

# Monitore a Disponibilidade da câmera IP no exemplo de utilização da configuração de SNMP VS 6.2

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Diagrama de Rede](#)

[Vista geral SNMP](#)

[Uso-casos da monitoração VS SNMP](#)

[Vista geral VSMC para configurar o SNMP](#)

[Procedimento de configuração](#)

[Apêndice A: Captações dos Ethernet de armadilhas bwConnectionEvent e bwProxyEvent](#)

[Apêndice B: Disparador para prender a matriz](#)

[Apêndice C: Definição BROADWARE-EVENT-MIB](#)

[Anexo D: Armadilhas adicionais VS](#)

[Informações Relacionadas](#)

## Introdução

Este documento é visado aos clientes do Gerenciador de vigilância por vídeo da Cisco (VS) que executam o servidor de mídia da Vigilância por vídeo (VS) 6.2.x ou mais cedo quem estão interessados na monitoração para a Disponibilidade da câmera IP através do SNMP ou de um mecanismo de alerta SNMP-provocado. Contém uma vista geral dos serviços da caça com armadilhas SNMP disponíveis em VS 6.2.x e para distribuir mais cedo a estratégia simples da alerta e de Monitoramento de redes de uma câmera IP, assim como um processo passo a passo para permitir o SNMP em VS além do que fluxos de chamadas e exemplos de Troubleshooting básicos. Esta configuração não se aplica a nenhuma 6.3.x ou versões mais atrasada dos VS, porque os VS 6.3 introduzem o painel do monitoramento de funcionamento, que prevenirá os procedimentos contidos neste documento através da introdução de uma estrutura detalhada da monitoração da Vigilância por vídeo. Além, o **BROADWARE-EVENT-MIB** será usado já não em 6.3.x e em umas liberações mais atrasadas dos VS. Refira por favor a documentação 6.3 para obter informações sobre das estratégias de gerenciamento disponíveis do Monitoramento de redes e da câmera em 6.3.x e de umas versões mais atrasadas dos VS.

## Pré-requisitos

## Requisitos

Não existem requisitos específicos para este documento.

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

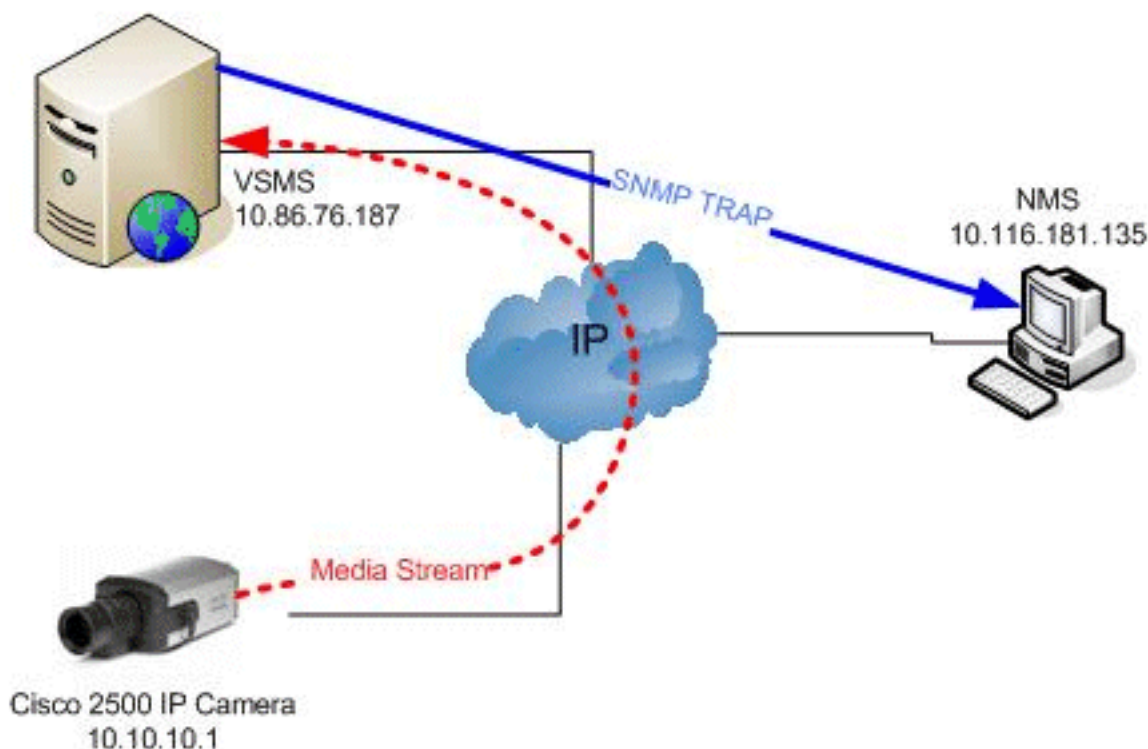
- Firmware running 2.1.2 da câmera 2500 IP de Cisco
- VS que executam 6.2.1-12d
- Gerenciador de operações da Vigilância por vídeo (VSOM) que executa 4.2.1-14

