Обнаружение и удаление зависших соединений по TCP с помощью протокола SNMP

Содержание

Введение

Этот документ описывает, как использовать Протокол SNMP, чтобы обнаружить и очиститься, "завис" TCP - подключения на устройстве Cisco IOS. Документ также объясняет, что SNMP возражает, что вы используете для этой цели.

Названный раздел, Сценарий PERL, чтобы Обнаружить и Очиститься "Завис" TCP - подключения, предоставляет ссылку на сценарий PERL, который внедряет эти инструкции.

Предварительные условия

Требования

Читатели данного документа должны обладать знаниями по следующим темам:

- Поймите, как просмотреть информацию о TCP - подключении об устройствах Cisco
- Общее использование **обхода** SNMP, **доберитесь**, **get-next**, и **установите** команды
- Поймите, как настроить SNMP на устройстве Cisco

Используемые компоненты

Этот документ применяется к маршрутизаторам Cisco и коммутаторам, выполняющим программное обеспечение IOS, поддерживающее TCP-MIB и модули CISCO-TCP-MIB.

Примечание: Модуль CISCO-TCP-MIB не загружен по умолчанию в NET-SNMP. Если модуль MIB не загружен в вашей системе, необходимо использовать OID для ссылки на объект вместо его названия.

Сведения в этом документе основываются на всех версиях программного и аппаратного обеспечения IOS.

Информация основана на этой версии NET-SNMP:

- Версия 5.1.2 NET-SNMP, доступная в http://www.net-snmp.org/

Сценарий PERL был протестирован с версиями PERL:

- 5.005_03 на FreeBSD
- 5.8.0 на Solaris 5.8
- 5.005_02 — поставленный как часть CiscoWorks SNMS на Microsoft Windows 2000
- ActivePerl 5.8.4 на Microsoft Windows 2000, доступном в http://www.activestate.com/Products/ActivePerl/.

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 Технические рекомендации Cisco. Условные обозначения.

Общие сведения

Подробные данные объектов MIB — включают идентификаторы объекта (OID)

Это объекты, которые вы используете:

От модуля CISCO-TCP-MIB:

- ciscoTcpConnInBytes, OID 1.3.6.1.4.1.9.9.6.1.1.1.1Количество байтов вводит на этом соединении.
- ciscoTcpConnInPkts, OID 1.3.6.1.4.1.9.9.6.1.1.1.2Количество пакетов вводит на этом соединении.
- ciscoTcpConnOutBytes, OID 1.3.6.1.4.1.9.9.6.1.1.1.3Количество байтов выведено на этом соединении
- ciscoTcpConnOutPkts, OID 1.3.6.1.4.1.9.9.6.1.1.1.4Количество пакетов выведено на этом соединении.
- ciscoTcpConnRetransPkts, OID 1.3.6.1.4.1.9.9.6.1.1.1.7Количество пакетов

ретранслируется на этом соединении.
- ciscoTcpConnRto, OID 1.3.6.1.4.1.9.9.6.1.1.1.9Значение таймаута retransmit для этого соединения.

От модуля TCP-MIB:

- tcpConnState, OID 1.3.6.1.2.1.6.13.1.1Статус для этого соединения.

Существует больше подробных данных об этих объектах в Подробной информации об Объекте MIB.

Используйте SNMP, чтобы Обнаружить, если TCP - подключение "Зависает"

Сводка

Эти шаги помогают вам определять, " зависает ли TCP - подключение ":

1. Чтобы определить, поддерживаются ли ciscoTcpConnRetransPkts и объекты ciscoTcpConnRto в устройстве, выполняют операцию **SNMP get-next** на ciscoTcpConnRto и проверяют, возвращены ли любые объекты.**Примечание:** Только необходимо проверить один объект, потому что поддержка их обоих была добавлена в то же время.**Примечание:** Не все устройства Cisco поддерживают последние два объекта (ciscoTcpConnRetransPkts и ciscoTcpConnRto), но их использование может увеличить точность обнаружения.Если ciscoTcpConnRetransPkts и объекты ciscoTcpConnRto **поддерживаются**, продолжаются к Шагу 2.Если ciscoTcpConnRetransPkts и объекты ciscoTcpConnRto **не** поддерживаются, продолжаются к Шагу 3.
2. Все объекты поддерживаются. Поскольку каждый TCP - подключение проверяет их:ciscoTcpConnOutBytes 0.ciscoTcpConnOutPkts 0.ciscoTcpConnRetransPkts больше, чем 0.ciscoTcpConnRto больше, чем 20,000.**Примечание:** Эти 20,000 могут быть уменьшены для ускорения обнаружения. Требуется приблизительно одна минута для Rto для достижения 20,000, как только соединение "зависнуто". Однако меньшие значения могут уменьшить точность результата.Если все предыдущие истинны, то этот TCP - подключение "зависнут" и может быть очищен. Продолжите Использовать SNMP для Очистки TCP - подключения, который "Зависает".
3. Только первые четыре объекта поддерживаются. Поскольку каждый TCP - подключение проверяет их:ciscoTcpConnInBytes больше, чем 0.ciscoTcpConnInPkts 0.ciscoTcpConnOutBytes 0.ciscoTcpConnOutPkts 0.Ждите несколько секунд и **заставьте** объекты снова проверять, что это не был TCP - подключение в процессе того, чтобы быть установленным.**Примечание:** Первые две проверки (положительное число входных байтов, но никаких входящих пакетов) могут казаться странными, но они были проверены против многочисленных устройств и версий IOS.**Примечание:** Версии IOS, которые поддерживают все шесть объектов, могут не показать это поведение и, поэтому, тест в Шаге 2 не включает эти первые два теста.Если все объекты встречают тесты оба раза тогда, этот TCP - подключение "зависнут" и может быть очищен. Продолжите Использовать SNMP для Очистки TCP - подключения, который "Зависает".

