in order to aid documentation):

```
1 2 3 4 5 6 7
Serial0: LAPB I CONNECT (5) IFRAME F 2 1
Serial0: LAPB O REJSENT (2) REJ F 3
Serial0: LAPB O REJSENT (5) IFRAME 0 3
Serial0: LAPB I REJSENT (2) REJ (C) 7
Serial0: LAPB I DISCONNECT (2) SABM P
Serial0: LAPB O CONNECT (2) UA F
Serial0: LAPB O CONNECT (5) IFRAME 0 0
Serial0: LAPB T1 CONNECT 357964 0
```

Each line of output describes a LAPB event. There are two types of LAPB events: frame events (when a frame enters or exits the LAPB) and timer events. In the sample output, the last line describes
a timer event; all of the other lines describe frame events. The table below describes the first seven fields.

**Table 96: debug lapb Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First field (1)</td>
<td>Interface type and unit number reporting the frame event.</td>
</tr>
<tr>
<td>Second field (2)</td>
<td>Protocol providing the information.</td>
</tr>
<tr>
<td>Third field (3)</td>
<td>Frame event type. Possible values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• I--Frame input</td>
</tr>
<tr>
<td></td>
<td>• O--Frame output</td>
</tr>
<tr>
<td></td>
<td>• T1--T1 timer expired</td>
</tr>
<tr>
<td></td>
<td>• T3--Interface outage timer expired</td>
</tr>
<tr>
<td></td>
<td>• T4--Idle link timer expired</td>
</tr>
<tr>
<td>Fourth field (4)</td>
<td>State of the protocol when the frame event occurred. Possible values are as</td>
</tr>
<tr>
<td></td>
<td>follows:</td>
</tr>
<tr>
<td></td>
<td>• BUSY (RNR frame received)</td>
</tr>
<tr>
<td></td>
<td>• CONNECT</td>
</tr>
<tr>
<td></td>
<td>• DISCONNECT</td>
</tr>
<tr>
<td></td>
<td>• DISCSENT (disconnect sent)</td>
</tr>
<tr>
<td></td>
<td>• ERROR (FRMR frame sent)</td>
</tr>
<tr>
<td></td>
<td>• REJSENT (reject frame sent)</td>
</tr>
<tr>
<td></td>
<td>• SABMSENT (SABM frame sent)</td>
</tr>
<tr>
<td>Fifth field (5)</td>
<td>In a frame event, this value is the size of the frame (in bytes). In a</td>
</tr>
<tr>
<td></td>
<td>timer event, this value is the current timer value (in milliseconds).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Sixth field (6)       | In a frame event, this value is the frame type name. Possible values for frame type names are as follows:  
  - DISC--Disconnect  
  - DM--Disconnect mode  
  - FRMR--Frame reject  
  - IFRAME--Information frame  
  - ILLEGAL--Illegal LAPB frame  
  - REJ--Reject  
  - RNR--Receiver not ready  
  - RR--Receiver ready  
  - SABM--Set asynchronous balanced mode  
  - SABME--Set asynchronous balanced mode, extended  
  - UA--Unnumbered acknowledgment  
  In a T1 timer event, this value is the number of retransmissions already attempted. |
| Seventh field (7)     | This field is present only in frame events. It describes the frame type identified by the LAPB address and Poll/Final bit. Possible values are as follows:  
  - (C)--Command frame  
  - (R)--Response frame  
  - P--Command/Poll frame  
  - F--Response/Final frame  
  - /ERR--Command/Response type is invalid for the control field. An ?ERR generally means that the data terminal equipment (DTE)/data communications equipment (DCE) assignments are not correct for this link.  
  - BAD-ADDR--Address field is neither Command nor Response |

A timer event displays only the first six fields of `debug lapb` command output. For frame events, however, the seventh field documents the LAPB control information present in the frame. Depending on the value of the frame type name shown in the sixth field, the seventh field may or may not appear.

After the Poll/Final indicator, depending on the frame type, three different types of LAPB control information can be printed.

For information frames, the value of the N(S) field and the N(R) field will be printed. The N(S) field of an information frame is the sequence number of that frame, so this field will rotate between 0 and 7 for (modulo 8 operation) or 0 and 127 (for modulo 128 operation) for successive outgoing
information frames and (under normal circumstances) also will rotate for incoming information frame streams. The N(R) field is a “piggybacked” acknowledgment for the incoming information frame stream; it informs the other end of the link which sequence number is expected next.

RR, RNR, and REJ frames have an N(R) field, so the value of that field is printed. This field has exactly the same significance that it does in an information frame.

For the FRMR frame, the error information is decoded to display the rejected control field, V(R) and V(S) values, the Response/Command flag, and the error flags WXYZ.

In the following example, the output shows an idle link timer action (T4) where the timer expires twice on an idle link, with the value of T4 set to five seconds:

```
Serial2: LAPB T4 CONNECT 255748
Serial2: LAPB O CONNECT (2) RR P 5
Serial2: LAPB I CONNECT (2) RR F 5
Serial2: LAPB T4 CONNECT 260748
Serial2: LAPB O CONNECT (2) RR P 5
Serial2: LAPB I CONNECT (2) RR F 5
```

The next example shows an interface outage timer expiration (T3):

```
Serial2: LAPB T3 DISCONNECT 273284
```

The following example output shows an error condition when no DCE to DTE connection exists. Note that if a frame has only one valid type (for example, a SABM can only be a command frame), a received frame that has the wrong frame type will be flagged as a receive error (R/ERR in the following output). This feature makes misconfigured links (DTE-DTE or DCE-DCE) easy to spot. Other less common errors will also be highlighted, such as a too-short or too-long frame or an invalid address (neither command nor response).

```
Serial2: LAPB T1 SABMSENT 1026508 1
Serial2: LAPB O SABMSENT (2) SABM P
Serial2: LAPB I SABMSENT (2) SABM (R/ERR)
Serial2: LAPB T1 SABMSENT 1029508 2
Serial2: LAPB O SABMSENT (2) SABM P
Serial2: LAPB I SABMSENT (2) SABM (R/ERR)
```

The output in the next example shows that the router is misconfigured and has a standard (modulo 8) interface connected to an extended (modulo 128) interface. This condition is indicated by the SABM balanced mode and SABME balanced mode extended messages appearing on the same interface.

```
Serial2: LAPB T1 SABMSENT 1428720 0
Serial2: LAPB O SABMSENT (2) SABME P
Serial2: LAPB I SABMSENT (2) SABM P
Serial2: LAPB T1 SABMSENT 1431720 1
Serial2: LAPB O SABMSENT (2) SABME P
Serial2: LAPB I SABMSENT (2) SABM P
```

The output in the next example shows that the `debug lapb` command is set for a single interface; that is, interface 0/0.

```
Serial0/0: LAPB O CONNECT (17) IFRAME 1 7
Serial0/0: LAPB I CONNECT (5) IFRAME 7 2
Serial0/0: LAPB I CONNECT (6) IFRAME 0 2
Serial0/0: LAPB O CONNECT (2) RR (R) 1
Serial0/0: LAPB O CONNECT (50) IFRAME 2 1
```
Serial0/0: LAPB I CONNECT (15) IFRAME 1 2
Serial0/0: LAPB O CONNECT (5) IFRAME 3 2
debug lapb-ta

To display debugging messages for Link Access Procedure, Balanced-Terminal Adapter (LAPB-TA), use the \texttt{debug lapb-ta} command in privileged EXEC mode. To disable debugging output, use the \texttt{no} form of this command.

