Armadilhas de SNMP do Cisco IOS suportadas e como configurá-las

Índice

Introdução

Note: 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 IOS Software padrão (Roteadores, Switches do Asynchronous Transfer Mode (ATM) e servidores de acesso remoto) de Cisco podem gerar muito SNMP traps.

Pré-requisitos

Requisitos

Os leitores deste documento devem compreender esta informação:

Você não quer um dispositivo Cisco enviar todo o SNMP traps que o dispositivo sabe enviar. Por exemplo, se você permite todas as armadilhas em um servidor de acesso remoto com 64 linhas de discagem de entrada, você obtém uma armadilha sempre que um usuário disca dentro e sempre que um usuário termina a conexão. Isso cria um excesso de desvios. O Cisco IOS Software define grupos de armadilhas que você pode permitir ou desabilitar. Há dois comandos global configuration que você se usa para configurar o SNMP traps em um dispositivo do Cisco IOS Software:

- **snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port** *port***] [notification-type]**
  Emita o **comando snmp-server host global configuration** especificar o receptor de uma operação da notificação de SNMP. Não emita **nenhum** formulário deste comando remover o host especificado.
- **snmp-server enable traps [***notification-type***] [***notification-option***]**
  Emita o **comando snmp-server enable traps global configuration** permitir o roteador de enviar o SNMP traps. Não emita **nenhum** formulário deste comando a fim desabilitar notificações de SNMP.

Os tipos de armadilhas podem ser especificados nos dois comandos. Você deve emitir o **comando snmp-server host** a fim definir os sistemas de gerenciamento de rede onde as armadilhas devem ser enviada. Você deve especificar os tipos de armadilha se você não quer todas as armadilhas ser enviado. Emita **comandos enable traps do** servidor snmp múltiplo, um para cada um dos tipos de armadilha que você usou no **comando snmp host.**

Note: Não todas as opções do `[notification-type]` são apoiadas nboth of these comandos. Por exemplo, o `[notification-type]` X.25 e o teletipo (tty) não são usados para o **snmp-server enable trap.** as armadilhas X.25, e tty são permitidas à revelia.

Por exemplo, emita estes comandos fazer um dispositivo do Cisco IOS Software relatar somente a configuração, o Border Gateway Protocol (BGP), e as armadilhas tty ao sistema de gerenciamento de rede 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.

Convenções

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

Comando snmp-server host

Emita o **comando snmp-server host global configuration** especificar o receptor de uma operação da

notificação de SNMP. Não emita **nenhum** formulário deste comando 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 do Internet do host (receptor visado).
armadilhas	(Opcional) Envie armadilhas SNMP para esse host. Esse é o padrão.
informações	(Opcional) envie o SNMP informa a este host.
versão	(Opcional) a versão do SNMP usado para enviar as armadilhas. A versão 3 é o modelo o mais seguro, porque este modelo permite a criptografia de pacote de informação com as **palavras-chave privadas**. Se você usa as palavras-chave de versão, você deve especificar uma destas opções: • **1** — SNMPv1. Esta opção não está disponível nos informativos. • **2c** — SNMPv2C • **3** — SNMPv3. Estas três palavras-chave opcionais podem seguir a palavra-chave da versão 3: **o AUTH** (opcional) permite a autenticação de pacote de informação do message digest 5 (MD5) e do Secure Hash Algorithm (SHA).**noauth** (padrão) o nível de segurança do noAuthNoPriv. Este é o padrão se [AUTH | noauth | a opção priv] keyword (palavra-chave privada) não está especificada.**o priv** (opcional) permite a criptografia de pacote de informação do Data Encryption Standard (DES) (igualmente chamada “privacidade”).
community-string	Senha-como o string de comunidade enviado com a operação de notificação. Embora você pode ajustar esta corda com o **comando snmp-server host** por si só, Cisco recomenda que você define esta corda com o **comando snmp-server community** antes que você emita o **comando snmp-server host**.
udp-port port	Porta User Datagram Protocol (UDP) do host a ser usado. O padrão é 162.
tipo de notifica	(Opcional) o tipo de notificação a ser enviado ao host. Se nenhum tipo é especificado, todas