Пошаговые инструкции

Значения в данном примере:

- Имя хоста устройства = nms-7206a (поддерживает все объекты),
- Имя хоста устройства b = nms-1605 (поддерживает только первые четыре объекта),
- Сообщество для чтения = общественность
- Сообщество с правом записи = частный

Замените строки имени и пароля и имя хоста в этих командах:

1. Определите, возражает ли это поддержки устройств ciscoTcpConnRetransPkts и ciscoTcpConnRto:Выполните операцию **SNMP get-next** на ciscoTcpConnRto: **`snmpgetnext -c public nms-7206a ciscoTcpConnRto`** Если объекты **поддерживаются**, вы видите ответ как это:`CISCO-TCP-MIB::ciscoTcpConnRto.14.32.100.75.2065.172.18.86.111.23092 =`
   `INTEGER: 303 milliseconds`
   Примечание: Индекс, используемый для этих объектов, в этом случае `14.32.100.75.2065.172.18.86.111.23092`, является конкатенацией local IP address — 14.32.100.75, локальный номер порта TCP — 2065, удаленный IP-адрес — 172.18.86.111, и удаленный номер порта TCP — 23092.Return для ciscoTcpConnRto. Перейдите к шагу 2.Если объекты **не** являются поддержкой, вы видите ответ как это: **`snmpgetnext -c public nms-1605 ciscoTcpConnRto`** `CISCO-FLASH-MIB::ciscoFlashDevicesSupported.0 = INTEGER: 1` Return не для объекта ciscoTcpConnRto. Точный объект возвратился, не важно. Продолжитесь к Шагу 3.
2. **Получите** информацию о каждом соединении TCP для устройства, которые поддерживают все шесть объектов в таблице TCP - подключения Cisco.Выполните операцию **SNMP get-next** на ciscoTcpConnOutBytes, ciscoTcpConnOutPkts, ciscoTcpConnRetransPkts и ciscoTcpConnRto: **`snmpgetnext -c public nms-7206a ciscoTcpConnOutBytes ciscoTcpConnOutPkts ciscoTcpConnRetransPkts ciscoTcpConnRto`** Вы видите ответ как это:`CISCO-TCP-MIB::ciscoTcpConnOutBytes.14.32.100.75.2065.172.18.86.111.23092 = Counter32: 383556`
   `CISCO-TCP-MIB::ciscoTcpConnOutPkts.14.32.100.75.2065.172.18.86.111.23092 = Counter32: 8061`
   `CISCO-TCP-MIB::ciscoTcpConnRetransPkts.14.32.100.75.2065.172.18.86.111.23092 = Counter32: 2`
   `CISCO-TCP-MIB::ciscoTcpConnRto.14.32.100.75.2065.172.18.86.111.23092 = INTEGER: 303 milliseconds`
   Проверьте их:ciscoTcpConnOutBytes 0.ciscoTcpConnOutPkts 0.ciscoTcpConnRetransPkts больше, чем 0.ciscoTcpConnRto больше, чем 20,000.**Примечание:** Эти 20,000 могут быть уменьшены для ускорения обнаружения. Требуется приблизительно одна минута для Rto для достижения 20,000, как только соединение "зависнуто". Однако меньшие значения могут уменьшить точность результата.Если все они истинны, то этот TCP - подключение "зависнут" и может быть очищен. Продолжите Использовать SNMP для Очистки TCP - подключения, который "Зависает".Продолжите **обходить** таблицу TCP - подключения. Чтобы сделать это, выполняйте операцию **SNMP get-next** неоднократно, поскольку вы проверяете для "зависнувших" соединений, с помощью возвращенных объектов, таких как они:
   `snmpgetnext -c public nms-7206a ciscoTcpConnOutBytes.14.32.100.75.2065.172.18.86.111.23092 ciscoTcpConnOutPkts.14.32.100.75.2065.172.18.86.111.23092 ciscoTcpConnRetransPkts.14.32.100.75.2065.172.18.86.111.23092 ciscoTcpConnRto.14.32.100.75.2065.172.18.86.111.23092`Проверьте каждую запись с помощью предшествующего теста, пока операция **get-next** не возвратит объекты этим способом:`CISCO-TCP-MIB::ciscoTcpConnInPkts.14.32.100.75.2065.172.18.86.111.23092 = Counter32: 8097`
   `CISCO-TCP-MIB::ciscoTcpConnElapsed.14.32.100.75.2065.172.18.86.111.23092 =`
   `Timeticks: (17296508) 2 days, 0:02:45.08`

```
CISCO-TCP-MIB::ciscoTcpConnFastRetransPkts.14.32.100.75.2065.172.18.86.111.23092 =
Counter32: 0
CISCO-FLASH-MIB::ciscoFlashDevicesSupported.0 = INTEGER: 5
```