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

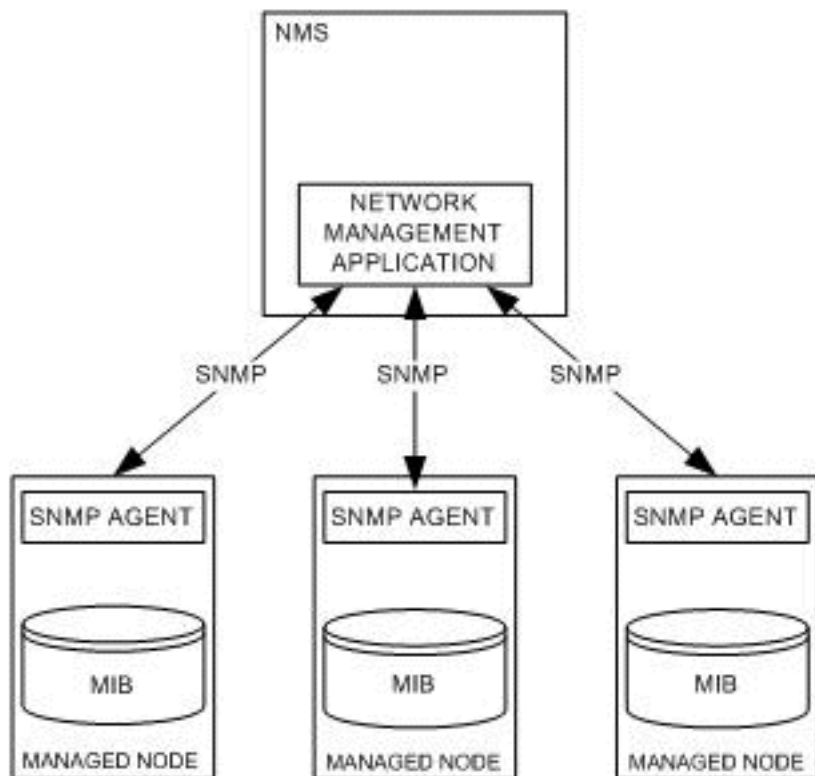
## Diagrama de Rede



## Vista geral SNMP

O Simple Network Management Protocol (SNMP) descreve uma estrutura do servidor cliente permitindo que um SNMP Manager recolha a informação (ou para configurar) de um agente SNMP que usa um Management Information Base (MIB), onde um agente SNMP está sendo

executado em todo o nó controlado. É incluída nesta coleta da informação a capacidade para que um agente SNMP transmita a informação de gerenciamento a um SNMP Manager sem ser solicitada a fazer assim pelo SNMP Manager. Este nó controlado (que abriga o agente SNMP) poderia ser um server, um telefone IP, um roteador de rede, switch de rede, ou todo o dispositivo capaz IP que incluir uma pilha de software SNMP e for conseqüentemente capaz do controle através do SNMP. Em resumo, o SNMP permite gerentes de rede remotamente monitora e controla a evolução dos objetos de rede.



Três versões geralmente distribuídas do SNMP existem: SNMPv1, SNMPv2C, e SNMPv3. O restante deste artigo concentra-se especificamente na capacidade da caça com armadilhas SNMPv2C como configurado em VS. Usando o diagrama acima como uma referência, o agente SNMP reside no server VS (o nó controlado) e relata a informação da caça com armadilhas SNMP ao SNMP Manager, que poderia ser uma plataforma da terceira do sistema de gerenciamento de rede (NMS). Os NMS comuns incluem o gerenciador de nó de rede do HP Open View, o Tivoli Netview, e o Solarwinds Orion.

**Nota:** Uma análise detalhada do protocolo de SNMP, incluindo diferenças versioning, é além do alcance deste documento.

As armadilhas SNMPv2C utilizam o protocolo de transporte UDP (dest. a porta 162) e é considerada conseqüentemente incerta. Por exemplo, se uma armadilha de SNMP que relata uma câmera IP que flui o erro é perdida no trânsito ao NMS, os VS serão inconscientes desta perda e a armadilha de SNMP não será retransmitida por VS. Em conseqüência, o operador do Network Operations Center (NOC) que confia unicamente no SNMP será inconsciente da falha da câmera IP. Este comportamento incerto é aplicável a todas as arquiteturas da caça com armadilhas SNMP e é conseqüentemente não específico aos VS. Além do uso da porta 162 UDP (comum a todas as aplicações da caça com armadilhas SNMP), cada armadilha transmitida dos VS ao NMS inclui alguma outra informação evento-diagnóstica comum:

- O string de comunidade "broadware-SNMP" SNMPv2CO demônio do receptor de armadilha NMS deve ser configurado tais que é capaz de processar e de apresentar o ingresso das

armadilhas SNMPv2C com a comunidade “broadware-SNMP”. Os nomes de comunidade SNMP são uns simples senha-como o mecanismo de segurança significado autenticar comunicações entre o SNMP NMS e o nó controlado SNMP. Ao contrário da versão do SNMP ou do endereço de estação de destino da caça com armadilhas, o padrão VS do “broadware-SNMP” não pode ser mudado. Veja a seção autorizada [procedimento de configuração](#) para confirmar que aspectos da implementação de SNMP VS são configuráveis.

- sysUpTime (OID 1.3.6.1.2.1.1.3) o sysUpTime é um objeto MIB particular definido no SNMPv2-MIB (RFC 1213) e relata o tempo (nos centésimo de um segundo) desde que a parcela do Gerenciamento de redes do sistema re-foi inicializada por último, que combina tipicamente o uptime do server VS.

A fim utilizar o procedimento abaixo para monitorar componentes VS, um NMS capaz de receber, de analisar gramaticalmente, e de apresentar armadilhas SNMPv2C é exigido. Mais, para traduzir armadilhas **BROADWARE-EVENT-MIB SNMPv2C** aos nomes compreensíveis do evento, o arquivo de definição de **BROADWARE-EVENT-MIB.txt** deve ser instalado no NMS. Transferiu este arquivo no formato apropriado, conectam-no aos VS através do **nome of\_vsms>/vsmc.html do <ip\_address\_or de http://, navegam-nos aos destinos SNMPTRAP, e clicam-nos sobre o hiperlink VSEVENT MIB.**

Os VS são capazes de transmitir armadilhas SNMPv1 e SNMPv2C, embora o SNMPv2C seja recomendado devido ao Suporte MIB aumentado. Os VS igualmente apoiam o SNMPv2C informam as mensagens, que são idênticas aos mensagens de armadilha, salvo que uma informação é reconhecida pelo NMS. Em consequência, uma camada de confiança é adicionada.

**Nota:** Em VS 6.2 e somente em uma caça com armadilhas espontânea mais adiantada SNMP é apoiado. O polling snmp do **BROADWARE-EVENT-MIB** nos VS de uma estação NMS é uma operação unsupported. [No C do apêndice](#), a cláusula **MAX-ACCESS** para o objeto do **bwEventDesc** é ajustada acessível-para-para notificar.

## [Uso-casos da monitoração VS SNMP](#)

### [Monitoramento de disponibilidade da câmera IP do Uso-caso #1](#)

Os VS mantêm um exemplo do proxy para cada dispositivo da codificação, que é usado para receber o fluxo de mídia do dispositivo da codificação e para o escrever à memória compartilhada para uma transmissão mais atrasada a um cliente da visão VSOM, uns outros VS (alimentação da criança), ou ao armazenamento local através de um arquivo. De uma perspectiva do protocolo, cada exemplo do proxy comporta-se de acordo com o tipo de dispositivo que estão sendo controlados e o tipo de configuração de mídia. Por exemplo, os proxys criados para as câmeras IP de Cisco4500 configuradas para 1080P que usa H.264 serão autenticados primeiramente por VS. No seguimento da autenticação, os VS informarão a câmera de suas propriedades de fluência desejadas usando o Real-Time Streaming Protocol (RTSP). Finalmente, usando-se fluindo a informação derivada através do RTSP, a câmera IP de Cisco4500 começará a fluir seus media flui aos VS usando o Real-Time Protocol (RTP). Esta transação inteira pode ser capturada nos VS CLI usando o **tcpdump** – comando do **<IP\_of\_encoding\_device> do host do nn.**

**Nota:** As câmeras IP de Cisco autenticarão os VS à revelia que usam o HTTPS nas versões 6.x dos VS. Se usando dispositivos não-Cisco da codificação, verifique para ver se há o requisito de autenticação e o método contratando o apoio de produtos de terceira parte.