ção	as notificações estão enviadas. O tipo de notificação pode ser umas ou várias destas palavras-chaves: • **AAA-server** — Envia notificação AAA. • **BGP** — Envia notificações da mudança de estado do Border Gateway Protocol (BGP). • **bstun** — Envia notificações do Block Serial Tunneling (BSTUN). • **calltracker** — Envia notificações ao CallTracker. • **configuração** — Envia notificações da configuração. • **dlsw** — Envia notificações do switching de link de dados (DLSw). • **ds0-busyout** — Envia notificações ds0-busyout. • **ds1-loopback** — Envia notificações ds1-loopback. • **dspu** — Envia notificações do Downstream Physical Unit (DSPU). • **dsp** — Envia notificações do processamento de sinal digital (DSP). • **entidade** — Notificações da alteração do Management Information Base do Envia entidade (MIB). • **envmon** — Envia notificações Cisco empreendimento-específico do monitor ambiental quando um ponto inicial ambiental é excedido. • **Frame Relay** — Envia notificações do Frame Relay. • **hsrp** — Envia notificações do Hot Standby Router Protocol (HSRP). • **isdn** — Envia notificações do Integrated Services Digital Network (ISDN). • **msdp** — Envia notificações do Multicast Source Discovery Protocol (MSDP). • **llc2** — Envia o Logical Link Control, o tipo-2 (LLC2) notificações. • **repetidor** — Envia notificações padrão do repetidor (hub). • **rsrb** — Envia notificações do Remote Source-Route Bridging (RSRB). • **rsvp** — Notificações do protocolo sends resource reservation (RSVP). • **rtr** — Notificações do Sends SA Agent (RTR). • **sdlc** — Envia notificações do Synchronous

	Data Link Control (SDLC). • **snmp** — Envia notificações do Simple Network Management Protocol (SNMP) (como definido no RFC 1157). • **aturdir** — Envia notificações do Serial Tunnel (STUN). • **Syslog** — Envia notificações de mensagem de erro (Syslog MIB de Cisco). Especifique o nível das mensagens a ser enviadas com **O comando logging history level.** • **tty** — Envia notificações Cisco empreendimento-específico quando uma conexão do Transmission Control Protocol (TCP) se fecha. • **Voz** — Envia notificações da Voz. • **x.25** — Envia as notificações de evento X.25. • **xgcp** — Envia notificações do protocolo external media gateway control (XGCP).

Defaults

O comando snmp-server host command 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.

Nenhum informa são enviados a este host. Se nenhuma **palavra-chave de versão** esta presente, o padrão é versão 1. **o comando no snmp-server host** sem palavras-chaves desabilita armadilhas, mas não informa-as, ao host. Emita o **comando no snmp-server host informs** desabilitar informa.

Note: Se a *série de comunidade* não está definida com o **comando snmp-server community** antes que você use este comando, o formulário do padrão do **comando snmp-server community** está introduzido automaticamente na configuração. A senha (série da comunidade) usada para esta configuração automática da comunidade snmp-server é a mesma que foi especificada no comando snmp-server host. 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	Estas palavras-chaves foram adicionadas: • **versão 3 [AUTH | noauth | priv]**

	• **hsrp**

Utilize as diretrizes

Notificações SNMP podem ser enviadas como armadilhas ou com solicitações de informação. As armadilhas são incertas porque o receptor não envia reconhecimentos quando este dispositivo recebe armadilhas. O remetente não pode determinar se as armadilhas foram recebidas. Contudo, uma Entidade SNMP que receba um pedido da informação reconhece a mensagem com uma unidade de dados de protocolo (PDU) da resposta de SNMP. Se o remetente nunca recebe a resposta, o pedido da informação pode ser enviado outra vez. , Informa consequentemente são mais provável alcançar seu 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 armadilhas estão enviadas somente uma vez, quando uma informação puder ser experimentada de novo diversas vezes. As novas tentativas aumentam o tráfego e contribuem para uma carga adicional maior na rede.

Se você não inscreve um **comando snmp-server host**, nenhuma notificação está enviada. Para configurar o roteador de forma a enviar notificações SNMP, é necessário informar pelo menos um comando snmp-server host. Se você incorpora o comando sem palavras-chaves, todos os tipos de armadilha estão permitidos para o host.

