# Configurar armadilhas de SNMP do IOS suportadas

## Contents



## Introduction

Este documento descreve como configurar Traps Cisco SNMP suportados.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

Você não deseja que um dispositivo da Cisco envie todas as interceptações SNMP que o dispositivo sabe enviar. Por exemplo, quando você ativa todas as interceptações em um servidor de acesso remoto com 64 linhas de discagem, recebe uma interceptação sempre que um usuário faz uma chamada e sempre que um usuário encerra a conexão. Isso cria um excesso de desvios. O software Cisco IOS® define grupos de interceptações que podem ser ativados ou desativados. Existem dois comandos de configuração global que você usa para configurar interceptações

SNMP em um dispositivo de Software Cisco IOS:

- **snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port] [notification-type]**
  Execute o snmp-server host global configuration para especificar o destinatário de uma operação de notificação SNMP. Execute o **no** forma desse comando para remover o host especificado.

- **snmp-server enable traps [notification-type] [notification-option]**
  Execute o**snmp-server enable traps global configuration**para permitir que o roteador envie interceptações SNMP (traps). Execute o **no** deste comando para desabilitar as notificações de SNMP.

Os tipos de armadilhas podem ser especificados nos dois comandos. Você deve emitir o comando **snmp-server host< /strong>** para definir os Sistemas de Gerenciamento de Rede para onde as interceptações devem ser enviadas. Especifique os tipos de interceptação se não quiser que todas elas sejam enviadas. Emitir vários **snmp-server enable traps** , um para cada um dos tipos de interceptação usados no **snmp host** comando.

> **Observação**: nem todos [*notification-type*] opções são suportadas em ambos os comandos. Por exemplo, [*notification-type*] x25 e teletype (tty) não são usados para **snmp-server enable trap** As interceptações x25 e tty são ativadas como padrão.

Por exemplo, emita estes comandos para fazer uma configuração somente de relatório de dispositivo do Cisco IOS Software, Border Gateway Protocol (BGP) e traps tty para o Network Management System 10.10.10.10:

```
snmp-server host 10.10.10.10 public config bgp tty
snmp-server enable traps config
snmp-server enable traps bgp
```

### Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

### Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

## Informações de Apoio

> **Observação**: o Cisco IOS Software Release 12.1(3)T foi usado para preparar este documento. Quando se utiliza uma versão anterior do software Cisco IOS, nem todas as opções são suportadas. Ao usar uma versão posterior à 12.1(3)T do Cisco IOS Software,

opções adicionais [notification-type] podem ser suportadas. Neste documento, você pode encontrar uma lista atual de todos os Identificadores de Objetos (OIDs) de armadilha de Protocolo Simples de Gerenciamento de Rede (SNMP) suportados pelo software Cisco IOS.

Os dispositivos Cisco que executam o Cisco IOS Software padrão (roteadores, switches de Modo de Transferência Assíncrono (ATM - Asynchronous Transfer Mode) e Servidores de Acesso Remoto) podem gerar muitas interceptações SNMP.

# Comandos

## O snmp-server host Comando

Execute o **snmp-server host global configuration** para especificar o destinatário de uma operação de notificação SNMP. Execute o **no** forma desse comando para remover o host especificado.

```
snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}]
community-string [udp-port port] [notification-type] no snmp-server host host [traps | informs]
```