Após o aperto de mão com HTTPS e RTSP, os VS transmitirão uma armadilha **bwProxyEvent** que indica o [proxy\_name] do proxy conectado ao #a\_# b@ip\_address do dispositivo, onde o #a é o

número da entrada do dispositivo e o *#b* é o número da configuração para a entrada. É importante notar esta armadilha **bwProxyEvent** é transmitido após o aperto de mão HTTPS/RTSP, de qualquer maneira se o fluxo de mídia está sendo recebido por VS. Veja o [apêndice A.2](#) para um **bwProxyEvent** do exemplo conectado à armadilha do dispositivo e verifique **ims.log** para ver se há o sucesso/status de falha plano do controle HTTPS e RTSP:

- Aperto de mão HTTPS bem sucedido:

```
[ proxy(851).p_s1_Mathers_1 GL_UTIL=1
<HttpsClient.cxx:267> ]
got reply header
```
- Aperto de mão HTTPS mal sucedido:

```
[ proxy(851).p_s1_Mathers_1 GL_UTIL=1
<HttpsClient.cxx:246> ]
Https(curl): Unable to curl perform[couldn't connect to host]
```
- Aperto de mão RTSP mal sucedido:

```
[ proxy(851).p_s1_Mathers_1 GL_UTIL=1
<RtspClient.cxx:546> ]
connect(addr='10.1.1.1:554', fd=6): Connection timed out
```

Se as conexões HTTPS ou RTSP dos VS à câmera IP são mal sucedidas, eventualmente, uma armadilha **bwConnectionEvent** são enviadas indicando o `[proxy_name]` do proxy incapaz de configurar ou o aperto de mão com o `#a_# b@ip_address` do dispositivo e está acompanhado desta mensagem de **ims.log**:

```
[ proxy(851).p_s1_Mathers_1 BE_PROXY=1 <Proxy.cxx:169> ]
Unable to configure or handshake with the device
```

Veja o [apêndice A.3](#) para de aperto de mão do exemplo “incapaz uma armadilha **bwConnectionEvent** de configurar ou”.

Após um aperto de mão bem sucedido, se o proxy VS não recebe o fluxo de mídia do dispositivo da codificação (câmera IP) por um período de 10s, os VS transmitem uma armadilha **bwConnectionEvent** que informa que um problema que conecta a um dispositivo de codificação dado existe. Esta armadilha indica o `[proxy_name]` do proxy que flui o erro. O dispositivo desligado ou o erro de rede e são acompanhados destas entradas de **ims.log**:

```
[ proxy(17741).p_s1_Mathers_1 GL_UTIL=1 <RtpClient.cxx:703> ]
Timeout (10 secs) waiting for data from encoder. [ proxy(17741).p_s1_Mathers_1 BE_PROXY=1
<Proxy.cxx:207> ]
Streaming error. Device disconnected or network error.
```

Consulte os direcionadores ou analise rastreamentos de rede para confirmar o aperto de mão e o comportamento do Protocolo streaming de um dispositivo não-Cisco da codificação.

**Nota:** Em linhas gerais, no evento uma câmera análoga conectada a um codificador do multiport perde a potência ou é removida do serviço, o dispositivo da codificação ainda fluirá a preto-tela. Em consequência, os VS não poderão compreender que a falha análoga da câmera e nenhuma trilha SNMP para fluir a perda estarão geradas.

## [Começo do arquivo do Uso-caso #2/para parar a notificação](#)

O tipo de notificação **bwArchiverEvent** pode ser usado para sinalizar os eventos do começo e da parada do laço configurado, do retorno, ou de únicos arquivos.