A fim permitir host múltiplos, você deve emitir um **comando host do** servidor snmp separado para cada host. Você pode especificar vários tipos de notificações no comando para cada host.

Quando os **comandos host do** servidor snmp múltiplo estiverem dados para o mesmos host e tipo de notificação (a armadilha ou informa), cada comando overwrites o comando precedente. Apenas o último comando snmp-server host é considerado. Por exemplo, se você digitar um comando snmp-server host inform para um host e depois digitar um outro comando snmp-server host inform para o mesmo host, o segundo comando substituirá o primeiro.

O comando snmp-server host é usado em conjunto com o comando snmp-server enable. Emita o **comando snmp-server enable** a fim especificar que notificações de SNMP são enviadas globalmente. Para que um host receba a maioria de notificações, pelo menos um **comando snmp-server enable** e o **comando snmp-server host** para esse host devem ser permitidos.

Contudo, alguns tipos de notificação não podem ser controlados com o **comando snmp-server enable**. Por exemplo, alguns tipos de notificação estão sempre habilitados. Outros tipos de notificação são permitidos por um comando diferente. Por exemplo, as `notificações linkUpDown` são controladas pelo **comando snmp trap link-status**. Esses tipos de notificação não exigem um comando snmp-server enable.

A Disponibilidade de uma opção do tipo de notificação depende do tipo de roteador e das Funcionalidades do software Cisco IOS apoiados no roteador. Por exemplo, o tipo de notificação do **envmon** está disponível somente se o monitor ambiental é parte do sistema.

Configurando informações

Termine estas etapas para poder enviar uma informação:

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

Exemplos

Se você quer configurar uma série de comunidade snmp original para armadilhas, mas você quer impedir o acesso do polling snmp com esta corda, a configuração deve incluir uma lista de acesso. Neste exemplo, o string de comunidade é nomeado “comaccess,” e a lista de acessos é numerada 10:

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

Este exemplo envia o SNMP traps ao 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 o SNMP e as armadilhas das específicas do empreendimento do Cisco environmental monitor para endereçar 172.30.2.160:

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

Este exemplo permite o roteador de enviar todas as armadilhas ao host myhost.cisco.com com o string pública de comunidade:

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

Este exemplo não envia armadilhas a nenhum 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 o roteador de enviar todo informa pedidos ao host myhost.cisco.com usando o string pública de comunidade:

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

Este exemplo envia armadilhas HSRP SNMPv2C ao 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
```

Comando snmp-server enable traps

Use o **comando snmp-server enable traps global configuration** permitir o roteador de enviar o SNMP traps. Use o no form desse comando para desativar 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 a permitir. Se nenhum tipo é especificado, todas as notificações estão enviadas (incluindo o **envmon** e as **notificações de repetidor**). O tipo de notificação pode ser uma destas palavras-chaves: • **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. Isto é do CISCO-AAA-SERVER-MIB, e as notificações são: empresa 1.3.6.1.4.1.9.10.56.2 1 casServerStateChange • **BGP** — Envia notificações da mudança de estado do Border Gateway Protocol (BGP). Isto é do BGP4-MIB, e as notificações são: a empresa 1.3.6.1.2.1.15.7 1 bgpEstablished o bgpBackwardTransition 2 • **calltracker** — Envia uma notificação sempre que uma entrada de chamada ativa nova é criada no cctActiveTable ou uma entrada de chamada nova da história é criada no cctHistoryTable isto é do CISCO-CALL-TRACKER-MIB, e as notificações são: empresa 1.3.6.1.4.1.9.9.163.2 1 cctCallTerminateNotification do

	cctCallSetupNotification 2 • **configuração** — Envia notificações da configuração. Isto é do CISCO-CONFIG-MAN-MIB, e as notificações são: empresa 1.3.6.1.4.1.9.9.43.2 1 ciscoConfigManEvent • **seletor** — Envia uma notificação sempre que uma chamada bem sucedida cancela, uma tentativa de chamada falha é determinado ter falhado finalmente, ou sempre que um mensagem de configuração de chamada é recebido ou enviado. Isto é do DIAL-CONTROL-MIB, e as notificações são: empresa 1.3.6.1.2.1.10.21.2 1 dialCtlPeerCallSetup do dialCtlPeerCallInformation 2 • **dlsw** — Envia notificação dos agentes de DLSw quando a palavra-chave do **dlsw** é usada, você pode especificar um *valor de opção de notificação*. Isto é do CISCO-DLSW-MIB, e as notificações são: empresa 1.3.6.1.4.1.9.10.9.1.7 1 ciscoDlswTrapCircuitDown do ciscoDlswTrapCircuitUp 6 do ciscoDlswTrapTConnDown 5 do ciscoDlswTrapTConnUp 4 do ciscoDlswTrapTConnProtViolation 3 do ciscoDlswTrapTConnPartnerReject 2 • **ds0-busyout** — Envia uma notificação sempre que o busyout de uma relação DS0 muda o estado. Essa palavra-chave é adicionada desde o Cisco IOS Software Release 12.1(3)T apenas para a plataforma Cisco AS5300. Isto é do CISCO-POP-MGMT-MIB, e a notificação é: empresa 1.3.6.1.4.1.9.10.19.2 1 cpmDS0BusyoutNotification • **ds1-loopback** — Envia uma notificação sempre que a relação DS1 entra no modo loopback. Essa palavra-chave é adicionada desde o Cisco IOS Software Release 12.1(3)T apenas para a plataforma Cisco AS5300. Isto é do CISCO-POP-MGMT-MIB, e a notificação é: empresa 1.3.6.1.4.1.9.10.19.2 2 cpmDS1LoopbackNotification • **dspu** — Envia uma notificação sempre que o estado operacional do physical unit (PU) ou do logical unit (LU) muda ou a falha de ativação é detectada. Isto é do CISCO-DSPU-MIB, e as

	notificações são: empresa 1.3.6.1.4.1.9.9.24.1.5.3 do newdspuPuActivationFailureTrap 1newdspuPuStateChangeTrap 2 da empresa 1.3.6.1.4.1.9.9.24.1.4.4 1 dspuLuActivationFailureTrap do newdspuLuStateChangeTrap 2 • **dsp** — Envia uma notificação sempre que o cartão DSP vai para cima ou para baixo. Isto é do CISCO-DSP-MGMT-MIB, e a notificação é: empresa 1.3.6.1.4.1.9.9.86.2 1 cdspMIBCardStateNotification • **entidade** — Notificações da alteração do Envia entidade MIB. Isto é do ENTITY-MIB, e as notificações são: empresa 1.3.6.1.2.1.47.2 1 entConfigChange • **envmon** — Envia notificações Cisco empreendimento-específico do monitoramento ambiental quando um ponto inicial ambiental é excedido. Quando a palavra-chave envmon for utilizada, é possível especificar um valor de opção de notificação. Isto é do CISCO-ENVMON-MIB, e as notificações são: empresa 1.3.6.1.4.1.9.9.13.3 1 ciscoEnvMonRedundantSupplyNotification do ciscoEnvMonFanNotification 5 do ciscoEnvMonTemperatureNotification 4 da ciscoEnvMonVoltageNotification 3 do ciscoEnvMonShutdownNotification 2 • **Frame Relay** — Envia notificações do Frame Relay. Isto é do RFC1315-MIB, e as notificações são: empresa 1.3.6.1.2.1.10.32 1 frDLCIStatusChange • **hsrp** — Envia notificações do Hot Standby Router Protocol (HSRP). Esta característica é apoiada desde o Cisco IOS Software Release 12.0(3)T. Isto é do CISCO-HSRP-MIB, e as notificações são: empresa 1.3.6.1.4.1.9.9.106.2 1 cHsrpStateChange • **isdn** — Envia notificações ISDN. Quando a palavra-chave isdn for utilizada, você pode especificar um valor de opção de notificação. Isto é do CISCO-ISDN-MIB, e as notificações são: a empresa 1.3.6.1.4.1.9.9.26.2 1 [supported since Cisco IOS Software Release 12.1(5)T] do demandNbrCNANotification do [supported since Cisco IOS Software Release