## Descrição da sintaxe

| | |
|---|---|
| host-addr | O nome ou o endereço da Internet do host (o destinatário desejado). |
| **traps** | (Opcional) Envie armadilhas SNMP para esse host. Esse é o padrão. |
| **informs** | (Opcional) Envie instruções de SNMP para esse host. |
| **version** | (Opcional) A versão do SNMP usada para enviar as interceptações. A versão 3 é o modelo mais seguro, pois permite a criptografia de pacotes com o **priv** palavra-chave. Se você usar palavra-chave de versão, especifique uma destas opções:<br>• 1 — SNMPv1. Esta opção não está disponível nos informativos.<br>• 2c — SNMPv2C<br>• 3 — SNMPv3. Essas três palavras-chave opcionais podem ser depois da palavra-chav version 3: **auth**(Opcional) Habilita a autenticação de pacotes Message Digest 5 (MD5) e Secure Hash Algorithm (SHA).**noauth** (Padrão) O nível de segurança noAuthNoPriv. Ess o padrão se [auth \| noauth A opção de palavra-chave \| priv] não foi especificada.**priv** (Opcional) Ativa a criptografia de pacotes DES (Data Encryption Standard) (também chamada de "privacidade"). |
| *community-string* | A sequência de comunidade em forma de senha enviada com a operação de notificação. Embora você possa definir essa string com o comando **snmp-server host** sozinho, a Cisco recomenda que você defina essa string com o comando **snmp-server community** antes de execu o comando **snmp-server host** comando. |
| **udp-port***port* | Porta User Datagram Protocol (UDP) do host a ser usado. O padrão é 162. |
| tipo de notificação | (Opcional) O tipo de notificação a ser enviada ao host. Se nenhum tipo for especificado, toc as notificações serão enviadas. O tipo de notificação pode ser uma ou mais dessas palavra chave:<br>• **aaa-server** —Envia notificações de AAA.<br>• **bgp** —Envio de notificações de alteração de estado do BGP (protocolo de gateway limit externo).<br>• **bstun**—Envia notificações de Block Serial Tunneling (BSTUN).<br>• **calltracker**—Envia notificações do CallTracker.<br>• **config**—Envia notificações de configuração |

- **dlsw**—Envia notificações de Switching de Enlace de Dados (DLSw).
- **ds0-busyout**—Envia notificações ds0-busyout.
- **ds1-loopback**—Envia notificações ds1-loopback.
- **dspu**—Envia notificações da unidade física de downstream (DSPU).
- **dsp**—Envia notificações de processamento de sinal digital (DSP).
- **entity**—Envia notificações de modificação MIB (Base de Informações de Gerenciamento entidade.
- **envmon**—Envia notificações empreendimento-específicas do monitor ambiental Cisco quando um limiar ambiental for excedido.
- **frame-relay**—Envia notificações de Frame Relay
- **hsrp**—Envia notificações do Hot Standby Router Protocol (HSRP).
- **isdn**—Envia notificações de ISDN (rede digital de serviços integrados).
- **msdp**—Envia notificações MSDP (Protocolo de Descoberta de Origem de Transmissão Múltipla).
- **llc2**—Envia notificações LLC2 (Logical Link Control, controle lógico de link) tipo 2.
- **repeater**—Envia notificações de repetidor padrão (hub).
- **rsrb**—Envia notificações de Remote Source-Route Bridging (RSRB).
- **rsvp**—Envia notificações de RSVP (protocolo de reservas de recursos).
- **rtr**—Envia notificações do SA Agent (RTR).
- **sdlc**—Envia notificações SDLC (controle sincronizado de circuitos de dados).
- **snmp**—Envia notificações do Simple Network Management Protocol (SNMP) (conforme definido no RFC 1157).
- **stun**—Envia notificações de túnel serial (STUN).
- **syslog**—Envia notificações de mensagem de erro (Cisco Syslog MIB). Especifique o nív mensagens a serem enviadas com o comando**logging history level**comando.
- **tty**—Envia notificações empreendimento-específicas da Cisco quando a conexão do protocolo TCP é fechada.
- **voice**—Envia notificações de voz.
- **x25**—Envia notificações de eventos X.25.
- **xgcp**—Envia notificações de Protocolo de Controle de Gateway de Mídia Externo (XGCP

# Defaults

O **snmp-server host** está desabilitado por padrão. Não são enviadas notificações.

Se você introduzir este comando sem palavras-chave, o padrão é enviar todos os tipos de desvio para o host.

Nenhuma instrução é enviada para este host. Se não **version** palavra-chave estiver presente, o padrão é a versão 1. O **no snmp-server host** sem palavras-chave desativa interceptações, mas não informações, para o host. Execute o **no snmp-server host informs** para desativar as informações.

> **Observação**: se a *community-string* não está definido com o **snmp-server community** antes de usar esse comando, a forma padrão do comando **snmp-server community** é automaticamente inserido na configuração. A senha (*community-string*) usado para esta configuração automática do **snmp-server community** é igual ao especificado no **snmp-server host** comando. Esse é o comportamento padrão do Cisco IOS Software Release 12.0(3) e posterior.

