Содержание

Введение

Этот документ предназначен к ПО Cisco Video Surveillance Manager (VSM) клиенты рабочий Медиасервер систем видеонаблюдения (VSMS) 6.2.x или ранее кто интересуется мониторингом для доступности IP-камеры через SNMP или инициированный SNMP механизм предупреждения. Это содержит обзор SNMP, поймавшего в ловушку сервисы, доступные в VSMS 6.2.x и ранее развернуть простое предупреждение IP-камеры и стратегию мониторинга сети, а также пошаговый процесс для включения SNMP на VSMS в дополнение к основным диаграммам вызовов и примерам устранения проблем. Эта конфигурация не применяется ни к кому 6.3.x или более поздние версии VSMS, поскольку VSMS 6.3 представляет информационную панель Контроля исправности, которая устранит процедуры, содержавшиеся в этом документе через введение всесторонней платформы мониторинга систем видеонаблюдения. Кроме того, **BROADWARE-MIB-СОБЫТИЙ** больше не будет использоваться в 6.3.x и более поздние версии VSMS. См. 6.3 документаций для получения информации относительно доступного мониторинга сети и стратегии управления камеры в 6.3.x и более поздние версии VSMS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

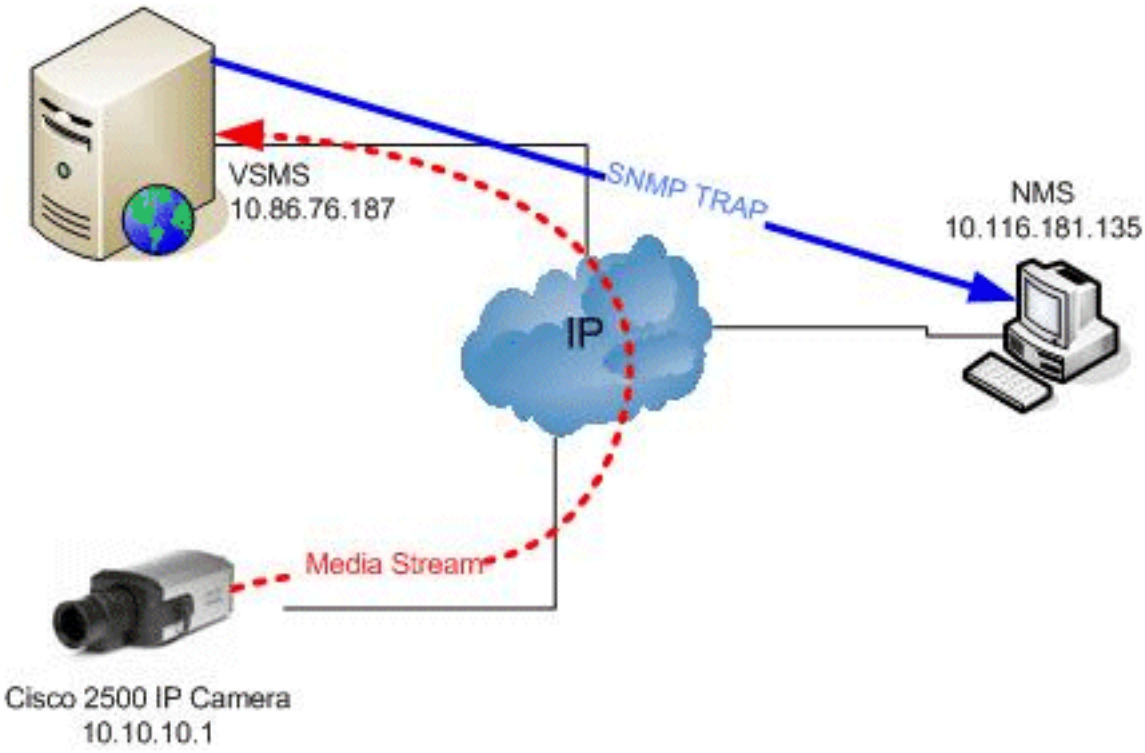
- IP-камера Cisco 2500 рабочих Микропрограммных обеспечений 2.1.2
- VSMS выполнение 6.2.1-12d
- Диспетчер операций систем видеонаблюдения (VSOM), работающий 4.2.1-14

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Схема сети



Обзор SNMP

Протокол SNMP описывает платформу клиент-сервер, позволяющую SNMP Manager собирать информацию от (или настраивать) Агент SNMP, использующий Информационную базу управления (MIB), где Агент SNMP работает на любом управляемом узле. Включенный в этот информационный сбор способность к Агенту SNMP передать данные для управления к SNMP Manager, не требуясь, чтобы сделать так SNMP Manager. Этот управляемый узел (который помещает Агента SNMP) мог быть сервером, IP-телефоном, сетевым маршрутизатором, сетевым коммутатором или любым устройством с поддержкой IP, которое включает программный стек SNMP и поэтому способно к тому, чтобы быть управляемым через SNMP. Таким образом, SNMP позволяет менеджерам сети удаленно контролировать и управлять развитием сетевых объектов.