\texttt{debug lapb-ta [\{error | event | traffic\}]}

\texttt{no debug lapb-ta [\{error | event | traffic\}]}

**Syntax Description**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>(Optional) Displays LAPB-TA errors.</td>
</tr>
<tr>
<td>event</td>
<td>(Optional) Displays LAPB-TA normal events.</td>
</tr>
<tr>
<td>traffic</td>
<td>(Optional) Displays LAPB-TA in/out traffic data.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging for LAPB-TA is not enabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the \texttt{debug lapb-ta} command with the \texttt{error}, \texttt{event}, and \texttt{traffic} keywords activated:

```
Router# debug lapb-ta error
LAPB-TA error debugging is on
Router# debug lapb-ta event
LAPB-TA event debugging is on
Router# debug lapb-ta traffic
LAPB-TA traffic debugging is on
```

```
Mar 9 12:11:36.468:LAPBTA:get_ll_config:BR3/0:1
Mar 9 12:11:36.468:LAPBTA:line 130 allocated for BR3/0:1
Mar 9 12:11:36.468:LAPBTA:process 79
Mar 9 12:11:36.468:LAPBTA:service change:LAPB physical layer up, context 6183E144 interface up, protocol down
Mar 9 12:11:36.468:LAPBTA:service change:, context 6183E144 up
Mar 9 12:11:36.468:LAPBTA:service change: BR3/0:1, 44 sent
2d14h:2%LINEPROTO-5-UPDOWN:line protocol on Interface BR3/0:1, changed state to up
2d14h:2%ISDN-6-CONNECT:Interface BR3/0:1 is now connected to 60213
Mar 9 12:11:44.508:LAPB-TA:BR3/0:1, 1 rcvd
Mar 9 12:11:44.508:LAPB-TA:BR3/0:1, 3 sent
Mar 9 12:11:44.700:LAPB-TA:BR3/0:1, 1 rcvd
Mar 9 12:11:44.700:LAPB-TA:BR3/0:1, 3 sent
Mar 9 12:11:44.840:LAPB-TA:BR3/0:1, 1 rcvd
```
debug lat packet

To display information on all local-area transport (LAT) events, use the `debug lat packet` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
d-debug lat packet
no debug lat packet
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

- Privileged EXEC

**Usage Guidelines**

For each datagram (packet) received or sent, a message is logged to the console.

⚠️ **Caution**

This command severely impacts LAT performance and is intended for troubleshooting use only.

**Examples**

The following is sample output from the `debug lat packet` command:

```
Router# debug lat packet
LAT: I int=Ethernet0, src=0000.0c01.0509, dst=0900.2b00.000f, type=0, M=0, R=0
LAT: I int=Ethernet0, src=0800.2b11.2d13, dst=0000.0c01.7876, type=A, M=0, R=0
LAT: O dst=0800.2b11.2d13, int=Ethernet0, type=A, M=0, R=0, len=20, next 0 ref 1
```

The second line of output describes a packet that is input to the router. The table below describes the fields in this line.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAT:</td>
<td>Indicates that this display shows LAT debugging output.</td>
</tr>
<tr>
<td>I</td>
<td>Indicates that this line of output describes a packet that is input to the</td>
</tr>
<tr>
<td></td>
<td>router (I) or output from the router (O).</td>
</tr>
<tr>
<td>int = Eth</td>
<td>Indicates the interface on which the packet event took place.</td>
</tr>
<tr>
<td>src =</td>
<td>Indicates the source address of the packet.</td>
</tr>
<tr>
<td>dst=</td>
<td>Indicates the destination address of the packet.</td>
</tr>
<tr>
<td>0800.2b11.2</td>
<td></td>
</tr>
<tr>
<td>0c01.7876</td>
<td></td>
</tr>
</tbody>
</table>
Indicates the message type (in hexadecimal notation). Possible values are as follows:

- 0 = Run Circuit
- 1 = Start Circuit
- 2 = Stop Circuit
- A = Service Announcement
- C = Command
- D = Status
- E = Solicit Information
- F = Response Information

The third line of output describes a packet that is output from the router. The table below describes the last three fields in this line.

**Table 98: debug lat packet Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>len= 20</td>
<td>Indicates the length (in hexadecimal notation) of the packet (in bytes).</td>
</tr>
<tr>
<td>next 0</td>
<td>Indicates the link on the transmit queue.</td>
</tr>
<tr>
<td>ref 1</td>
<td>Indicates the count of packet users.</td>
</tr>
</tbody>
</table>
To enable debugging for Lightweight Directory Access Protocol (LDAP) configuration, use the `debug ldap` command in privileged EXEC mode. To disable debugging, use the `no debug ldap` form of this command.

```
ddebug ldap {all | error | event | legacy | packet}
no debug ldap {all | error | event | legacy | packet}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Displays all event, legacy, and packet related messages.</td>
</tr>
<tr>
<td><code>error</code></td>
<td>Displays error messages about the local authentication server.</td>
</tr>
<tr>
<td><code>event</code></td>
<td>Displays debug messages related to LDAP proxy events.</td>
</tr>
<tr>
<td><code>legacy</code></td>
<td>Displays legacy messages.</td>
</tr>
<tr>
<td><code>packet</code></td>
<td>Displays the content of the RADIUS packets that are sent and received.</td>
</tr>
</tbody>
</table>

### Command Modes

- Privileged EXEC (`#`)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `debug ldap legacy` command:

```
Router# debug ldap legacy
put_filter "(&(objectclass=*)(cn=firewall_user))"
put_filter: AND
put_filter_list "(objectclass=*)(cn=firewall_user)"
put_filter: simple
put_filter: simple
Doing socket write
Wait4msg (timeout 0 sec, 1 usec)
ldap_select_fd_wait (select)
ldap_read_activity lc 0x6804D354
Doing socket read
LDAP-TCP: Bytes read = 1478
ldap_match_request succeeded for msgid 2 h 0
ldap_get_dn
ldap_get_dn
ldap_msgfree
ldap_result
Wait4msg (timeout 0 sec, 1 usec)
ldap_read_activity lc 0x6804D354
ldap_match_request succeeded for msgid 2 h 0
changing lr 0x6774F8D4 to COMPLETE as no continuations
removing request 0x6774F8D4 from list as 1m 0x681C9B78 all 0
ldap_msgfree
ldap_msgfree
ldap_parse_result
```
ldap_parse_result
ldap_req_encode
Doing socket writeldap_msgfree
ldap_result
wait4msg (timeout 0 sec, 1 usec)
ldap_result
ldap_select_fd_wait (select)
ldap_result
wait4msg (timeout 0 sec, 1 usec)
 ldap_result
ldap_select_fd_wait (select)
ldap_read_activity lc 0x6804D354
Doing socket read
LDAP-TCP:Bytes read = 22
ldap_match_request succeeded for msgid 3 h 0
changing lr 0x6774F8D4 to COMPLETE as no continuations
removing request 0x6774F8D4 from list as lm 0x681C9B78 all 0
ldap_msgfree
ldap_msgfree
ldap_parse_result
ldap_parse_result
ldap_msgfree
ldap_result
wait4msg (timeout 0 sec, 1 usec)
ldap_select_fd_wait (select)

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4 (ldap)</td>
<td>Creates an IPv4 address within an LDAP server address pool</td>
</tr>
<tr>
<td>ldap server</td>
<td>Defines an LDAP server and enters LDAP server configuration mode.</td>
</tr>
<tr>
<td>transport port (ldap)</td>
<td>Configures the transport protocol for establishing a connection with the LDAP server.</td>
</tr>
</tbody>
</table>
debug lex rcmd

To debug LAN Extender remote commands, use the `debug lex rcmd` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug lex rcmd
no debug lex rcmd
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Examples**

The following is sample output from the `debug lex rcmd` command:

```
Router# debug lex rcmd
LEX-RCMD: "shutdown" command received on unbound serial interface- Serial0
LEX-RCMD: Lex0: "inventory" command received
Rcvd rcmd: FF 03 80 41 41 13 00 1A 8A 00 00 16 01 FF 00 00
Rcvd rcmd: 00 02 00 00 07 5B CD 15 00 00 0C 01 15 26
LEX-RCMD: ACK or response received on Serial0 without a corresponding ID
LEX-RCMD: REJ received
LEX-RCMD: illegal CODE field received in header: <number>
LEX-RCMD: illegal length for Lex0: "lex input-type-list"
LEX-RCMD: Lex0 is not bound to a serial interface
LEX-RCMD: encapsulation failure
LEX-RCMD: re-transmitting Lex0: "lex priority-group" command
LEX-RCMD: lex_setup_and_send called with invalid parameter
LEX-RCMD: bind occurred on shutdown LEX interface
LEX-RCMD: Serial0- No free Lex interface found with negotiated MAC address 0000.0c00.d8db
LEX-RCMD: No active Lex interface found for unbind
```

The following output indicates that a LAN Extender remote command packet was received on a serial interface that is not bound to a LAN Extender interface:

```
LEX-RCMD: "shutdown" command received on unbound serial interface- Serial0
```

This message can occur for any of the LAN Extender remote commands. Possible causes of this message are as follows:

- FLEX state machine software error
- Serial line momentarily goes down, which is detected by the host but not by FLEX

The following output indicates that a LAN Extender remote command response has been received. The hexadecimal values are for internal use only.

```
LEX-RCMD: Lex0: "inventory" command received
Rcvd rcmd: FF 03 80 41 41 13 00 1A 8A 00 00 16 01 FF 00 00
Rcvd rcmd: 00 02 00 00 07 5B CD 15 00 00 0C 01 15 26
```

The following output indicates that when the host router originates a LAN Extender remote command to FLEX, it generates an 8-bit identifier that is used to associate a command with its corresponding response:
LEX-RCMD: ACK or response received on Serial0 without a corresponding ID

This message could be displayed for any of the following reasons:

- FLEX was busy at the time that the command arrived and could not send an immediate response.
  The command timed out on the host router and then FLEX finally sent the response.

- Transmission error.

- Software error.

Possible responses to Config-Request are Config-ACK, Config-NAK, and Config-Rej. The following output shows that some of the options in the Config-Request are not recognizable or are not acceptable to FLEX due to transmission errors or software errors:

LEX-RCMD: REJ received

The following output shows that a LAN Extender remote command response was received but that the CODE field in the header was incorrect:

LEX-RCMD: illegal CODE field received in header: <number>

The following output indicates that a LAN Extender remote command response was received but that it had an incorrect length field. This message can occur for any of the LAN Extender remote commands.

LEX-RCMD: illegal length for Lex0: "lex input-type-list"

The following output shows that a host router was about to send a remote command when the serial link went down:

LEX-RCMD: Lex0 is not bound to a serial interface

The following output shows that the serial encapsulation routine of the interface failed to encapsulate the remote command datagram because the LEX-NCP was not in the OPEN state. Due to the way the PPP state machine is implemented, it is normal to see a single encapsulation failure for each remote command that gets sent at bind time.

LEX-RCMD: encapsulation failure

The following output shows that the timer expired for the given remote command without having received a response from the FLEX device. This message can occur for any of the LAN Extender remote commands.

LEX-RCMD: timeout for Lex0: "lex priority-group" command

This message could be displayed for any of the following reasons:

- FLEX too busy to respond

- Transmission failure

- Software error

The following output indicates that the host is resending the remote command after a timeout:
LEX-RCMD: re-transmitting Lex0: “lex priority-group” command

The following output indicates that an illegal parameter was passed to the lex_setup_and_send routine. This message could be displayed due to a host software error.

LEX-RCMD: lex_setup_and_send called with invalid parameter

The following output is informational and shows when a bind occurs on a shutdown interface:

LEX-RCMD: bind occurred on shutdown LEX interface

The following output shows that the LEX-NCP reached the open state and a bind operation was attempted with the FLEX's MAC address, but no free LAN Extender interfaces were found that were configured with that MAC address. This output can occur when the network administrator does not configure a LAN Extender interface with the correct MAC address.

LEX-RCMD: Serial0- No free Lex interface found with negotiated MAC address 0000.0c00.d8db

The following output shows that the serial line that was bound to the LAN Extender interface went down and the unbind routine was called, but when the list of active LAN Extender interfaces was searched, the LAN Extender interface corresponding to the serial interface was not found. This output usually occurs because of a host software error.

LEX-RCMD: No active Lex interface found for unbind
debug license

To enable controlled Cisco IOS software license debugging activity on a device, use the `debug license` command in privileged EXEC mode. To disable debugging, use the `no debug license` form of this command.