# Modos de comando

## Configuração global – Histórico de comandos

| Versão do Cisco IOS Software | Modificação |
|---|---|
| 10.0 | Comando introduzido. |
| 12.0(3)T | Essas palavras-chave foram adicionadas:<br>• **version 3 [auth \| noauth \| priv]**<br>• **hsrp** |

## Utilize as diretrizes

Notificações SNMP podem ser enviadas como armadilhas ou com solicitações de informação. As interceptações não são confiáveis porque o receptor não envia confirmações, quando elas são recebidas por este dispositivo. O remetente não pode determinar se as armadilhas foram recebidas. No entanto, uma entidade SNMP que recebe uma solicitação de instrução confirma a mensagem com uma unidade de dados de protocolo (PDU) de resposta de SNMP. Se o remetente nunca recebe a resposta, a solicitação de instrução pode ser enviada novamente. Portanto, as instruções têm maior probabilidade de alcançar o destino pretendido.

Entretanto, as informações consomem muitos recursos no agente e na rede. Diferente de um desvio, que é descartado assim que enviado, uma solicitação de informações deve ser mantida na memória até que uma resposta seja recebida ou a solicitação expire. As interceptações são enviadas somente uma vez, e as instruções podem ser enviadas várias vezes. As novas tentativas aumentam o tráfego e contribuem para uma carga adicional maior na rede.

Se você não inserir um **snmp-server host** não serão enviadas notificações. Para configurar o roteador para enviar notificações SNMP, você deve inserir pelo menos um **snmp-server host** comando. Se você inserir o comando sem palavras-chave, todos os tipos de interceptação serão ativados para o host.

Para habilitar vários hosts, você deve emitir um comando **snmp-server host** para cada host. Você pode especificar vários tipos de notificações no comando para cada host.

Quando vários **snmp-server host** são fornecidos comandos para o mesmo host e tipo de notificação (interceptar ou informar), cada comando substitui o comando anterior. Somente os últimos **snmp-server host** é levado em conta. Por exemplo, se você inserir um snmp-server host inform para um host e depois insira outro **snmp-server host inform** para o mesmo host, o segundo comando substitui o primeiro.

O **snmp-server host** é usado em conjunto com o comando **snmp-server enable** comando. Execute o **snmp-server enable** para especificar quais notificações SNMP são enviadas globalmente. Para que um host receba a maioria das notificações, pelo menos uma **snmp-server enable** e o comando **snmp-server host** para esse host deve ser habilitado.

No entanto, alguns tipos de notificação não podem ser controlados com o comando **snmp-server enable** comando. Por exemplo, alguns tipos de notificação estão sempre habilitados. Outros tipos de notificação são ativados por um comando diferente. Por exemplo, o `linkUpDown` as notificações são controladas pelo **snmp trap link-status** comando. Esses tipos de notificação não exigem uma **snmp-server enable** comando.

A disponibilidade de uma opção notification-type depende do tipo de roteador e dos recursos do

software Cisco IOS compatíveis com o roteador. Por exemplo, o **envmon** o tipo de notificação estará disponível apenas se o monitor ambiental fizer parte do sistema.

## Configurar Informações

Siga estas etapas para enviar instruções:

1. Configure um ID de mecanismo remoto.
2. Configure um usuário remoto.
3. Configure um grupo em um dispositivo remoto.
4. Habilitar armadilhas no dispositivo remoto.
5. Ative o gerenciador de SNMP.

## Examples

Se você quiser configurar uma sequência de comunidade SNMP exclusiva para interceptações, mas quiser impedir o acesso de sondagem de SNMP com essa cadeia, a configuração deverá incluir uma lista de acesso. Neste exemplo, a sequência de comunidade chama-se "comaccess" e a lista de acesso é numerada como 10:

```
snmp-server community comaccess ro 10
snmp-server host 172.20.2.160 comaccess
access-list 10 deny any
```

Este exemplo envia as interceptações SNMP para o host especificado pelo nome myhost.cisco.com. A série de comunidade é definida como comaccess:

```
snmp-server enable traps
snmp-server host myhost.cisco.com comaccess snmp
```

