



Monitoring of Modem Call Status

Last Updated: December 4, 2012

This appendix describes configuration for modem call status. Modem call status provides monitoring and maintaining of modem calls at digital signal level zero (DS-0), the PRI bearer channel level, and the modem level.

- [Finding Feature Information, page 1](#)
- [Prerequisites for Configuring Modem Call Status, page 1](#)
- [Information about Modem Call Status, page 2](#)
- [Configuring Modem Call Status, page 3](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Modem Call Status

Before configuring your access server or gateway to enable monitoring of modem call status, perform the following tasks:

- Install the SNMP manager on your workstation.
- Configure the SNMP agent on the access server with the following commands:

```
snmp-server
community

public
RO
snmp-server
host
```



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

10.1.2.3
public

Information about Modem Call Status

Modem call status is supported by:

- The generation of DS-0 busyout traps
- The generation of ISDN PRI-requested channel-not-available traps
- The generation of modem health traps
- Using the **show controllers** command
- DS-1 loopback traps

Monitoring and maintaining of modem call status offers the following benefits:

- Improved visibility into the line status of the access server for comprehensive status monitoring and notification capability
- Improved troubleshooting and diagnostics for large dial networks

DS-0 Busyout Traps

A DS-0 busyout trap is generated when one of the following conditions is met:

- A request occurs to busy out a DS-0
- A busyout is complete and the DS-0 is out of service
- A request occurs to take a DS-0 out of busyout mode

DS-0 busyout traps are generated at the DS-0 level for channel-associated signalling (CAS) and ISDN configured lines.

ISDN PRI-Requested Channel-Not-Available Traps

ISDN PRI-requested channel-not-available traps are generated when a requested DS-0 channel is not available or when there is no modem available to take an incoming call. This feature is available only on ISDN PRI interfaces.

Modem Health Traps

Modem health traps are generated when a modem port is bad, disabled, reflashed, or shut down, or when there is a request to busy out the modem.

show controllers timeslots Command

The **show controllers** command, with the keyword **timeslots**, displays the channel state in detail. This command shows whether the DS-0 channels of a particular controller are in idle, in-service, maintenance, or busyout states. The **show controllers** command applies to both CAS and ISDN PRI interfaces.

DS-1 Loopback Traps

DS-1 loopback traps are generated when a DS-1 line goes into loopback mode.

Configuring Modem Call Status

To configure modem call status on your access server or gateway, perform the following tasks, all of which are optional:



Note

For a complete description of the commands, refer to the Cisco IOS Voice, Video, and Fax Command Reference. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

- [Enabling DS-0 Busyout Traps, page 3](#)
- [Enabling ISDN PRI-Requested Channel-Not-Available Traps, page 3](#)
- [Enabling Modem Health Traps, page 4](#)
- [Enabling DS-1 Loopback Traps, page 4](#)
- [Verifying Enabled Traps, page 4](#)
- [Troubleshooting Enabled Traps, page 4](#)
- [Modem Call Status Configuration Example, page 5](#)

Enabling DS-0 Busyout Traps

To generate DS-0 busyout traps, use the following command in global configuration mode:

Command	Purpose
Router(config)# snmp-server enable traps ds0-busyout	Generates a trap when there is a request to busy out a DS-0 or when busyout finishes. DS-0 busyout traps are disabled by default. The ds0-busyout keyword specifies that DS-0 busyout traps be enabled.

Enabling ISDN PRI-Requested Channel-Not-Available Traps

To generate ISDN PRI-requested channel-not-available traps, use the following command in global configuration mode:

Command	Purpose
Router(config)# snmp-server enable traps isdn chan-not-avail	Generates a trap when the network access server (NAS) rejects an incoming call on an ISDN PRI interface because the channel is not available. ISDN PRI-requested channel-not-available traps are disabled by default. The isdn chan-not-avail keywords specify that ISDN PRI-requested channel-not-available traps be enabled.

Enabling Modem Health Traps

To generate modem health traps, use the following command in global configuration mode:

Command	Purpose
Router(config)# snmp-server enable traps modem-health	Generates a trap when a modem port is bad, disabled, or downloading firmware; when a download fails; when a modem is placed in loopback mode for maintenance; or when there is a request to busy out the modem. Modem health traps are disabled by default. The modem-health keyword specifies that modem health traps be enabled.