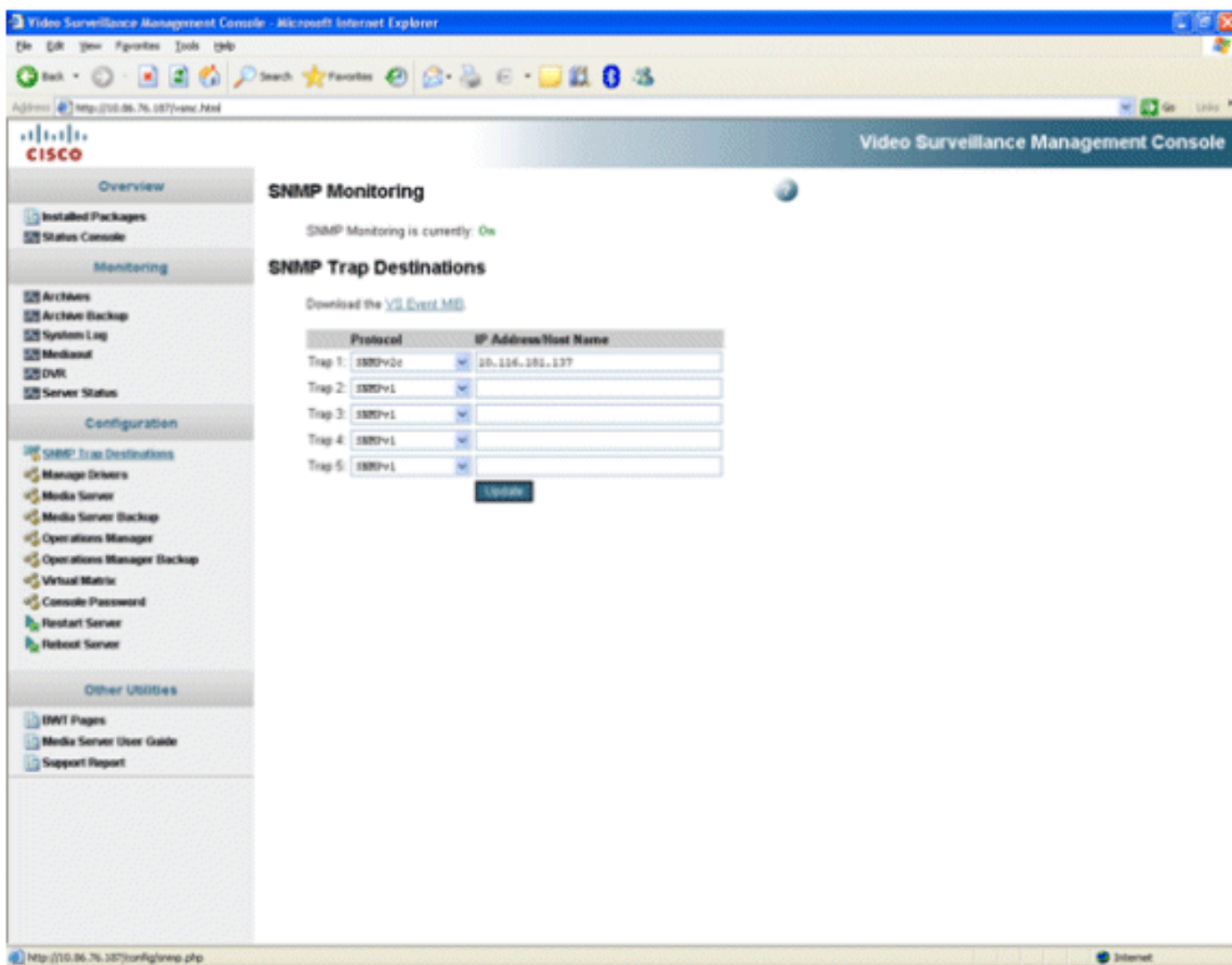
- Quando um arquivo é começado, uma armadilha **bwArchiverEvent** está gerada que indica o arquivo do começo BEM SUCEDIDO para o `archive_name`.
- Quando um arquivo é parado, uma armadilha **bwArchiverEvent** está gerada que indica o arquivo da parada BEM SUCEDIDO para o `archive_name`.

## Vista geral VSMC para configurar o SNMP

O console de gerenciamento da Vigilância por vídeo (VSMC) é uma configuração com base na Web GUI usada para ver diretamente e configurar opções de gerenciamento dos sistemas VS, sem usar VSOM ou o HTTP API. Em linhas gerais, VSOM é um USER-revestimento GUI, usado primeiramente para configurar e ver artigos característicos da aplicação, tais como proxys, arquivos, eventos e vistas. Inversamente, os artigos sistema-largos do Gerenciamento podem ser vistos e configurado em VSMC, incluindo log de sistema, SNMP, backup de dados, etc.

### Procedimento de configuração

Alcance o VSMC do servidor de mídia através do **nome of\_media\_server>/vsmc.html** do **<ip\_or\_de http://**, **escolha destinos SNMPTRAP > SNMPv2c** from a lista de Protocol pull-down, e incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do NMS a que as armadilhas serão enviadas:



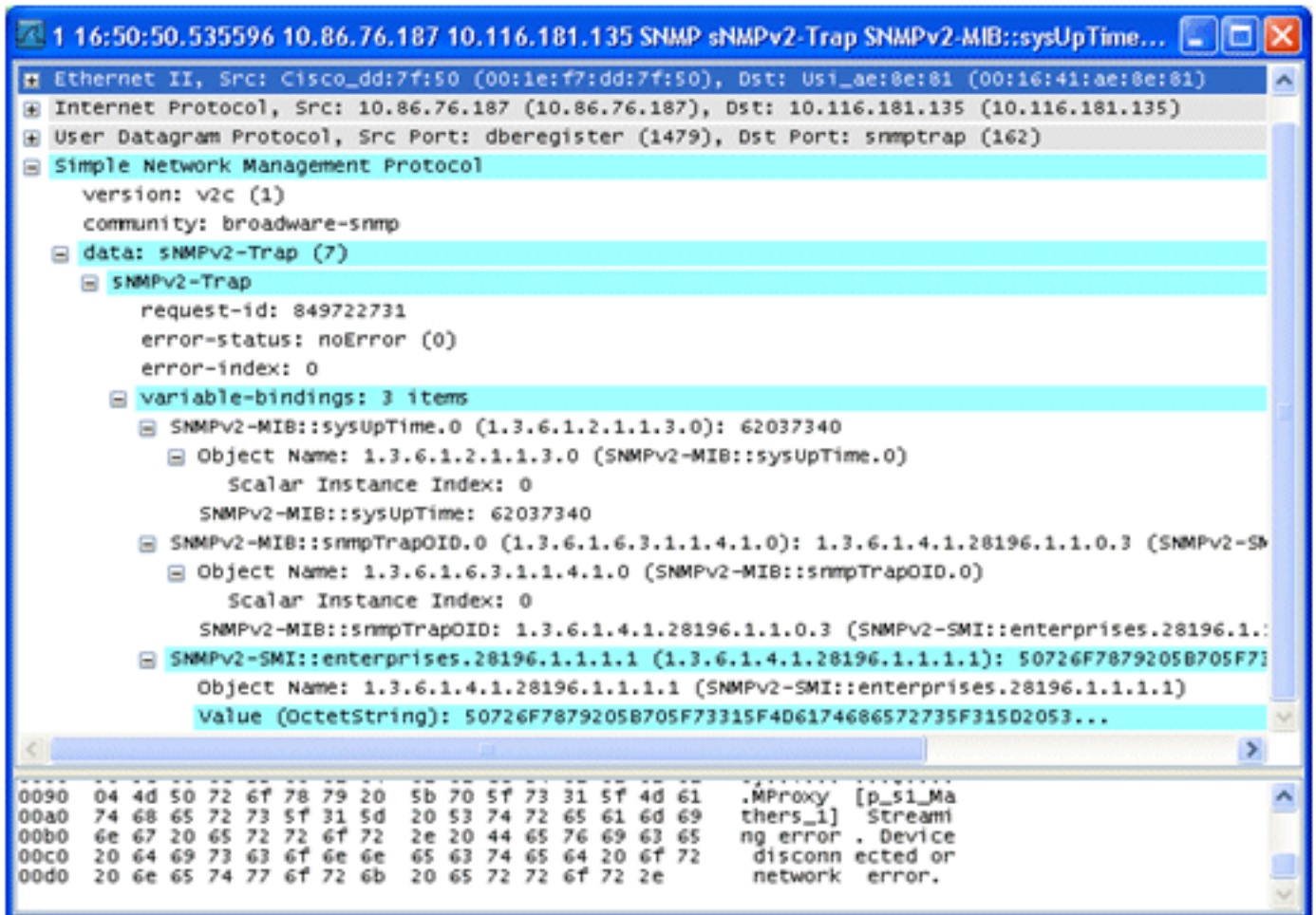
Após ter atualizado **destinos da armadilha de SNMP** no console VSMC, verifique que estão colocados com sucesso em **/usr/BWhttpd/etc/snmpd.conf**:

```
bxb-vsm:~ # more /usr/BWhttpd/etc/snmpd.conf | grep trap2sink
# trap2sink: A SNMPv2c trap receiver
#trap2sink localhost broadware-snmp
trap2sink 10.116.181.137 broadware-snmp
```

Além do que armadilhas BROADWARE-EVENT-MIB, permitir o SNMP por este processo inicia algumas armadilhas genéricas do nível de sistema. Veja para uma descrição detalhada destas armadilhas adicionais.

## Apêndice A: Captações dos Ethernet de armadilhas bwConnectionEvent e bwProxyEvent

### A.1 bwConnectionEvent (fluindo o erro)



### A.2 bwProxyEvent (conectado ao dispositivo)

2 16:54:21.357170 10.86.76.187 10.116.181.135 SNMP sNMPv2-Trap SNMPv2-MIB::sysUpTi...

Frame 2 (205 bytes on wire, 205 bytes captured)

- Ethernet II, Src: Cisco\_dd:7f:50 (00:1e:f7:dd:7f:50), Dst: Usi\_ae:8e:81 (00:16:41:ae:8e:81)
- Internet Protocol, Src: 10.86.76.187 (10.86.76.187), Dst: 10.116.181.135 (10.116.181.135)
- User Datagram Protocol, Src Port: pacerforum (1480), Dst Port: snmptrap (162)
- Simple Network Management Protocol
  - version: v2c (1)
  - community: broadware-snmp
  - data: sNMPv2-Trap (7)
    - sNMPv2-Trap
      - request-id: 849722734
      - error-status: noError (0)
      - error-index: 0
      - variable-bindings: 3 items
        - SNMPv2-MIB::sysUpTime.0 (1.3.6.1.2.1.1.3.0): 62058424
          - Object Name: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)
          - Scalar Instance Index: 0
          - SNMPv2-MIB::sysUpTime: 62058424
        - SNMPv2-MIB::snmpTrapOID.0 (1.3.6.1.6.3.1.1.4.1.0): 1.3.6.1.4.1.28196.1.1.0.1 (SNMPv2-SMI::enterprises.28196.1.1.0.1)
          - Object Name: 1.3.6.1.6.3.1.1.4.1.0 (SNMPv2-MIB::snmpTrapOID.0)
          - Scalar Instance Index: 0
          - SNMPv2-MIB::snmpTrapOID: 1.3.6.1.4.1.28196.1.1.0.1 (SNMPv2-SMI::enterprises.28196.1.1.0.1)
        - SNMPv2-SMI::enterprises.28196.1.1.1.1 (1.3.6.1.4.1.28196.1.1.1.1): 50726F7879205B705F73315F406174686572735F31502043...
          - Object Name: 1.3.6.1.4.1.28196.1.1.1.1 (SNMPv2-SMI::enterprises.28196.1.1.1.1)
          - Value (OctetString): 50726F7879205B705F73315F406174686572735F31502043...