Este exemplo envia as interceptações específicas de empresas do monitoramento ambiental do SNMP e da Cisco para o endereço 172.30.2.160:

```
snmp-server enable traps
snmp-server host 172.30.2.160 public snmp envmon
```

Este exemplo permite que o roteador envie todas as interceptações para o host myhost.cisco.com, com a sequência de comunidade pública:

```
snmp-server enable traps
snmp-server host myhost.cisco.com public
```

Este exemplo não envia interceptações para qualquer host. Os desvios do BGP são ativados para todos os hosts, porém somente os desvios da ISDN estão habilitados para serem enviados a um host.

```
snmp-server enable traps bgp
snmp-server host bob public isdn
```

Este exemplo permite que o roteador envie todas as solicitações de informação ao host myhost.cisco.com com a sequência de comunidade pública:

```
snmp-server enable traps
snmp-server host myhost.cisco.com informs version
```

Este exemplo envia as interceptações HSRP SNMPv2c para o host especificado pelo nome myhost.cisco.com. A série de comunidade está definida como pública.

```
snmp-server enable traps
snmp-server host myhost.cisco.com traps version 2c public hsrp
```

# O snmp-server enable traps Comando

Use o **snmp-server enable traps** global configuration para permitir que o roteador envie interceptações SNMP. Use o **no** forma desse comando para desabilitar as notificações de SNMP.

```
snmp-server enable traps [notification-type] [notification-option]

no snmp-server enable traps [notification-type] [notification-option]
```

## Descrição da sintaxe

*tipo de notificação*

(Opcional) O tipo de notificação para ativar. Se nenhum tipo for especificado, todas as notifica serão enviadas (incluindo o **envmon** e **repeater** notificações). O tipo de notificação pode ser uma dessas palavras-chave:

- **aaa-server**—Envia notificações do servidor AAA. Essa palavra-chave é adicionada desde a versão 12.1(3)T do Software Cisco IOS para as plataformas Cisco AS5300 e AS5800 somente. Proveniente de CISCO-AAA-SERVER-MIB e as notificações são: enterprise 1.3.6.1.4.1.9.10.56.2 1 casServerStateChange
- **bgp** —Envio de notificações de alteração de estado do BGP (protocolo de gateway limite externo). Proveniente de BGP4-MIB, e as notificações são: enterprise 1.3.6.1.2.1.15.7 1 bgpEstablished 2 bgpBackwardTransition
- **calltracker** —Envia uma notificação sempre que uma nova entrada de chamada ativa é cria em cctActiveTable ou uma nova entrada de chamada histórica é criada em cctHistoryTab Proveniente de CISCO-CALL-TRACKER-MIB, e as notificações são: enterprise 1.3.6.1.4.1.9.9.163.2 1 cctCallSetupNotification 2 cctCallTerminateNotification
- **config** —Envia notificações de configuração Proveniente de CISCO-CONFIG-MAN-MIB, e notificações são: enterprise 1.3.6.1.4.1.9.9.43.2 1 ciscoConfigManEvent
- **dial** —Envia uma notificação sempre que uma chamada bem-sucedida é eliminada, uma tentativa de chamada com falha é determinada como falha final ou sempre que uma mensagem de configuração de chamada é recebida ou enviada. Proveniente de DIAL-CONTROL-MIB, e as notificações são: enterprise 1.3.6.1.2.1.10.21.2 1 dialCtlPeerCallInformation 2 dialCtlPeerCallSetup
- **dlsw** —Envia notificações de agentes DLSw quando o **dlsw** palavra-chave é usada, você po especificar *anotification*-optionvalue. Proveniente de CISCO-DLSW-MIB, e as notificaçõe

são: enterprise 1.3.6.1.4.1.9.10.9.1.7 1 ciscoDlswTrapTConnPartnerReject 2 ciscoDlswTrapTConnProtViolation 3 ciscoDlswTrapTConnUp 4 ciscoDlswTrapTConnDow ciscoDlswUpTrapCircuitCircuit 6 ciscoDlswTrapCircuitDown

