

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[How Do I Find Out What Traps Are Enabled on My Switch?](#)

[How Do I Configure the SNMP Trap Receiver on the Switch?](#)

[How Do I Enable Traps on the Switch, and What Does Each Trap Mean?](#)

[Syntax](#)

[Syntax Description](#)

[How Do I Enable Traps on Individual Ports, Such as linkUp/linkDown?](#)

[Syntax](#)

[Syntax Description](#)

[Example](#)

[What Other Traps Can the Catalyst Switch Send?](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes the traps that the Catalyst OS (CatOS) supports and how to configure them on the switch.

Trap operations allow Simple Network Management Protocol (SNMP) agents to send asynchronous notifications of the occurrence of an event. Traps are sent on a best-effort basis and without any method to verify their receipt.

Prerequisites

Requirements

Cisco recommends that b

Note: Refer to [How to Configure SNMP Community Strings](#) for more information.

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst 4500/4000, 5500/5000, and 6500/6000 series switches
- CatOS version 7.3

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

How Do I Find Out What Traps Are Enabled on My Switch?

Issue the **show snmp** command in the enable mode. Here is a sample output:

```
6509 (enable) show snmp

RMON:                               Enabled
Extended RMON Netflow Enabled : None.
Traps Enabled:
Port,Module,Chassis,Bridge,Repeater,Vtp,Auth,ippermit,Vmps,config,entity,stpx,syslog
Port Traps Enabled: 2/1-2,3/1-48,4/1-8

Community-Access      Community-String
....
....
!--- Output suppressed.
```

How Do I Configure the SNMP Trap Receiver on the Switch?

Issue the command **set snmp trap host string** .

Note: The command syntax includes:

- host - IP address or IP alias of the system to receive SNMP traps.
- string - Community string to use in order to send authentication traps.

Here is an example:

```
6509 (enable) set snmp trap 1.1.1.1 public
SNMP trap receiver added.
```

Issue the **show snmp** command in order to verify the addition of this **set snmp trap** statement. Here is a sample output:

```
6509 (enable) show snmp
6509 (enable) show snmp
RMON:                               Enabled
Extended RMON Netflow Enabled : None.
!--- Output suppressed. .... !--- Output suppressed. Trap-Rec-Address  Trap-Rec-Community
-----
1.1.1.1                               public
```

How Do I Enable Traps on the Switch, and What Does Each Trap Mean?

Issue the **set snmp trap** command in order to enable or disable the different SNMP traps on the system. The command also adds an entry into the SNMP authentication trap receiver table.

Syntax

```
set snmp trap {enable | disable} [all | auth | bridge | chassis | config | entity | entityfru |
envfan | envpower | envshutdown | ippermit | module | repeater | stpx | syslog | system |
```

vmps | vtp]

Note: *one line.*

Syntax Description

Keyword	Description	Trap
enable	Keyword to enable SNMP traps.	
disable	Keyword to disable SNMP traps.	
all	(Optional) Keyword to specify all trap types. Refer to the switch documentation before you use this option.	
auth	(Optional) Keyword to specify the authenticationFailure trap from RFC 1157  .	authenticationFailure (.1.3.6.1.2.1.11.0.4)
bridge	(Optional) Keyword to specify the newRoot and topologyChange traps from RFC 1493  . Refer to BRIDGE-MIB .	newRoot (.1.3.6.1.2.1.17.0.1) topologyChange (.1.3.6.1.2.1.17.0.2)
chassis	(Optional) Keyword to specify the chassisAlarmOn (.1.3.6.1.4.1.9.5.0.5) and chassisAlarmOff (.1.3.6.1.4.1.9.5.0.6) traps from the CISCO-STACK-MIB .	chassisAlarmOn (.1.3.6.1.4.1.9.5.0.5) chassisAlarmOff (.1.3.6.1.4.1.9.5.0.6)
config	(Optional) Keyword to specify the sysConfigChange trap from the CISCO-STACK-MIB .	sysConfigChangeTrap (.1.3.6.1.4.1.9.5.0.9)
entity	(Optional) Keyword to specify the entityMIB trap from the ENTITY-MIB .	entConfigChange (.1.3.6.1.2.1.47.2.0.1)
entityfru	(Optional) Keyword to specify the entity FRU.	cefcModuleStatusChange (.1.3.6.1.4.1.9.9.117.2.0.1) cefcPowerStatusChange (.1.3.6.1.4.1.9.9.117.2.0.2) cefcFRUInserted (.1.3.6.1.4.1.9.9.117.2.0.3) cefcFRURemoved (.1.3.6.1.4.1.9.9.117.2.0.4)
envfan	(Optional) Keyword to specify the environmental fan.	ciscoEnvMonFanNotification (.1.3.6.1.4.1.9.9.13.3.0.4)
envpower	(Optional) Keyword to specify the environmental power.	ciscoEnvMonRedundantSupplyNotification (.1.3.6.1.4.1.9.9.13.3.0.5)
envshutdown	(Optional) Keyword to specify the environmental shutdown.	ciscoEnvMonShutdownNotification (.1.3.6.1.4.1.9.9.13.3.0.1)
envtemp	(Optional) Keyword to specify the environmental temperature notification.	ciscoEnvMonTemperatureNotification (.1.3.6.1.4.1.9.9.13.3.0.3)
ippermit	(Optional) Keyword to specify the IP Permit Denied access from the CISCO-STACK-MIB .	ipPermitDeniedTrap (.1.3.6.1.4.1.9.5.0.7)