```
debug license {agent {all | error} | core {all | errors | events} | errors | events | ipc}
no debug license {agent {all | error} | core {all | errors | events} | errors | events | ipc}
```

Cisco ASR 1001 Router Platforms
```
default license {core {all | errors | events} | errors | ipc}
no default license {core {all | errors | events} | errors | ipc}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>agent</code></td>
<td>Debugs license agent information.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>--Debugs all license agent messages.</td>
</tr>
<tr>
<td><code>error</code></td>
<td>--Debugs only license agent error messages.</td>
</tr>
<tr>
<td><code>core</code></td>
<td>Debugs messages from a license core module.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>--Debugs all license core messages</td>
</tr>
<tr>
<td><code>errors</code></td>
<td>--Debugs only license core error messages</td>
</tr>
<tr>
<td><code>events</code></td>
<td>--Debugs only license core event messages.</td>
</tr>
<tr>
<td><code>errors</code></td>
<td>Debugs license warnings and errors.</td>
</tr>
<tr>
<td><code>events</code></td>
<td>Debugs license event messages.</td>
</tr>
<tr>
<td><code>ipc</code></td>
<td>Debugs license interprocess communication (IPC)</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(35)SE2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(15)XZ</td>
<td>This command was integrated into Cisco IOS Release 12.4(15)XZ.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2S</td>
<td>This command was implemented on the Cisco ASR 1001 router.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to help troubleshoot issues with licenses on a device.
On the Cisco ASR 1001 router, the output from the `debug license` command is not in standard IOS format. You must execute the `request platform software trace rotate all` privileged EXEC command to make the output in the log files in the bootflash:tracelogs directory.

**Examples**

The following example shows how to enable debugging for license warnings and errors on a router:

```
Router# debug license errors
```

The following example shows how to enable debugging for all license agent information on a switch:

```
Switch# debug license agent all
```

---

Cisco IOS Debug Command Reference - Commands I through L

**debug license**

On the Cisco ASR 1001 router, the output from the `debug license` command is not in standard IOS format. You must execute the `request platform software trace rotate all` privileged EXEC command to make the output in the log files in the bootflash:tracelogs directory.

**Examples**

The following example shows how to enable debugging for license warnings and errors on a router:

```
Router# debug license errors
```

The following example shows how to enable debugging for all license agent information on a switch:

```
Switch# debug license agent all
```

---

Cisco IOS Debug Command Reference - Commands I through L
**debug link monitor**

To display the statistics of the executing process, use the **debug link monitor** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug link monitor
no debug link monitor
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is used to display the statistics, which are used for debugging the status of the various conditions occurred during execution of the monitoring process.

**Examples**

The following example enables link monitoring statistics:

```
Router# debug link monitor
%DEBUG-ENABLED Error Rate Link Monitor
```

The following example disables link monitoring statistics:

```
Router# no debug link monitor
%DEBUG-DISABLED Error Rate Link Monitor
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug all</td>
<td>Enables debugging for link monitoring.</td>
</tr>
<tr>
<td>no debug all</td>
<td>Disables debugging for link monitoring.</td>
</tr>
<tr>
<td>clear counters</td>
<td>Clears show interface counters on all interfaces.</td>
</tr>
<tr>
<td>show link monitor debug</td>
<td>Show link monitor error statistics.</td>
</tr>
</tbody>
</table>
**debug list**

To filter debugging information on a per-interface or per-access list basis, use the `debug list` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug list [list] [interface]
no debug list [list] [interface]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>list</strong></td>
<td>(Optional) An access list number in the range from 1100 to 1199.</td>
</tr>
<tr>
<td><strong>interface</strong></td>
<td>(Optional) The interface type. Allowed values are the following:</td>
</tr>
<tr>
<td></td>
<td>• channel --IBM Channel interface</td>
</tr>
<tr>
<td></td>
<td>• ethernet --IEEE 802.3</td>
</tr>
<tr>
<td></td>
<td>• fddi --ANSI X3T9.5</td>
</tr>
<tr>
<td></td>
<td>• null --Null interface</td>
</tr>
<tr>
<td></td>
<td>• serial --Serial</td>
</tr>
<tr>
<td></td>
<td>• tokenring --IEEE 802.5</td>
</tr>
<tr>
<td></td>
<td>• tunnel --Tunnel interface</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC

### Usage Guidelines

The `debug list` command is used with other `debug` commands for specific protocols and interfaces to filter the amount of debug information that is displayed. In particular, this command is designed to filter specific physical unit (PU) output from bridging protocols. The `debug list` command is supported with the following commands:

- debug arp
- debug llc2 errors
- debug llc2 packets
- debug llc2 state
- debug rif
- debug sdlc
- debug token ring

### Note

All `debug` commands that support access list filtering use access lists in the range from 1100 to 1199. The access list numbers shown in the examples are merely samples of valid numbers.
To use the **debug list** command on only the first of several Logical Link Control, type 2 (LLC2) connections, use the **show llc2** command to display the active connections:

```bash
Router# show llc2
SdllcVirtualRing2008 DTE: 4000.2222.22c7 4000.1111.111c 04 04 state NORMAL
SdllcVirtualRing2008 DTE: 4000.2222.22c8 4000.1111.1120 04 04 state NORMAL
SdllcVirtualRing2008 DTE: 4000.2222.22c1 4000.1111.1104 04 04 state NORMAL
```

Next, configure an extended bridging access list, numbered 1103, for the connection you want to filter:

```bash
access-list 1103 permit 4000.1111.111c 0000.0000.0000 4000.2222.22c7 0000.0000.0000 0xC 2 eq 0x404
```

The convention for the LLC **debug list** command filtering is to use dmac = 6 bytes, smac = 6 bytes, dsap_offset = 12, and ssap_offset = 13.

Finally, you invoke the following **debug** commands:

```bash
Router# debug list 1103
Router# debug llc2 packet
LLC2 Packets debugging is on
for access list: 1103
```

To use the **debug list** command for Synchronous Data Link Control (SDLC) connections, with the exception of address 04, create access list 1102 to deny the specific address and permit all others:

```bash
access-list 1102 deny 0000.0000.0000 0000.0000.0000 0000.0000.0000 0000.0000.0000 0xC 1 eq 0x4
access-list 1102 permit 0000.0000.0000 0000.0000.0000 0000.0000.0000 0000.0000.0000 0000.0000.0000
```

The convention is to use dmac = 0.0.0, smac = 0.0.0, and sdlc_frame_offset = 12.

Invoke the following **debug** commands:

```bash
Router# debug list 1102
Router# debug sdlc
SDLC link debugging is on
for access list: 1102
```

To enable SDLC debugging (or debugging for any of the other supported protocols) for a specific interface rather than for all interfaces on a router, use the following commands:

```bash
Router# debug list serial 0
Router# debug sdlc
SDLC link debugging is on
for interface: Serial0
```

To enable Token Ring debugging between two MAC address, 0000.3018.4acd and 0000.30e0.8250, configure an extended bridging access list 1106:

```bash
access-list 1106 permit 0000.3018.4acd 8000.0000.0000 0000.30e0.8250 8000.0000.0000
access-list 1106 permit 0000.30e0.8250 8000.0000.0000 0000.3018.4acd 8000.0000.0000
```

Invoke the following **debug** commands:

```bash
Router# debug list 1106
Router# debug token ring
```
Token Ring Interface debugging is on
for access list: 1106

To enable routing information field (RIF) debugging for a single MAC address, configure an access list 1109:

```
access-list 1109 permit permit 0000.0000.0000 ffff.ffff.ffff 4000.2222.22c6 0000.0000.0000
```

Invoke the following `debug` commands:

```
Router# debug list 1109
Router# debug rif
```

RIF update debugging is on
for access list: 1109

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug llc2 errors</code></td>
<td>Displays LLC2 protocol error conditions or unexpected input.</td>
</tr>
<tr>
<td><code>debug llc2 packet</code></td>
<td>Displays all input and output from the LLC2 protocol stack.</td>
</tr>
<tr>
<td><code>debug llc2 state</code></td>
<td>Displays state transitions of the LLC2 protocol.</td>
</tr>
<tr>
<td><code>debug rif</code></td>
<td>Displays information on entries entering and leaving the RIF cache.</td>
</tr>
<tr>
<td><code>debug rtsp</code></td>
<td>Displays information on SDLC frames received and sent by any router serial interface involved in supporting SDLC end station functions.</td>
</tr>
<tr>
<td><code>debug token ring</code></td>
<td>Displays messages about Token Ring interface activity.</td>
</tr>
</tbody>
</table>
**debug llc2 dynwind**

To display changes to the dynamic window over Frame Relay, use the `debug llc2 dynwind` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug llc2 dynwind
no debug llc2 dynwind
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Examples**

The following is sample output from the `debug llc2 dynwind` command:

```
Router# debug llc2 dynwind
LLC2/DW: BECN received! event REC_I_CMD, Window size reduced to 4
LLC2/DW: 1 consecutive I-frame(s) received without BECN
LLC2/DW: 2 consecutive I-frame(s) received without BECN
LLC2/DW: 3 consecutive I-frame(s) received without BECN
LLC2/DW: 4 consecutive I-frame(s) received without BECN
LLC2/DW: 5 consecutive I-frame(s) received without BECN
LLC2/DW: Current working window size is 5
```

In this example, the router receives a backward explicit congestion notification (BECN) and reduces the window size to 4. After receiving five consecutive I frames without a BECN, the router increases the window size to 5.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug llc2 errors</code></td>
<td>Displays LLC2 protocol error conditions or unexpected input.</td>
</tr>
<tr>
<td><code>debug llc2 packet</code></td>
<td>Displays all input and output from the LLC2 protocol stack.</td>
</tr>
<tr>
<td><code>debug llc2 state</code></td>
<td>Displays state transitions of the LLC2 protocol.</td>
</tr>
</tbody>
</table>
**debug llc2 errors**

To display Logical Link Control, type 2 (LLC2) protocol error conditions or unexpected input, use the `debug llc2 errors` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug llc2 errors
no debug llc2 errors
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Examples**

The following is sample output from the `debug llc2 errors` command from a router ignoring an incorrectly configured device:

```
Router# debug llc2 errors
LLC: admstate: 4000.1014.0001 0000.0000.0000 04 04 REC_RR_RSP
LLC: admstate: 4000.1014.0001 0000.0000.0000 04 04 REC_RR_RSP
LLC: admstate: 4000.1014.0001 0000.0000.0000 04 04 REC_RR_RSP
LLC: admstate: 4000.1014.0001 0000.0000.0000 04 04 REC_RR_RSP
LLC: admstate: 4000.1014.0001 0000.0000.0000 04 04 REC_RR_RSP
LLC: admstate: 4000.1014.0001 0000.0000.0000 04 04 REC_RR_RSP
```

Each line of output contains the remote MAC address, the local MAC address, the remote service access point (SAP), and the local SAP. In this example, the router receives unsolicited RR frames marked as responses.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug list</code></td>
<td>Filters debugging information on a per-interface or per-access list basis.</td>
</tr>
<tr>
<td><code>debug llc2 dynwind</code></td>
<td>Displays changes to the dynamic window over Frame Relay.</td>
</tr>
<tr>
<td><code>debug llc2 packet</code></td>
<td>Displays all input and output from the LLC2 protocol stack.</td>
</tr>
<tr>
<td><code>debug llc2 state</code></td>
<td>Displays state transitions of the LLC2 protocol.</td>
</tr>
</tbody>
</table>
debug llc2 packet

To display all input and output from the Logical Link Control, type 2 (LLC2) protocol stack, use the `debug llc2 packet` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug llc2 packet
no debug llc2 packet
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

This command also displays information about some error conditions as well as internal interactions between the Common Link Services (CLS) layer and the LLC2 layer.

**Examples**

The following is sample output from the `debug llc2 packet` command from the router sending ping data back and forth to another router:

```
Router# debug llc2 packet
LLC: llc2_input
401E54F0: 10400000 .@..
401E5500: 303A90CF 0006F4E1 2A200404 012B5E 0:.ta* ..+
LLC: i REC_RR_CMD N(R)=21 p/f=1
LLC: 0006.F4E1.2a20 0000.303a.90cf 04 04 NORMAL REC_RR_CMD (3)
LLC (rs): 0006.F4E1.2a20 0000.303a.90cf 04 04 REC_RR_CMD N(R)=42
LLC: 0006.F4E1.2a20 0000.303a.90cf 04 04 txmt RR_RSP N(R)=20 p/f=1
LLC: llc_sendframe
401E5610: 0040 0006F4E1 2A200000 .@..ta* ..
401E5620: 303A90CF 04050129 00 N 0:.O...). 2012
LLC: llc_sendframe
4022E3A0: 0040 0006F4E1 .@..ta
4022E3B0: 2A200000 303A90CF 04042A28 2C000202 * ..0:..*(...
4022E3C0: 00050B90 A02E0502 FF0003D1 004006C1 .... ......Q.@.A
4022E3D0: D7C9D5C ...128
C400130A C1D7D7D5 4BD5F2F0 WIUGD...AWWUKUp
4022E3E0: F1F50000 011B6F67 00010860 D7027000 qs....g...W.p.
4022E3F0: 00003B00 1112FF01 03000243 6973636F ........Cisco
4022E400: 20494F53 69 IOSi
LLC: 0006.F4E1.2a20 0000.303a.90cf 04 04 txmt I N(S)=21 N(R)=20 p/f=0 size=90
LLC: llc2_input
401E5620: 10400000 303A90CF 0006F4E1 .@..:0:.0
401E5630: 0006F4E1 2A200404 282C2C00 02020004 ..ta* ..(,...
401E5640: 03002000 1112FF01 03000243 6973636F ........Cisco
401E5650: 20494F53 A0 IOS
LLC: i REC_I_CMD N(R)=22 N(S)=20 V(R)=20 p/f=0
LLC: 0006.F4E1.2a20 0000.303a.90cf 04 04 NORMAL REC_I_CMD (1)
LLC (rs): 0006.F4E1.2a20 0000.303a.90cf 04 04 REC_I_CMD N(S)=20 V(R)=20
LLC (rs): 0006.F4E1.2a20 0000.303a.90cf 04 04 REC_I_CMD N(R)=44
LLC: INFO: 0006.F4E1.2a20 0000.303a.90cf 04 04 v(R) 20
LLC: llc2_input
```

The first three lines indicate that the router has received some input from the link:
ThenextlineindicatesthatthisinputwasanRRcommandwiththepollbitset. Theotherrouterhas receivedsequence number21 and is waiting for the final bit.

LLC: i REC_RR_CMD N(R)=21 p/f=1

The next two lines contain the MAC addresses of the sender and receiver, and the state of the router when it received this frame:

LLC: 0006.f4e1.2a20 0000.303a.90cf 04 04 NORMAL REC_RR_CMD (3)
LLC (rs): 0006.f4e1.2a20 0000.303a.90cf 04 04 REC_RR_CMD N(R)=42

The next four lines indicate that the router is sending a response with the final bit set:

LLC: 0006.f4e1.2a20 0000.303a.90cf 04 04 txmt RR_RSP N(R)=20 p/f=1
LLC: llc_sendframe

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug list</td>
<td>Filters debugging information on a per-interface or per-access list basis.</td>
</tr>
<tr>
<td>debug llc2 dynwind</td>
<td>Displays changes to the dynamic window over Frame Relay.</td>
</tr>
<tr>
<td>debug llc2 errors</td>
<td>Displays LLC2 protocol error conditions or unexpected input.</td>
</tr>
<tr>
<td>debug llc2 state</td>
<td>Displays state transitions of the LLC2 protocol.</td>
</tr>
</tbody>
</table>
**debug llc2 state**

To display state transitions of the Logical Link Control, type 2 (LLC2) protocol, use the `debug llc2 state` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug llc2 state
no debug llc2 state
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

Refer to the ISO/IEC standard 8802-2 for definitions and explanations of `debug llc2 state` command output.

**Examples**

The following is sample output from the `debug llc2 state` command when a router disables and enables an interface:

```
Router# debug llc2 state
LLC (stsw): 0006.f4e1.2a20 0000.303a.90cf 04 04, NORMAL -> AWAIT (P_TIMER_EXP)
LLC(rs): 0006.f4e1.2a20 0000.303a.90cf 04 04, AWAIT -> D_CONN (P_TIMER_EXP)
LLC: cleanup 0006.f4e1.2a20 0000.303a.90cf 04 04, UNKNOWN (17)
LLC (stsw): 0006.f4e1.2a20 0000.303a.90cf 04 04, ADM -> SETUP (CONN_REQ)
LLC: normalstate: set_local_busy 0006.f4e1.2a20 0000.303a.90cf 04 04
LLC (stsw): 0006.f4e1.2a20 0000.303a.90cf 04 04, NORMAL -> BUSY (SET_LOCAL_BUSY)
LLC: Connection established: 0006.f4e1.2a20 0000.303a.90cf 04 04, success
LLC (stsw): 0006.f4e1.2a20 0000.303a.90cf 04 04, SETUP -> BUSY (SET_LOCAL_BUSY)
LLC: busystate: 0006.f4e1.2a20 0000.303a.90cf 04 04 local busy cleared
LLC (stsw): 0006.f4e1.2a20 0000.303a.90cf 04 04, BUSY -> NORMAL (CLEAR_LOCAL_BUSY)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug list</code></td>
<td>Filters debugging information on a per-interface or per-access list basis.</td>
</tr>
<tr>
<td><code>debug llc2 dynwind</code></td>
<td>Displays changes to the dynamic window over Frame Relay.</td>
</tr>
<tr>
<td><code>debug llc2 errors</code></td>
<td>Displays LLC2 protocol error conditions or unexpected input.</td>
</tr>
<tr>
<td><code>debug llc2 packet</code></td>
<td>Displays all input and output from the LLC2 protocol stack.</td>
</tr>
</tbody>
</table>
**debug lnm events**

To display any unusual events that occur on a Token Ring network, use the `debug lnm events` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```plaintext
debug lnm events
no debug lnm events
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

Unusual events include stations reporting errors or error thresholds being exceeded.

**Examples**

The following is sample output from the `debug lnm events` command:

```
Router# debug lnm events
IBMNM3: Adding 0000.3001.1166 to error list
IBMNM3: Station 0000.3001.1166 going into preweight condition
IBMNM3: Station 0000.3001.1166 going into weight condition
IBMNM3: Removing 0000.3001.1166 from error list
LANMGR0: Beaconing is present on the ring
LANMGR0: Ring is no longer beaconing
IBMNM3: Beaconing, Postmortem Started
IBMNM3: Beaconing, heard from 0000.3000.1234
IBMNM3: Beaconing, Postmortem Next Stage
IBMNM3: Beaconing, Postmortem Finished
```

The following message indicates that station 0000.3001.1166 reported errors and has been added to the list of stations reporting errors. This station is located on Ring 3.

```
IBMNM3: Adding 0000.3001.1166 to error list
```

The following message indicates that station 0000.3001.1166 has passed the “early warning” threshold for error counts:

```
IBMNM3: Station 0000.3001.1166 going into preweight condition
```

The following message indicates that station 0000.3001.1166 is experiencing a severe number of errors:

```
IBMNM3: Station 0000.3001.1166 going into weight condition
```

The following message indicates that the error counts for station 0000.3001.1166 have all decayed to zero, so this station is being removed from the list of stations that have reported errors:

```
IBMNM3: Removing 0000.3001.1166 from error list
```

The following message indicates that Ring 0 has entered failure mode. This ring number is assigned internally.

```
LANMGR0: Beaconing is present on the ring
```
The following message indicates that Ring 0 is no longer in failure mode. This ring number is assigned internally.