- **ds0-busyout**—Envia uma notificação sempre que o busyout de uma interface DS0 altera o estado. Essa palavra-chave é adicionada desde o Cisco IOS Software Release 12.1(3)T apenas para a plataforma Cisco AS5300. Proveniente de CISCO-POP-MGMT-MIB, e a notificação é: enterprise 1.3.6.1.4.1.9.10.19.2 1 cpmDS0BusyoutNotification
- **ds1-loopback**—Envia uma notificação sempre que a interface DS1 entra no modo loopback. Essa palavra-chave é adicionada desde o Cisco IOS Software Release 12.1(3)T apenas a plataforma Cisco AS5300. Proveniente de CISCO-POP-MGMT-MIB, e a notificação é: enterprise 1.3.6.1.4.1.9.10.19.2 2 cpmDS1LoopbackNotification
- **dspu**—Envia uma notificação sempre que o estado operacional da unidade física (PU) ou unidade lógica (LU) é alterado ou uma falha de ativação é detectada. Proveniente de CIS DSPU-MIB, e as notificações são: enterprise 1.3.6.1.4.1.9.9.24.1.4.4 1newdspuPuStateChangeTrap 2 newdspuPuActivationFailureTrap enterprise 1.3.6.1.4.1.9.24.1.5.3 1 newdspuLuStateChangeTrap 2 dspuLuActivationFailureTrap
- **dsp**—Envia uma notificação sempre que a placa DSP fica ativa ou inativa. Proveniente de CISCO-DSP-MGMT-MIB, e a notificação é: enterprise 1.3.6.1.4.1.9.9.86.2 1 cdspMIBCardStateNotification
- **entity**—Envia notificações de modificação MIB do Entity. Proveniente de ENTITY-MIB, e a notificações são: enterprise 1.3.6.1.2.1.47.2 1 entConfigChange
- **envmon**—Envia notificações de monitoramento ambiental específico da empresa da Cisco quando um limite ambiental é excedido. Quando o comando**envmon**palavra-chave é usada você pode especificar *anotification*-optionvalue. Proveniente de CISCO-ENVMON-MIB, e notificações são: empresa 1.3.6.1.4.1.9.9.13.3 1 ciscoEnvMonShutdownNotification 2 ciscoEnvMonVoltageNotification 3 ciscoEnvMonTemperatureNotification 4 ciscoEnvMonFanNotification 5 ciscoEnvMonRedundantSupplyNotification
- **frame-relay**—Envia notificações de Frame Relay Proveniente de RFC1315-MIB, e as notificações são: enterprise 1.3.6.1.2.1.10.32 1 forDLCIStatusChange
- **hsrp**—Envia notificações do Hot Standby Router Protocol (HSRP). Este recurso é compati desde o Cisco IOS Software Release 12.0(3)T. Proveniente de CISCO-HSRP-MIB, e as notificações são: enterprise 1.3.6.1.4.1.9.9.106.2 1 cHsrpStateChange
- **isdn**—Envia notificações ISDN. Quando o comando**isdn**palavra-chave é usada, você pode especificar *anotification*-optionvalue. Proveniente de CISCO-ISDN-MIB, e as notificações empresa 1.3.6.1.4.1.9.9.26.2 1 demandaNbrCallInformation 2 demandaNbrCallDetails 3 demandaNbrLayer2Change [suportado desde o Cisco IOS Software Release 12.1(1)T ] 4 demandaNbrCNANotification [suportado desde o Cisco IOS Software Release 12.1(5)T ] Proveniente de CISCO-ISDNU-IF-MIB, e as notificações são: empresa 1.1 3.6.1.4.1.9.9.1 ciuIfLoopStatusNotification
- **msdp**—Envia notificações MSDP (Protocolo de Descoberta de Origem de Transmissão Múltipla). Proveniente de MSDP-MIB, e as notificações são: enterprise 1.3.6.1.3.92.1.1.7 msdpEstablished 2 msdpBackwardTransition
- **repeater**—Envia um hub Ethernet**repeater**notificações. Quando a palavra-chave do repetidor selecionada, você pode especificar um *notification-option* valor. Proveniente de CISCO-REPEATER-MIB, e as notificações são: enterprise 1.3.6.1.4.1.9.9.22.3 1 ciscoRptrIllegalSrcAddrTrap
- **rsvp**—Envia notificações de RSVP (protocolo de reservas de recursos). Este recurso é

compatível desde o Cisco IOS Software Release 12.0(2)T. Proveniente de RSVP-MIB, e
notificações são: enterprise 1.3.6.1.3.71.2 1 newFlow 2 lostFlow