macnotification	(Optional) Keyword that specifies MAC address notification.	cmnMacChangedNotification (.1.3.6.1.4.1.9.9.215.2.0.1)
module	(Optional) Keyword to specify the <code>moduleUp</code> and <code>moduleDown</code> traps from the CISCO-STACK-MIB .	<code>moduleUp</code> (.1.3.6.1.4.1.9.5.0.3) <code>moduleDown</code> (.1.3.6.1.4.1.9.5.0.4)
repeater	(Optional) Keyword to specify the <code>rpPtrHealth</code> , <code>rpPtrGroupChange</code> , and <code>rpPtrResetEvent</code> traps from RFC 1516 ¹ . Refer to SNMP-REPEATER-MIB .	<code>rpPtrHealth</code> (.1.3.6.1.2.1.22.0.1) <code>rpPtrGroupChange</code> (.1.3.6.1.2.1.22.0.2) <code>rpPtrResetEvent</code> (.1.3.6.1.2.1.22.0.3)
stpX	(Optional) Keyword to specify the STPX trap.	<code>stpXInconsistencyUpdate</code> (.1.3.6.1.4.1.9.9.82.2.0.1) <code>stpXLoopInconsistencyUpdate</code> (.1.3.6.1.4.1.9.9.82.2.0.3) <code>stpXRootInconsistencyUpdate</code> (.1.3.6.1.4.1.9.9.82.2.0.2)
syslog	(Optional) Keyword to specify the syslog notification traps.	<code>clogMessageGenerated</code> (.1.3.6.1.4.1.9.9.41.2.0.1)
system	(Optional) Keyword to specify the system.	<code>ciscoSystemClockChanged</code> (1.3.6.1.4.1.9.9.131.2.0.1)
vmPs	(Optional) Keyword to specify the <code>vmVmPsChange</code> trap from the CISCO-VLAN-MEMBERSHIP-MIB .	<code>vmVmPsChange</code> (.1.3.6.1.4.1.9.9.68.2.0.1)
vtp	(Optional) Keyword to specify the VTP from the CISCO-VTP-MIB .	<code>vtpConfigDigestError</code> (.1.3.6.1.4.1.9.9.46.2.0.2) <code>vtpConfigRevNumberError</code> (.1.3.6.1.4.1.9.9.46.2.0.1) <code>vlanTrunkPortDynamicStatusChange</code> (.1.3.6.1.4.1.9.9.46.2.0.7) <code>vtpVersionOneDeviceDetected</code> (.1.3.6.1.4.1.9.9.46.2.0.6)

¹ FRU = field-replaceable unit

² STPX = Spanning Tree Protocol Extensions

³ VTP = VLAN Trunk Protocol

How Do I Enable Traps on Individual Ports, Such as linkUp/linkDown?

Issue the **set port trap** command in order to enable or disable the operation of the standard SNMP link trap for a port or range of ports. By default, all port traps are disabled.

Note: The Network Analysis Module (NAM) does not support this command.

Syntax

set port trap *mod/port* {enable | disable}

Syntax Description

- **mod/port**- Number of the module and the port on the module.
- **enable** - Keyword to activate the SNMP link trap.
- **disable** - Keyword to deactivate the SNMP link trap.

If you enable the traps, the corresponding traps that generate are `linkUp` (.1.3.6.1.2.1.11.0.3) and `linkDown` (.1.3.6.1.2.1.11.0.2). These traps are from the [IF-MIB](#).

Example

This example shows how to enable the SNMP link trap for module 1, port 2:

```
Console> (enable) set port trap 1/2 enable
Port 1/2 up/down trap enabled.
Console> (enable)
```

What Other Traps Can the Catalyst Switch Send?

See this table:

MIB Object Name	OID	MIB
ciscoFlashCopyCompletionTrap	.1.3.6.1.4.1.9.9.10.1.3.0.1	CISCO-FLASH-MIB
ciscoFlashDeviceChangeTrap	.1.3.6.1.4.1.9.9.10.1.3.0.4	CISCO-FLASH-MIB
ciscoFlashMiscOpCompletionTrap	.1.3.6.1.4.1.9.9.10.1.3.0.3	CISCO-FLASH-MIB
coldStart	.1.3.6.1.6.3.1.1.5.1	RFC 1157-SNMP ↗ (SNMPv2-MIB)
warmStart	.1.3.6.1.6.3.1.1.5.2	RFC 1157-SNMP ↗ (SNMPv2-MIB)
tokenRingSoftErrExceededTrap	.1.3.6.1.4.1.9.5.0.10	CISCO-STACK-MIB
lerAlarmOn	.1.3.6.1.4.1.9.5.0.1	CISCO-STACK-MIB
lerAlarmOff	.1.3.6.1.4.1.9.5.0.2	CISCO-STACK-MIB
entSensorThresholdNotification	.1.3.6.1.4.1.9.9.91.2.0.1	CISCO-ENTITY-SENSOR-MIB
fallingAlarm	.1.3.6.1.2.1.16.0.2	RMON-MIB
risingAlarm	.1.3.6.1.2.1.16.0.1	RMON-MIB

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [Cisco Products & Services - Switches](#)
- [Cisco IOS SNMP Traps Supported and How to Configure Them](#)
- [IP Application Services Configuration Examples and TechNotes](#)
- [Network Management Software Downloads - MIBs](#) ([registered](#) customers only)

- [LAN Switching Support Page](#)
- [Technical Support & Documentation - Cisco Systems](#)