Существуют три обычно развертываемых версии SNMP: SNMPv1, SNMPv2c и SNMPv3. Остаток от этой статьи концентрируется в частности на SNMPv2c, Поймавшем в ловушку возможность согласно конфигурации в VSMS. Использование вышеупомянутой схемы как ссылка, Агент SNMP находится на сервере VSMS (управляемый узел) и сообщает SNMP, Поймавший в ловушку информация SNMP Manager, который мог быть сторонней платформой Системы управления сетью (NMS). Общие NMSs включают Диспетчер узлов сети HP Open View, Netview Tivoli и Solarwinds Orion.

Примечание: Подробный анализ протокола SNMP, включая различия в управлении версиями, выходит за рамки этого документа.

Trap-сообщения SNMPv2c используют транспортный протокол UDP (dest. порт 162) и поэтому считаются ненадежными. Например, если trap-сообщение SNMP, сообщая об ошибке потоковой передачи IP-камеры будет потеряно в пути NMS, то VSMS будет не знать об этой потере, и trap-сообщение SNMP не будет ретранслироваться VSMS. В результате оператор Network Operations Center (NOC), полагающийся исключительно на SNMP, будет не знать о сбое IP-камеры. Это ненадежное поведение является применимым ко всему SNMP, поймавшему в ловушку архитектуры, и является поэтому не определенным для VSMS. Помимо использования порта 162 UDP (характерный для всего SNMP, поймавшего в ловушку реализации), каждое trap-сообщение, переданное от VSMS до NMS, включает некоторую другую диагностическую информацию стандартного события:

- Строка имени и пароля SNMPv2c? broadware-snmp?Демон приемника прерываний NMS должен быть настроен таким образом, что это способно к обработке и предоставлению входу trap-сообщений SNMPv2c с сообществом? broadware-snmp?. Названия сообщества SNMP являются подобным простому паролю механизмом обеспечения безопасности, предназначенным для аутентификации связи между NMS SNMP, и SNMP управлял узлом. В отличие от версии SNMP или адреса станции назначения захвата, по умолчанию VSMS? broadware-snmp? не может быть изменен. Посмотрите, что раздел назвал Процедуру настройки подтверждать, какие аспекты реализации SNMP VSMS конфигурируемы.
- sysUpTime (OID 1.3.6.1.2.1.1.3)sysUpTime является объектом некорпоративной базы управляющих данных, определенным в MIB SNMPv2 (RFC 1213), и сообщает о времени (за сотые части секунды), так как часть управления сетью системы в последний раз повторно инициализировалась, который, как правило, совпадает со временем работы без сбоев сервера VSMS.

Для использования процедуры ниже для мониторинга компонентов VSMS, NMS, способный к получению, парсингу, и представление trap-сообщений SNMPv2c требуется. Далее, для перевода trap-сообщений **SNMPv2c BROADWARE-MIB-СОБЫТИЙ** в понятные названия события файл определения **BROADWARE-EVENT-MIB.txt** должен быть установлен на NMS. Чтобы к загруженному этот файл в соответствующем формате, соединитесь с VSMS через **http://<ip_address_or, называют of_vsms>/vsmc.html**, перешли **Назначениям TRAP-СООБЩЕНИЯ SNMP** и щелкают по гиперссылке **Базы MIB (управляющей информации для событий) VS**.

VSMS способен к передаче и SNMPv1 и trap-сообщения SNMPv2c, невзирая на то, что SNMPv2c рекомендуется из-за расширенной Поддержки MIB. VSMS также поддерживает SNMPv2c, сообщают сообщениям, которые идентичны сообщениям прерывания, за исключением того, что inform-сообщение подтверждено NMS. В результате уровень надежности добавлен.