- **rtr**—Envia notificações RTR de Agentes de Garantia de Serviço (RTR). Proveniente de CISCO-RTTMON-MIB, e as notificações são: enterprise 1.3.6.1.4.1.9.9.42.2 1 rttMonConnectionChangeNotification 2 rttMonTimeoutNotification 3 rttMonThresholdNotification 4 rttMonVerifyErrorNotification
- **snmp**—Envia notificações do protocolo SNMP. Quando o comando**snmp**for usada, você po especificar um valor de opção de notificação. Proveniente de CISCO-GENERAL-TRAPS, notificações são: empresa 1.3.6.1.2.1.11 0 coldStart 2 linkDown 3 linkUp 4 authenticationFailure 5 egpNeighborLoss empresa 1.3.6.1.4.1.9 0 reload **Nota**:Esta interceptação é controlada pelo tipo de notificação "tty": 1 tcpConnectionClose
- **syslog**—Envia notificações de mensagem de erro (Cisco Syslog MIB). Especifique o nível mensagens a serem enviadas com o comando**logging history level**comando. Proveniente de CISCO-SYSLOG-MIB, e as notificações são: enterprise 1.3.6.1.4.1.9.9.41.2 1 clogMessageGenerated
- **voice**—Envia notificações de voz de baixa qualidade. Proveniente de CISCO-VOICE-DIAL CONTROL-MIBSMI, e as notificações são: enterprise 1.3.6.1.4.1.9.9.63.2 1 cvdcPoorQoVNotification
- **xgcp**—Envia notificações de Protocolo de Controle de Gateway de Mídia Externo (XGCP). Proveniente de XGCP-MOB, e as notificações são: enterprise 1.3.6.1.3.90.2 1 xgcpUpDownNotification

(Opcional)

- **dlsw [circuit | tconn]**—Quando o**dlsw**for usada, você poderá especificar o tipo de notificação específico que deseja ativar ou desativar. Se nenhuma palavra-chave for utilizada, todos tipos de notificação de DLSw serão permitidos. A opção pode ser uma ou mais dessas palavras-chave: **circuit**—Habilita os desvios do circuito do DLSw.**tconn**—Habilita as armadi de conexão de transporte de correspondente DLSw.
- **envmon [voltage | shutdown | supply | fan | temperature]**—Quando o**envmon**for usada, você poderá a um tipo de notificação ambiental específico ou aceitar todos os tipos de notificação do sis de monitoramento ambiental. Se nenhuma opção for especificada, todas as notificações ambientais serão ativadas. A opção pode ser uma ou mais dessas palavras-chave:**voltage**,**shutdown**,**supply**,**fan**,e**temperature**.
- **isdn [call-information | isdn u-interface | chan-not-avail | layer2]**—Quando o**isdn**palavra-chave for usad você pode especificar a**call-information**para ativar uma notificação de informações de chama ISDN SNMP para o subsistema MIB ISDN ou você pode especificar a**isdn u-interface**para at uma notificação de interface SNMP ISDN U para o subsistema MIB da interface ISDN U.

*opção de notificação*

- **repeater [health | reset]**—Quando o **repeater** for usada, você pode especificar a opção de repeti Se nenhuma opção foi especificada, todas as notificações do repetidor serão ativadas. A opção pode ser uma ou mais destas palavras-chave: health—Habilita a notificação de integridade do IETF (Internet Engineering Task Force) Repeater Hub MIB (RFC 1516). reset—Habilita a notificação de redefinição do IETF Repeater Hub MIB (RFC 1516). **health**—Ativa a notificação de integridade do hub repetidor MIB (RFC 1516) da Internet Engineering Task Force (IETF).**reset**—Ativa a notificação de redefinição do IETF Repeater MIB (RFC 1516).
- **snmp [authentication | linkup | linkdown | coldstart]**palavras-chave **linkup | linkdown | coldstart** adicionad desde o Cisco IOS Software Release 12.1(3)T. —Quando o **snmp** for usada, você poderá especificar o tipo de notificação específico que deseja ativar ou desativar. Se nenhuma palavra-chave for usada, todos os tipos de notificação SNMP serão habilitados (ou