0070	00 06 0c 2b 06 01 04 01 81 dc 24 01 01 00 01 30	...+.... ..\$.....0
0080	4c 06 0c 2b 06 01 04 01 81 dc 24 01 01 01 01 04	L...+.... ..\$.....
0090	3c 50 72 6f 78 79 20 5b 70 5f 73 31 5f 4d 61 74	<Proxy [ p_sl_Mat
00a0	68 65 72 73 5f 31 5d 20 43 6f 6e 6e 65 63 74 65	hers_1] Connecte
00b0	64 20 74 6f 20 64 65 76 69 63 65 5b 31 5f 31 40	d to dev ice[1_1@
00c0	31 34 2e 31 31 34 2e 31 2e 32 35 5d 2e	14.114.1 .25]..

### A.3 bwConnectionEvent (incapaz de configurar ou aperto de mão)



## Apêndice B: Disparador para prender a matriz

Trigger	Trap Event	OID	bwEventDesc
Archive Started	bwArchiverEvent	1.3.6.1.4.1.28196.1.1.0.2	Start archive SUCCESSFUL for <a href="#">archive_name</a>
Archive Stopped	bwArchiverEvent	1.3.6.1.4.1.28196.1.1.0.2	Stop archive SUCCESSFUL for <a href="#">archive_name</a>
Loss of Connection to Device	bwConnectionEvent	1.3.6.1.4.1.28196.1.1.0.3	1. Proxy [ <a href="#">proxy_name</a> ] Streaming error. Device disconnected or network error. 2. Proxy [ <a href="#">proxy_name</a> ] Unable to configure or handshake with the device #a_#b@ip_address.
Proxy Added	bwProxyEvent	1.3.6.1.4.1.28196.1.1.0.1	Proxy [ <a href="#">proxy_name</a> ] started Successfully
Proxy Deleted	bwProxyEvent	1.3.6.1.4.1.28196.1.1.0.1	Proxy [ <a href="#">proxy_name</a> ] stopped
View Proxy	bwProxyEvent	1.3.6.1.4.1.28196.1.1.0.1	Proxy [ <a href="#">proxy_name</a> ] Connected to device #a_#b@ip_address

## Apêndice C: Definição BROADWARE-EVENT-MIB

```
BROADWARE-EVENT-MIB DEFINITIONS ::= BEGIN
```

```
IMPORTS
```

```

MODULE-IDENTITY, OBJECT-TYPE, Integer32, enterprises,
NOTIFICATION-TYPE FROM SNMPv2-SMI
SnmpAdminString FROM SNMP-FRAMEWORK-MIB
netSnmp FROM NET-SNMP-MIB
RowStatus, StorageType FROM SNMPv2-TC

```

InetAddressType, InetAddress FROM INET-ADDRESS-MIB

;

broadware MODULE-IDENTITY

LAST-UPDATED "200701300000Z"

ORGANIZATION "www.broadware.com"

CONTACT-INFO

"postal: BroadWare Support  
3333 Octavius Dr.  
Santa Clara CA 95054

email: support@broadware.com"

DESCRIPTION

"Top-level infrastructure of the Broadware enterprise MIB tree"

REVISION "200701300000Z"

DESCRIPTION

"First draft"