	12.1(1)T] 4 dos demandNbrCallDetails 3 demandNbrLayer2Change da demandNbrCallInformation 2 isto é do CISCO-ISDNU-IF-MIB, e as notificações são: empresa 1.3.6.1.4.1.9.9.18.2 1 ciuIfLoopStatusNotification • **msdp** — Envia notificações do Multicast Source Discovery Protocol (MSDP). Isto é do MSDP-MIB, e as notificações são: a empresa 1.3.6.1.3.92.1.1.7 1 msdpEstablished o msdpBackwardTransition 2 • **repetidor** — Envia **notificações de repetidor do** concentrador de Ethernet. Quando a palavra-chave do repetidor é selecionada, é possível especificar um valor para a opção de notificação. Isto é do CISCO-REPEATER-MIB, e as notificações são: empresa 1.3.6.1.4.1.9.9.22.3 1 ciscoRptrIllegalSrcAddrTrap • **rsvp** — Notificações do protocolo sends resource reservation (RSVP). Esta característica é apoiada desde o Cisco IOS Software Release 12.0(2)T. Isto é do RSVP-MIB, e as notificações são: empresa 1.3.6.1.3.71.2 1 lostFlow do newFlow 2 • **rtr** — Envia notificações do Service Assurance Agent RTR (RTR). Isto é do CISCO-RTTMON-MIB, e as notificações são: empresa 1.3.6.1.4.1.9.9.42.2 1 rttMonVerifyErrorNotification do rttMonThresholdNotification 4 do rttMonTimeoutNotification 3 do rttMonConnectionChangeNotification 2 • **SNMP** — Envia notificações do Simple Network Management Protocol (SNMP). Quando a palavra-chave snmp é utilizada, você pode especificar um valor de opção de notificação. Isto é do CISCO-GENERAL-TRAPS, e as notificações são: a empresa 1.3.6.1.2.1.11 0 inicializações lentas 2 desativa o link 3 a empresa 1.3.6.1.4.1.9 dos egpNeighborLoss do authenticationFailure 5 da associação 4 0 reload **Note**: Esta armadilha é controlada pelo tipo de notificação “tty”:**Note**: 1 tcpConnectionClose • **Syslog** — Envia notificações de mensagem de erro (Syslog MIB de Cisco). Especifique o

	nível das mensagens a ser enviadas com o **comando logging history level**. Isto é do CISCO-SYSLOG-MIB, e as notificações são: empresa 1.3.6.1.4.1.9.9.41.2 1 clogMessageGenerated • **voz** — Envia a notificação de qualidade ruim de voz. Isto é do CISCO-VOICE-DIAL-CONTROL-MIBSMI, e as notificações são: empresa 1.3.6.1.4.1.9.9.63.2 1 cvdcPoorQoVNotification • **xgcp** — Envia notificações do protocolo external media gateway control (XGCP). Isto é do XGCP-MIB, e as notificações são: empresa 1.3.6.1.3.90.2 1 xgcpUpDownNotification
opção de notificação	(Opcional) • **dlsw [circuito | tconn]** — quando a palavra-chave do **dlsw** for usada, você pode especificar o tipo de notificação que específico você deseja permitir ou desabilitar. Se nenhuma palavra-chave for utilizada, todos os tipos de notificação de DLSw serão permitidos. A opção pode ser umas ou várias destas palavras-chaves: **circuito** — Permite armadilhas de circuito de DLSw.**tconn** — Permite armadilhas de conexão de transporte de peer de DLSw. • **envmon [tensão | fechamento | fonte | fã | temperatura]** — quando o **palavra-chave envmon** for usado, você pode permitir um tipo de notificação ambiental específico, ou aceite todos os tipos de notificação do sistema de monitoramento ambiental. Se nenhuma opção é especificada, todas as notificações ambientais estão permitidas. A opção pode ser umas ou várias destas palavras-chaves: voltagem, fechamento, alimentação, ventilação e temperatura. • **isdn [informação de chamada | isdn u-interface | chan-not-avail | layer2]** — Quando o **palavra-chave ISDN** é usado, você pode especificar a palavra-chave da **informação de chamada** para permitir uma notificação de informação da chamada ISDN SNMP para o subsistema ISDN MIB, ou você pode especificar a palavra-chave do **isdn u-interface** para permitir uma notificação da interface U SNMP ISDN para o subsistema de MIB da interface U ISDN.