desabilitados, se for usado nenhum formulário). Os tipos de notificação disponíveis são: **authentication**—Controla a distribuição de notificações de falha de autenticação SNMP. Um desvio authenticationFailure(4) significa que a entidade remetente do protocolo é o destinatário de uma mensagem de protocolo não autenticada corretamente.**linkup**—Contro envio de notificações de link SNMP. Uma interceptação linkUp(3) significa que a entidade protocolo de envio reconhece que um dos links de comunicação representado na configuração do agente ficou ativo.**linkdown**—Controla como as notificações de link de SN são enviadas. Uma interceptação linkDown(2) significa que a entidade de protocolo de er reconhece uma falha em um dos links de comunicação representado na configuração do agente.**coldstart**—Controla o envio de notificações de início frio SNMP. Uma armadilha coldStart(0) significa que a entidade de protocolo de envio é reinicializada de forma que a configuração do agente ou a implementação da entidade de protocolo pode ser alterada.

### Defaults

As notificações do SNMP estão desativadas.

Se digitar este comando sem palavras-chave do tipo de notificação, por padrão, todos os tipos de notificações controladas por este comando serão ativadas.

## Modos de comando

### Configuração global – Histórico de comandos

| Versão do Cisco IOS Software | Modificação |
|---|---|
| 11.1 | Esse comando foi introduzido. |
| 12.0(2)T | O **rsvp**palavra-chave foi adicionada. |
| 12.0(3)T | O **hsrp** palavra-chave foi adicionada. |
| 12.1(3)T | Essas palavras-chave foram adicionadas ao **snmp-server enable traps snmp** forma d comando:<br>• **linkup**<br>• **linkdown**<br>• **coldstart**<br>Essas palavras-chave tipo notificação foram adicionadas à plataforma Cisco AS5300 apenas:<br>• **ds0-busyout**<br>• **isdn chan-not-avail**<br>• **modem-health**<br>• **ds1-loopback**<br>Essa notificação tipo palavra-chave foi adicionada às plataformas Cisco AS53 AS5800 apenas:<br>• **aaa-server** |

### Utilize as diretrizes

O **snmp-server enable traps snmp [ linkup] [linkdown]** forma deste comando substitui a **snmp trap link-status interface** comando do modo de configuração.

O **no** forma do **snmp-server enable traps** é útil para desativar notificações que geram uma grande quantidade de ruído desnecessário na rede.

Notificações SNMP podem ser enviadas como armadilhas ou com solicitações de informação. Esse comando permite as duas armadilhas e informa solicitações para os tipos de notificação especiais.

Se você não inserir um **snmp-server enable traps** não serão enviadas notificações controladas por esse comando. Para configurar o roteador para enviar essas notificações SNMP, você deve inserir pelo menos um **snmp-server enable traps** comando. Se você introduzir o comando sem nenhuma palavra-chave, todos os tipos de notificação são ativados. Se digitar um comando com a palavra-chave, somente o tipo de notificação relativo à palavra-chave será habilitado. Para habilitar vários tipos de notificações, você deve emitir um comando **snmp-server enable traps** para cada tipo e opção de notificação.

O **snmp-server enable traps** é usado em conjunto com o comando **snmp-server host** comando. Execute o **snmp-server host** para especificar que host ou hosts recebem notificações SNMP. Para enviar notificações, você deve configurar pelo menos um **snmp-server host** comando.

Para que um host receba uma notificação controlada por esse comando, os dois **snmp-server enable traps** e o comando **snmp-server host** para esse host deve ser habilitado. Se o tipo de notificação não for controlado por esse comando, somente os **snmp-server host** deve ser habilitado.

Os tipos de notificação usadosneste comando têm um objeto MIB associado que permite que sejam ativados ou desativados (por exemplo, interceptações HSRP são definidas com MIB HSRP, as interceptações de repetidores são definidas com MIB do hub do repetidor, e assim por diante). Nem todos os tipos de notificação disponíveis no **snmp-server host** possuem objetos **notificationEnable MIB**, portanto alguns deles não podem ser controlados com o comando **snmp-server enable** comando.

# Informações Relacionadas

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.