Примечание: В VSMS 6.2 и ранее только поддерживается незапрашиваемый захват SNMP. Последовательный опрос SNMP **BROADWARE-MIB-СОБЫТИЙ** на VSMS от Станции NMS является недопустимой операцией. В Приложении C пункт **MAX-ACCESS** для объекта **bwEventDesc** установлен в **accessible-notify**.

SNMP VSMS, контролирующий примеры использования

Пример использования #1 мониторинг доступности IP-камеры

VSMS поддерживает экземпляр прокси для каждого шифратора, который используется, чтобы получить поток мультимедиа от шифратора и записать его в совместно используемую память для более поздней передачи к VSOM просмотр клиента, другой VSMS (дочерний канал), или к локальному хранилищу через архив. С точки зрения протокола каждый экземпляр прокси ведет себя согласно типу устройства, являющемуся управляемым и тип настройки носителя. Например, прокси, созданные для IP-камер Cisco 4500, настроенных для 1080P использующий H.264, будут сначала аутентифицироваться VSMS. Последующий за аутентификацией, VSMS сообщит камере своих желаемых свойств потоковой передачи с помощью Протокола RTSP. Наконец, с помощью потоковой передачи информации, полученной через RTSP, IP-камера Cisco 4500 начнет передавать свой поток сред потоком к VSMS использование Протокола RTP. Эта вся транзакция может быть перехвачена на CLI VSMS с помощью **tcpdump?** команда *<IP_of_encoding_device>* **хоста nn**.

Примечание: IP-камеры Cisco будут аутентифицировать VSMS по умолчанию с помощью HTTPS в 6.x версии VSMS. При использовании шифраторов не-Cisco проверьте для требования проверки подлинности и метода привлекательной поддержкой стороннего продукта.

После квитирования с HTTPS и RTSP, VSMS передаст trap-сообщение **bwProxyEvent**, сообщая `Proxy [proxy_name] Connected to device #a_#b@ip_address`, где *#a* является номером ввода устройства, и *#b* является номером конфигурации для ввода. Важно обратить внимание, что это trap-сообщение **bwProxyEvent** передано после квитирования HTTPS/RTSP, независимо относительно того, получается ли поток мультимедиа VSMS. См. Приложение A. 2 для примера **bwProxyEvent Связанный к Устройству** поймали в ловушку и проверяют **ims.log** для успеха/статуса ошибки уровня управления RTSP и HTTPS:

- Успешное квитирование HTTPS:
- Неуспешное квитирование HTTPS:
- Неуспешное квитирование RTSP:

Если или HTTPS или соединения RTSP от VSMS до IP-камеры неуспешны, в конечном счете, trap-сообщение **bwConnectionEvent** передается, сообщая `Proxy [proxy_name] Unable to configure or handshake with the device #a_#b@ip_address` и сопровождается этим сообщением **ims.log**:

См. Приложение A. 3 для примера? Неспособный настроить или квитировать? Trap-сообщение bwConnectionEvent.

После успешного квитирования, если прокси VSMS не в состоянии получать поток мультимедиа от шифратора (IP-камера) сроком на 10-е, VSMS передает trap-сообщение **bwConnectionEvent**, сообщающее, что существует проблема, соединяющаяся с данным шифратором. Это trap-сообщение сообщает `Proxy [proxy_name] Streaming error. Device disconnected or network error` и сопровождается этими **ims.log** записями:

Консультируйтесь с драйверами или проанализируйте трассировки сети для подтверждения протокола подтверждения связи и поведения протокола RTSP шифратора не-Cisco.

Примечание: Вообще говоря, в конечном счете аналоговая камера, связанная с многопортовым кодером, теряет питание или удалена из сервиса, шифратор все еще передаст черный экран потоком. В результате VSMS не будет в состоянии понять аналоговый сбой камеры, и никакая дорожка SNMP для потоковой передачи потери не будет генерироваться.

Пример использования #2 Архив запускает/останавливает Уведомление

bwArchiverEvent Notification-Type может использоваться, чтобы сигнализировать запуск и остановить события настроенной петли, повторения или одноразовых архивов.