	• **repetidor [saúde | restauração]** — quando o **palavra-chave de repetidor** for usado, você pode especificar a opção de repetidor. Se nenhuma opção foi especificada, todas as notificações do repetidor serão ativadas. A opção pode ser umas ou várias destas palavras-chaves: saúde--Habilita a notificação da integridade (RFC 1516) do concentrador de repetidor MIB da Internet Engineering Task Force (IETF). restauração--Habilita a notificação de reinicialização do concentrador de repetidor MIB da ETF (RFC 1516). **saúde** — Permite a notificação de saúde do concentrador de repetidor MIB do Internet Engineering Task Force (IETF) (RFC 1516).**restauração** — Permite a notificação de reinicialização do concentrador de repetidor MIB IETF (RFC 1516). • **SNMP [autenticação | linkup | linkdown |** conexão de palavras-chave da **inicialização lenta] | linkdown | inicialização lenta** adicionada desde o Cisco IOS Software Release 12.1(3)T. — Quando as **palavras-chave de SNMP** são usadas, você pode especificar o tipo de notificação que específico você deseja permitir ou desabilitar. 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: **autenticação** — Controla a distribuição de notificações de falha da autenticação SNMP. Um desvio authenticationFailure(4) significa que a entidade remetente do protocolo é o destinatário de uma mensagem de protocolo não autenticada corretamente.**associação** — Controla a emissão de notificações do link ativado/desativado SNMP. LinkUp(3) uma armadilha significa que a entidade de protocolo de emissão reconhece que um dos links de comunicação representados na configuração do agente veio acima.**desativar o link** — Controla como as notificações de link desativado SNMP são enviadas. LinkDown(2) uma armadilha significa que a entidade de protocolo de emissão reconhece uma falha em um dos links de comunicação representados na configuração do agente.**inicialização lenta**

	— Controla a emissão de notificações de partida à frio SNMP. ColdStart(0) uma armadilha significa que a entidade de protocolo de emissão reinitializing tais que a configuração do agente ou da aplicação da entidade de protocolo pôde 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	A palavra-chave do **rsvp** foi adicionada.
12.0(3)T	A palavra-chave hsrp foi adicionada.
12.1(3)T	Estas palavras-chaves foram adicionadas ao **servidor snmp permitem o** formulário **SNMP das armadilhas d**este comando: • **linkup** • **linkdown** • **coldstart** Estas palavras-chave de tipo de notificação foram adicionadas para a plataforma do Cisco AS5300 somente: • **ds0-busyout** • **isdn chan-not-avail** • **modem-saúde** • **Loopback ds1** Estas palavras-chave de tipo de notificação foram adicionadas para o Cisco AS5300 and AS5800 platforms somente: • **aaa-server**

Utilize as diretrizes

A forma snmp-server enable traps snmp [linkup] [linkdown] deste comando substitui o comando de modo de configuração snmp trap link-status interface.

Nenhum formulário do **comando snmp-server enable traps** é útil a fim desabilitar as notificações que gerenciem uma grande quantidade de ruído unneeded em sua 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 inscreve um **comando snmp-server enable traps**, nenhuma notificação controlada por este comando está enviada. Para configurar o roteador para enviar essas notificações SNMP, você deve digitar pelo menos um comando snmp-server enable traps. 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, emita um comando snmp-server enable traps separado para cada tipo e opção de notificação.

O comando snmp-server enable traps é usado em conjunto com o comando snmp-server host. Emita o **comando snmp-server host** especificar qual o host ou os anfitriões recebem notificações de SNMP. Para enviar notificações, você deve configurar pelo menos um comando snmp-server host.

Para que um host receba uma notificação controlada por este comando, o **comando snmp-server enable traps** e o **comando snmp-server host** para esse host devem ser permitidos. Se o tipo de notificação não é controlado por este comando, simplesmente o **comando snmp-server host** apropriado deve ser permitido.

Os tipos de notificação usados neste comando all têm um objeto MIB associado que permita que sejam permitidos ou desabilitados (por exemplo, as armadilhas HSRP são definidas com o HSRP MIB, armadilhas de repetidor são definidas com o concentrador de repetidor MIB, e assim por diante). Não todos os tipos de notificação disponíveis no **comando snmp-server host** têm objetos MIB notificationEnable, assim que alguma destes não pode ser controlada com o **comando snmp-server enable.**

Informações Relacionadas

- Aprimoramentos de interceptação de ATM/SNMP e OAM
- Suporte Técnico - Cisco Systems