LANMGR0: Ring is no longer beaconing

The following message indicates that the router is beginning its attempt to determine whether any stations left the ring during the automatic recovery process for the last beaconing failure. The router attempts to contact stations that were part of the fault domain to detect whether they are still operating on the ring.

IBMNM3: Beaconing, Postmortem Started

The following message indicates that the router is attempting to determine whether any stations left the ring during the automatic recovery process for the last beaconing failure. It received a response from station 0000.3000.1234, one of the two stations in the fault domain.

IBMNM3: Beaconing, heard from 0000.3000.1234

The following message indicates that the router is attempting to determine whether any stations left the ring during the automatic recovery process for the last beaconing failure. It is initiating another attempt to contact the two stations in the fault domain.

IBMNM3: Beaconing, Postmortem Next Stage

The following message indicates that the router has attempted to determine whether any stations left the ring during the automatic recovery process for the last beaconing failure. It has successfully heard back from both stations that were part of the fault domain.

IBMNM3: Beaconing, Postmortem Finished

Explanations follow for other messages that the debug lnm events command can generate.

The following message indicates that the router is out of memory:

LANMGR: memory request failed, find_or_build_station()

The following message indicates that Ring 3 is experiencing a large number of errors that cannot be attributed to any individual station:

IBMNM3: Non-isolating error threshold exceeded

The following message indicates that a station (or stations) on Ring 3 is receiving frames faster than they can be processed:

IBMNM3: Adapters experiencing congestion

The following message indicates that the beaconing has lasted for over 1 minute and is considered a “permanent” error:

IBMNM3: Beaconing, permanent

The following message indicates that the beaconing lasted for less than 1 minute. The router is attempting to determine whether either station in the fault domain left the ring.

IBMNM: Beaconing, Destination Started
In the preceding line of output, the following can replace “Started”: “Next State,” “Finished,” “Timed out,” and “Cannot find station n.”
debug lnm llc

To display all communication between the router/bridge and the LAN Network Managers (LNMs) that have connections to it, use the `debug lnm llc` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

`debug lnm llc`  
`no debug lnm llc`

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

One line is displayed for each message sent or received.

**Examples**

The following is sample output from the `debug lnm llc` command:

```
Router# debug lnm llc
IBMNM: Received LRM Set Reporting Point frame from 1000.5ade.0d8a.
IBMNM: found bridge: 001-2-00A, addresses: 0000.3040.a630 4000.3040.a630
IBMNM: Sending LRM LAN Manager Accepted to 1000.5ade.0d8a on link 0.
IBMNM: sending LRM New Reporting Link Established to 1000.5a79.dbf8 on link 1.
IBMNM: Determining new controlling LNM
IBMNM: Sending Report LAN Manager Control Shift to 1000.5ade.0d8a on link 0.
IBMNM: Sending Report LAN Manager Control Shift to 1000.5a79.dbf8 on link 1.
IBMNM: Bridge 001-2-00A received Request Bridge Status from 1000.5ade.0d8a.
IBMNM: Sending Report Bridge Status to 1000.5ade.0d8a on link 0.
IBMNM: Bridge 001-2-00A received Request REM Status from 1000.5ade.0d8a.
IBMNM: Sending Report REM Status to 1000.5ade.0d8a on link 0.
IBMNM: Bridge 001-2-00A received Set Bridge Parameters from 1000.5ade.0d8a.
IBMNM: Sending Bridge Parameters Set to 1000.5ade.0d8a on link 0.
IBMNM: sending Bridge Params Changed Notification to 1000.5a79.dbf8 on link 1.
IBMNM: Bridge 001-2-00A received Set REM Parameters from 1000.5ade.0d8a.
IBMNM: Sending REM Parameters Set to 1000.5ade.0d8a on link 0.
IBMNM: sending REM Parameters Changed Notification to 1000.5a79.dbf8 on link 1.
IBMNM: Bridge 001-2-00A received Set REM Parameters from 1000.5ade.0d8a.
IBMNM: Sending REM Parameters Set to 1000.5ade.0d8a on link 0.
IBMNM: sending REM Parameters Changed Notification to 1000.5a79.dbf8 on link 1.
IBMNM: Received LRM Set Reporting Point frame from 1000.5ade.0d8a.
IBMNM: found bridge: 001-1-00A, addresses: 0000.3080.2d79 4000.3080.2d7
```

As the output indicates, the `debug lnm llc` command output can vary somewhat in format.

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBMNM:</td>
<td>Displays LLC-level debugging information.</td>
</tr>
<tr>
<td>Received</td>
<td>Router received a frame. The other possible value is Sending, to indicate that the router is sending a frame.</td>
</tr>
</tbody>
</table>
The function of the LLC-level software that is communicating as follows:

- CRS--Configuration Report Server
- LBS--LAN Bridge Server
- LRM--LAN Reporting Manager
- REM--Ring Error Monitor
- RPS--Ring Parameter Server
- RS--Ring Station

Name of the specific frame that the router sent or received. Possible values include the following:

- Bridge Counter Report
- Bridge Parameters Changed Notification
- Bridge Parameters Set
- CRS Remove Ring Station
- CRS Report NAUN Change
- CRS Report Station Information
- CRS Request Station Information
- CRS Ring Station Removed
- LRM LAN Manager Accepted
- LRM Set Reporting Point
- New Reporting Link Established
- REM Forward MAC Frame
- REM Parameters Changed Notification
- REM Parameters Set
- Report Bridge Status
- Report LAN Manager Control Shift
- Report REM Status
- Request Bridge Status
- Request REM Status
- Set Bridge Parameters
- Set REM Parameters
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>from 1000.5ade.0d8a</td>
<td>If the router has received the frame, this address is the source address of the frame. If the router is sending the frame, this address is the destination address of the frame.</td>
</tr>
</tbody>
</table>

The following message indicates that the lookup for the bridge with which the LAN Manager was requesting to communicate was successful:

IBMNM: found bridge: 001-2-00A, addresses: 0000.3040.a630 4000.3040.a630

The following message indicates that the connection is being opened:

IBMNM: Opening connection to 1000.5ade.0d8a on TokenRing0

The following message indicates that a LAN Manager has connected or disconnected from an internal bridge and that the router computes which LAN Manager is allowed to change parameters:

IBMNM: Determining new controlling LNM

The following line of output indicates which bridge in the router is the destination for the frame:

IBMNM: Bridge 001-2-00A received Request Bridge Status from 1000.5ade.0d8a.
debug lnm mac

To display all management communication between the router/bridge and all stations on the local Token Rings, use the `debug lnm mac` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
debug lnm mac
no debug lnm mac
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

One line is displayed for each message sent or received.