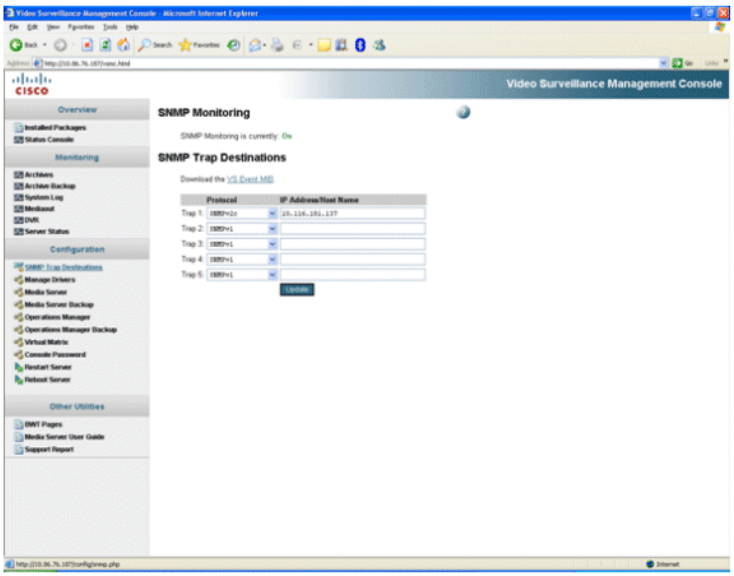
- Когда архив запущен, trap-сообщение **bwArchiverEvent** генерируется, сообщая `Start archive SUCCESSFUL for archive_name`.
- Когда архив остановлен, trap-сообщение **bwArchiverEvent** генерируется, сообщая `Stop archive SUCCESSFUL for archive_name`.

Обзор VSMC для SNMP Настройки

Консоль управления систем видеонаблюдения (VSMC) является находящимся на web GUI конфигурации, используемым, чтобы просмотреть и настроить опции управления системами VSMS непосредственно, не используя VSOM или API HTTP. Вообще говоря, VSOM является стоящим с пользователем GUI, прежде всего используемым, чтобы настроить и просмотреть специализированные элементы, такие как прокси, архивы, события и представления. С другой стороны элементы управления в масштабе всей системы могут быть просмотрены и настроены в VSMC, включая системные журналы, SNMP, резервные копирования данных, и т.д.

Процедура конфигурации

Обратитесь VSMC Медиасервера через **http://<ip_or называют of_media_server>/vsmc.html**, выбирают **SNMP Trap Destinations> SNMPv2c** от раскрывающегося списка **Протокола** и вводят IP-адрес NMS, которому будут передаваться trap-сообщения:

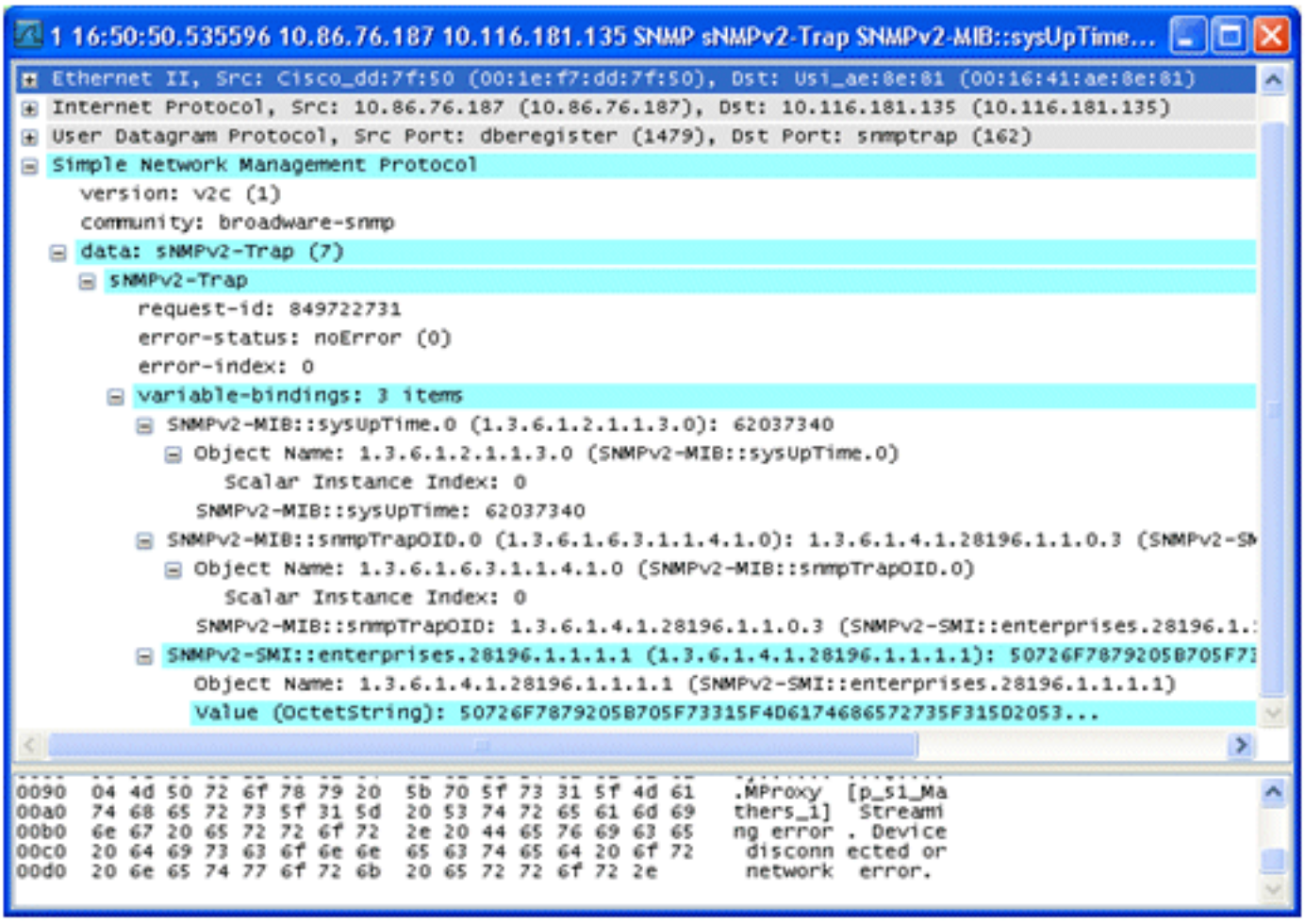


После обновления **Назначений TRAP-СООБЩЕНИЯ SNMP** в консоли VSMC проверьте, что они успешно размещены в**/usr/BWhttpd/etc/snmpd.conf**:

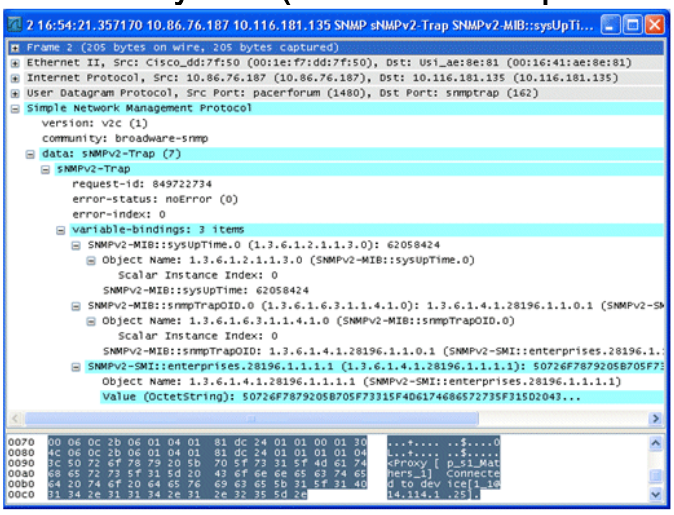
В дополнение к Trap-сообщениям BROADWARE-MIB-СОБЫТИЙ, включая SNMP на этот процесс инициирует некоторые trap-сообщения уровня системы общего назначения. Видьте подробное описание этих дополнительных trap-сообщений.