Enabling DS-1 Loopback Traps

To generate DS-1 loopback traps, use the following command in global configuration mode:

Command	Purpose
Router(config)# snmp-server enable traps ds1-loopback	Generates a trap when the DS-1 line goes into loopback mode. DS-1 loopback traps are disabled by default. The ds1-loopback keyword specifies that DS-1 loopback traps be enabled.

Verifying Enabled Traps

Use the **show running-config** command to verify that the traps are enabled. The following output indicates that all the traps are enabled:

```
.
Router(config)# show running-config
snmp-server enable traps ds0-busyout
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps modem-health
snmp-server enable traps ds1-loopback
.
```

Troubleshooting Enabled Traps

To troubleshoot the traps, enable debugging for SNMP packets by entering the **debug snmp packets** command in privileged EXEC mode. Check the resulting output to see that the SNMP trap information packet is being sent. The output will vary according to the kind of packet sent or received.

The following example shows the **debug snmp packets** command followed by an excerpt from the debug output. The first and last lines of the sample output show SNMP trap packets that have been sent and received.

```
Router# debug snmp packets
SNMP: Packet received via UDP from 10.5.4.1 on Ethernet0
```

```

SNMP: Get-next request, reqid 23584, errstat 0, erridx 0
sysUpTime = NULL TYPE/VALUE
system.1 = NULL TYPE/VALUE
system.6 = NULL TYPE/VALUE
SNMP: Response, reqid 23584, errstat 0, erridx 0
sysUpTime.0 = 2217027
system.1.0 = Cisco Internetwork Operating System Software
system.6.0 =
SNMP: Packet sent via UDP to 10.5.4.1

```

You can also use trap monitoring and logging tools such as **snmptrapd** with debugging flags turned on to monitor output.

Modem Call Status Configuration Example

The following example shows modem call status configured with DS-0 busyout traps enabled:

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
aaa new-model
aaa authentication ppp default group radius
enable password <password>
!
spe 1/0 1/7
firmware location system:/ucode/mica_port_firmware
spe 2/0 2/7
firmware location system:/ucode/mica_port_firmware
!
resource-pool disable
!
clock timezone PDT -8
clock calendar-valid
no modem fast-answer
modem country mica usa
modem link-info poll time 60
modem buffer-size 300
ip subnet-zero
!
isdn switch-type primary-5ess
isdn voice-call-failure 0
!
controller T1 0
framing esf
clock source line primary
linecode b8zs
pri-group timeslots 1-24
!
controller T1 1
framing esf
linecode b8zs
ds0-group 0 timeslots 1-24 type e&m-fgb
cas-custom 0
!
interface Loopback0
ip address 10.5.4.1
!
interface Ethernet0
no ip address
shutdown
!
interface Serial0
no ip address
shutdown
!
interface Serial1
no ip address

```

```

shutdown
!
interface Serial0:23
no ip address
ip mroute-cache
isdn switch-type primary-5ess
isdn incoming-voice modem
no cdp enable
!
interface FastEthernet0
ip address 10.5.4.1
duplex full
speed auto
no cdp enable
!
interface Group-Async1
ip unnumbered FastEthernet0
encapsulation ppp
ip tcp header-compression passive
no ip mroute-cache
async mode interactive
peer default ip address pool swattest
no fair-queue
ppp authentication chap
ppp multilink
group-range 1 192
!
interface Dialer1
ip unnumbered FastEthernet0
encapsulation ppp
ip tcp header-compression passive
dialer-group 1
peer default ip address pool swattest
pulse-time 0
no cdp enable
!
ip local pool swattest 10.5.4.1
ip default-gateway 10.5.4.1
ip classless
!
dialer-list 1 protocol ip permit
snmp-server engineID local 00000000DDDDDDDDFFFFFFFF
snmp-server community public RO
snmp-server packetize 2048
snmp-server enable traps pop
snmp-server host 10.5.4.1 public
!
radius-server host 10.5.4.1 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key <password>
!
line con 0
transport input none
line 1 192
autoselect ppp
modem InOut
transport preferred none
transport input all
transport output none
line aux 0
line vty 0 4
end

```

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.