::= { enterprises 28196}

events OBJECT IDENTIFIER ::= { broadware 1 }

```
!--- !--- Broadware Notifications !--- broadwareEventNotificationPrefix OBJECT IDENTIFIER ::= {
events 1 } broadwareEventNotifications OBJECT IDENTIFIER ::= { broadwareEventNotificationPrefix
0 } broadwareEventNotificationObjects OBJECT IDENTIFIER ::= { broadwareEventNotificationPrefix 1
} !--- !--- Broadware Notificationi Desc !--- bwProxyEvent NOTIFICATION-TYPE OBJECTS {
bwEventDesc } STATUS current DESCRIPTION "Notification that the proxy hosted in Broadware Media
Server (BMS) has changed its state. Proxy is a process which maintains the view of a particular
video cam." ::= { broadwareEventNotifications 1 } bwArchiverEvent NOTIFICATION-TYPE OBJECTS {
bwEventDesc } STATUS current DESCRIPTION "Notification that the archiver hosted in Broadware
Media Server (BMS) has changed its state. Archiver stores the captured video information into a
secondary storage device." ::= { broadwareEventNotifications 2 } bwConnectionEvent NOTIFICATION-
TYPE OBJECTS { bwEventDesc } STATUS current DESCRIPTION "Notification that the network
connection has been lost with the encoder/ camera". ::= { broadwareEventNotifications 3 } !---
!--- Broadware Notification Objects !--- bwEventDesc OBJECT-TYPE SYNTAX SnmpAdminString MAX-
ACCESS accessible-for-notify STATUS current DESCRIPTION "This object describes the event
corresponding to the notifying entity." ::= { broadwareEventNotificationObjects 1 } END
```

## [Anexo D: Armadilhas adicionais VS](#)

Trap	Trigger Criteria	Variable Bindings				
		MIB	Object NAME	OID	Type	VALUE
Partition Disk Space Usage	Any partition >90% full	DISMAN-EXPRESSION-MIB	sysUpTimeInstance	1.3.6.1.2.1.1.3.0	TimeTick	<time> <variable>
		SNMPv2-MIB	snmpTrapOID	1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1 (mteTriggerFired)
		DISMAN-EVENT-MIB	mteHotTrigger	1.3.6.1.2.1.88.2.1.1.0	string	dskTable
		DISMAN-EVENT-MIB	mteHotTargetName	1.3.6.1.2.1.88.2.1.2.0	string	0
		DISMAN-EVENT-MIB	mteHotContextName	1.3.6.1.2.1.88.2.1.3.0	string	0
		DISMAN-EVENT-MIB	mteHotOID	1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.9.1.100.2 (dskErrorFlag)
		DISMAN-EVENT-MIB	mteHotValue	1.3.6.1.2.1.88.2.1.5.0	integer	1
		UCD-SNMP-MIB	dskPath	1.3.6.1.4.1.2021.9.1.2.2	string	/proc (directory)
		UCD-SNMP-MIB	dskErrorMsg	1.3.6.1.4.1.2021.9.1.101.2	string	/proc: less than 10% Free
HTTPD Process Check	<1 or >100 httpd processes running	DISMAN-EXPRESSION-MIB	sysUpTimeInstance	1.3.6.1.2.1.1.3.0	TimeTick	<time> <variable>
		SNMPv2-MIB	snmpTrapOID	1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1 (mteTriggerFired)
		DISMAN-EVENT-MIB	mteHotTrigger	1.3.6.1.2.1.88.2.1.1.0	string	procTable
		DISMAN-EVENT-MIB	mteHotTargetName	1.3.6.1.2.1.88.2.1.2.0	string	0
		DISMAN-EVENT-MIB	mteHotContextName	1.3.6.1.2.1.88.2.1.3.0	string	0
		DISMAN-EVENT-MIB	mteHotOID	1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.2.1.100.1 (prErrorFlag)
		DISMAN-EVENT-MIB	mteHotValue	1.3.6.1.2.1.88.2.1.5.0	integer	1
		UCD-SNMP-MIB	prNames	1.3.6.1.4.1.2021.2.1.2.1	string	httpd
		UCD-SNMP-MIB	prErrMsg	1.3.6.1.4.1.2021.2.1.101.1	string	Too few httpd running (n = 0)
CPU Load Average	1min >12% 5min >12% 15min >12%	DISMAN-EXPRESSION-MIB	sysUpTimeInstance	1.3.6.1.2.1.1.3.0	TimeTick	<time> <variable>
		SNMPv2-MIB	snmpTrapOID	1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.2.1.88.2.0.1 (mteTriggerFired)
		DISMAN-EVENT-MIB	mteHotTrigger	1.3.6.1.2.1.88.2.1.1.0	string	lsTable
		DISMAN-EVENT-MIB	mteHotTargetName	1.3.6.1.2.1.88.2.1.2.0	string	0
		DISMAN-EVENT-MIB	mteHotContextName	1.3.6.1.2.1.88.2.1.3.0	string	0
		DISMAN-EVENT-MIB	mteHotOID	1.3.6.1.2.1.88.2.1.4.0	OID	1.3.6.1.4.1.2021.10.1.100 (lsErrorFlag)
		DISMAN-EVENT-MIB	mteHotValue	1.3.6.1.2.1.88.2.1.5.0	integer	1
		UCD-SNMP-MIB	lsNames	1.3.6.1.4.1.2021.10.1.2	string	Load-15
		UCD-SNMP-MIB	lsErrMsg	1.3.6.1.4.1.2021.10.1.101	string	15 min Load Average too high (= 0.24)

## Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)