Приложение A: Перехваты Ethernet bwConnectionEvent и Trap-сообщений bwProxyEvent

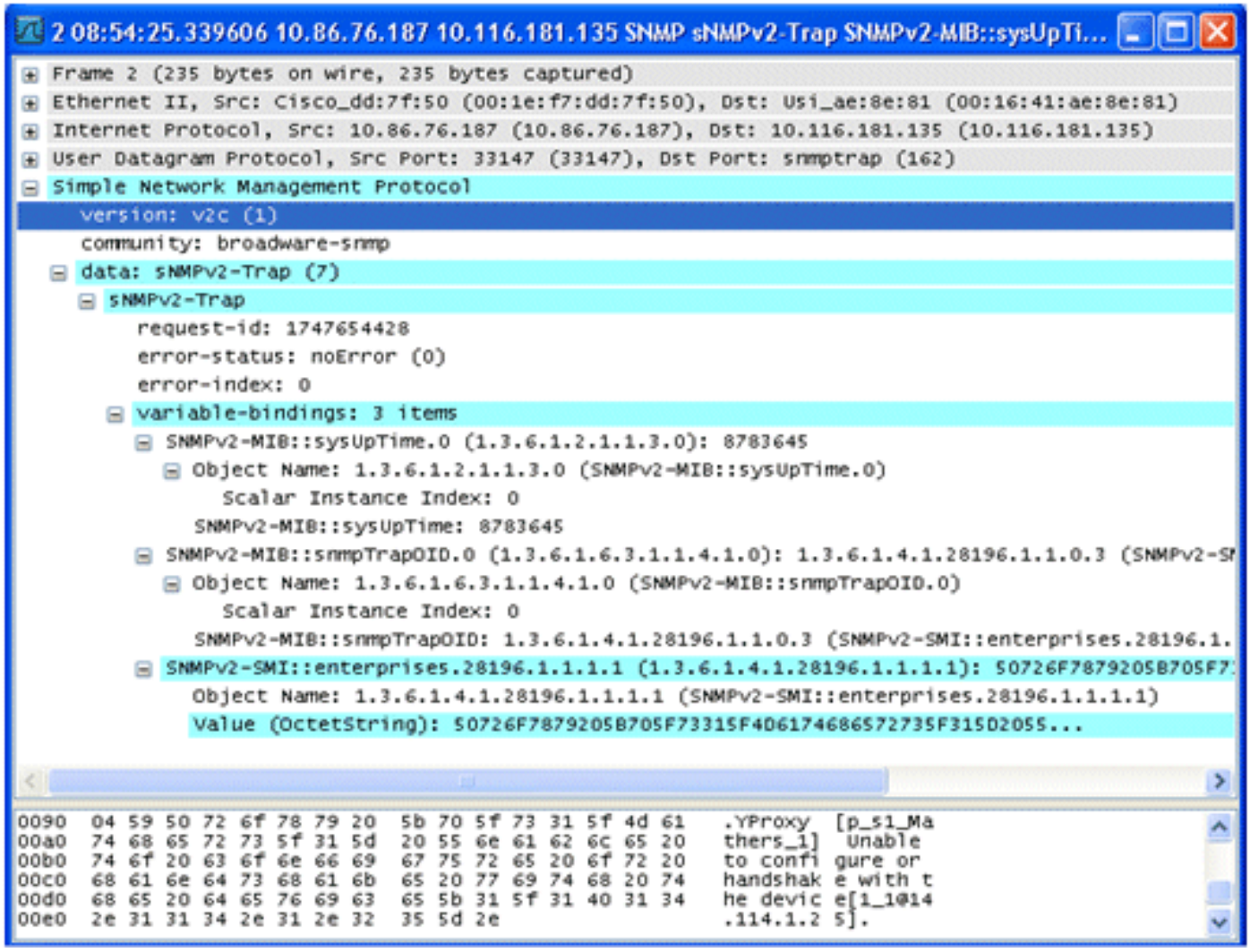
O. 1 bwConnectionEvent (Передающий Ошибку потоком)



O. 2 bwProxyEvent (Связанный с Устройством)



O. 3 bwConnectionEvent (Неспособный настроить или квитировать)

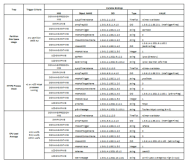


Приложение Б: Триггер для захвата матрицы

Trigger	Trap Event	OID	bwEventDesc
Archive Started	bwArchiverEvent	1.3.6.1.4.1.28196.1.1.0.2	Start archive SUCCESSFUL for archive_name
Archive Stopped	bwArchiverEvent	1.3.6.1.4.1.28196.1.1.0.2	Stop archive SUCCESSFUL for archive_name
Loss of Connection to Device	bwConnectionEvent	1.3.6.1.4.1.28196.1.1.0.3	1. Proxy [proxy_name] Streaming error. Device disconnected or network error. 2. Proxy [proxy_name] 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 [proxy_name] started Successfully
Proxy Deleted	bwProxyEvent	1.3.6.1.4.1.28196.1.1.0.1	Proxy [proxy_name] stopped
View Proxy	bwProxyEvent	1.3.6.1.4.1.28196.1.1.0.1	Proxy [proxy_name] Connectedto device #a_#b@ip_address

Приложение B: Определение BROADWARE-MIB-СОБЫТИЙ

Приложение D: Дополнительные trap-сообщения VSMS



Дополнительные сведения

- Cisco Systems – техническая поддержка и документация