The following is sample output from the `debug lnm mac` command:

```
Router# debug lnm mac
LANMGR0: RS received request address from 4000.3040.a670.
LANMGR0: RS sending report address to 4000.3040.a670.
LANMGR0: RS received request state from 4000.3040.a670.
LANMGR0: RS sending report state to 4000.3040.a670.
LANMGR0: RS received request attachments from 4000.3040.a670.
LANMGR0: RS sending report attachments to 4000.3040.a670.
LANMGR2: RS received ring purge from 0000.3040.a630.
LANMGR2: CRS received report NAUN change from 0000.3040.a630.
LANMGR2: RS start watching ring poll.
LANMGR0: CRS received report NAUN change from 0000.3040.a630.
LANMGR0: RS start watching ring poll.
LANMGR2: REM received report soft error from 0000.3040.a630.
LANMGR0: REM received report soft error from 0000.3040.a630.
LANMGR2: RS received ring purge from 0000.3040.a630.
LANMGR2: RS received AMP from 0000.3040.a630.
LANMGR2: RS received SMP from 0000.3080.2d79.
LANMGR2: CRS received report NAUN change from 1000.5ade.0d8a.
LANMGR2: RS start watching ring poll.
LANMGR0: RS received ring purge from 0000.3040.a630.
LANMGR0: RS received AMP from 0000.3040.a630.
LANMGR0: RS received SMP from 0000.3080.2d79.
LANMGR0: CRS received report NAUN change from 1000.5ade.0d8a.
LANMGR0: RS start watching ring poll.
LANMGR2: RS received SMP from 1000.5ade.0d8a.
LANMGR2: RPS received request initialization from 1000.5ade.0d8a.
LANMGR2: RPS sending initialize station to 1000.5ade.0d8a.
```

The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LANMGR0:</td>
<td>Indicates that this line of output displays MAC-level debugging information. 0 indicates the number of the Token Ring interface associated with this line of debugging output.</td>
</tr>
</tbody>
</table>
RS | Indicates which function of the MAC-level software is communicating as follows:
   • CRS--Configuration Report Server
   • REM--Ring Error Monitor
   • RPS--Ring Parameter Server
   • RS--Ring Station

RS | Indicates that the router received a frame. The other possible value is sending, to indicate that the router is sending a frame.

received | Indicates the name of the specific frame that the router sent or received. Possible values include the following:
   • AMP
   • initialize station
   • report address
   • report attachments
   • report nearest active upstream neighbor (NAUN) change
   • report soft error
   • report state
   • request address
   • request attachments
   • request initialization
   • request state
   • ring purge
   • SMP

RS | Indicates the source address of the frame, if the router has received the frame. If the router is sending the frame, this address is the destination address of the frame.

from 4000.3040.a670 | Indicates the source address of the frame, if the router has received the frame. If the router is sending the frame, this address is the destination address of the frame.

As the output indicates, all `debug lnm mac` command messages follow the format described in the table above except the following:

LANMGR2: RS start watching ring poll
LANMGR2: RS stop watching ring poll

These messages indicate that the router starts and stops receiving AMP and SMP frames. These frames are used to build a current picture of which stations are on the ring.
**debug local-ack state**

To display the new and the old state conditions whenever there is a state change in the local acknowledgment state machine, use the `debug local-ack state` command in privileged EXEC mode. To disable debugging output, use the `no` form of this command.

```
d debug local-ack state
no debug local-ack state
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Examples**

The following is sample output from the `debug local-ack state` command:

```
Router# debug local-ack state
LACK_STATE: 2370300, hashp 2AE628, old state = disconn, new state = awaiting
   LLC2 open to finish
LACK_STATE: 2370304, hashp 2AE628, old state = awaiting LLC2 open to finish,
   new state = connected
LACK_STATE: 2373816, hashp 2AE628, old state = connected, new state = disconnected
LACK_STATE: 2489548, hashp 2AE628, old state = disconn, new state = awaiting
   LLC2 open to finish
LACK_STATE: 2489548, hashp 2AE628, old state = awaiting LLC2 open to finish,
   new state = connected
LACK_STATE: 2490132, hashp 2AE628, old state = connected, new state = awaiting
   linkdown response
LACK_STATE: 2490140, hashp 2AE628, old state = awaiting linkdown response,
   new state = disconnected
LACK_STATE: 2497640, hashp 2AE628, old state = disconn, new state = awaiting
   LLC2 open to finish
LACK_STATE: 2497644, hashp 2AE628, old state = awaiting LLC2 open to finish,
   new state = connected
```

The table below describes the significant fields shown in the display.

**Table 101: debug local-ack state Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LACK_STATE:</td>
<td>Indicates that this packet describes a state change in the local acknowledgment state machine.</td>
</tr>
<tr>
<td>2370300</td>
<td>System clock.</td>
</tr>
<tr>
<td>hashp 2AE628</td>
<td>Internal control block pointer used by technical support staff for debugging purposes.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>old state = disconn</td>
<td>Old state condition in the local acknowledgment state machine. Possible values include the following:</td>
</tr>
<tr>
<td></td>
<td>• Disconn (disconnected)</td>
</tr>
<tr>
<td></td>
<td>• awaiting LLC2 open to finish</td>
</tr>
<tr>
<td></td>
<td>• connected</td>
</tr>
<tr>
<td></td>
<td>• awaiting linkdown response</td>
</tr>
<tr>
<td>new state = awaiting LLC2 open to finish</td>
<td>New state condition in the local acknowledgment state machine. Possible values include the following:</td>
</tr>
<tr>
<td></td>
<td>• Disconn (disconnected)</td>
</tr>
<tr>
<td></td>
<td>• awaiting LLC2 open to finish</td>
</tr>
<tr>
<td></td>
<td>• connected</td>
</tr>
<tr>
<td></td>
<td>• awaiting linkdown response</td>
</tr>
</tbody>
</table>
debug local-ack state