Вы теперь обошли все TCP - подключения на этом устройстве, и вы сделаны.

3. **Получите** информацию о каждом соединении TCP для устройства, которые только поддерживают первые четыре объекта в таблице TCP - подключения Cisco.Выполните операцию **SNMP get-next** на ciscoTcpConnInBytes, ciscoTcpConnInPkts ciscoTcpConnOutBytes, и ciscoTcpConnOutPkts:
snmpgetnext -c public nms-1605 ciscoTcpConnInBytes ciscoTcpConnInPkts ciscoTcpConnOutBytes ciscoTcpConnOutPkts Вы видите ответ как это:
```
CISCO-TCP-MIB::ciscoTcpConnInBytes.14.32.6.185.23.14.32.100.33.2249 = Counter32: 68
CISCO-TCP-MIB::ciscoTcpConnInPkts.14.32.6.185.23.14.32.100.33.2249 = Counter32: 12
CISCO-TCP-MIB::ciscoTcpConnOutBytes.14.32.6.185.23.14.32.100.33.2249 = Counter32: 170
CISCO-TCP-MIB::ciscoTcpConnOutPkts.14.32.6.185.23.14.32.100.33.2249 = Counter32: 17
```
Проверьте, чтобы видеть, истинны ли они:ciscoTcpConnInBytes больше, чем 0.ciscoTcpConnInPkts 0.ciscoTcpConnOutBytes 0.ciscoTcpConnOutPkts 0.Ждите несколько секунд и **получите** объекты снова. Проверьте, что это не был TCP - подключение в процессе того, чтобы быть установленным.Если все вышеупомянутое истинно, то этот TCP - подключение "зависнут" и может быть очищен. Продолжите Использовать SNMP для Очистки TCP - подключения, который "Зависает".Продолжите **обходить** таблицу TCP - подключения. Чтобы сделать это, выполняйте операцию **SNMP get-next** неоднократно, поскольку вы проверяете для "зависнувших" соединений, с помощью возвращенных объектов, таких как они:
snmpgetnext -c public nms-1605 ciscoTcpConnInBytes.14.32.6.185.23.14.32.100.33.2249 ciscoTcpConnInPkts.14.32.6.185.23.14.32.100.33.2249 ciscoTcpConnOutBytes.14.32.6.185.23.14.32.100.33.2249 ciscoTcpConnOutPkts.14.32.6.185.23.14.32.100.33.2249 Проверьте каждую запись с помощью предшествующего теста, пока операция **get-next** не возвратит объекты этим способом:
```
CISCO-TCP-MIB::ciscoTcpConnOutBytes.14.32.6.185.23.14.32.100.33.4184 = Counter32:
170
CISCO-TCP-MIB::ciscoTcpConnOutPkts.14.32.6.185.23.14.32.100.33.4184 = Counter32: 17
CISCO-TCP-MIB::ciscoTcpConnInPkts.14.32.6.185.23.14.32.100.33.4184 = Counter32: 12
CISCO-TCP-MIB::ciscoTcpConnElapsed.14.32.6.185.23.14.32.100.33.4184 = Timeticks: (4345)
0:00:43.45
```
Вы теперь обошли все TCP - подключения на этом устройстве, и вы сделаны.

Используйте SNMP для Очистки TCP - подключения, который "Зависает"

Пошаговые инструкции

Можно использовать SNMP для очистки "зависнувшего" TCP - подключения. Команда SNMP эквивалентна **clear tcp, локальному** *<local_ip> <local_port>* **удаленная** *<remote_ip>* команда *<remote_port>*. Объект, который вы используете для очистки линии, является **tcpConnState**.

Для очистки "зависнувшего" TCP - подключения с SNMP выполните эту команду:

snmpset -c private nms-7206a tcpConnState.14.32.100.75.2065.172.18.86.111.23092 integer deleteTCB TCP-MIB::tcpConnState.14.32.100.75.2065.172.18.86.111.23092 = INTEGER: deleteTCB(12)

Примечание: Индекс, используемый для этих объектов, в этом случае 14.32.100.75.2065.172.18.86.111.23092, является конкатенацией local IP address —

14.32.100.75, локальный номер порта TCP — 2065, удаленный IP-адрес — 172.18.86.111, и удаленный номер порта TCP — 23092.

Примечание: Необходимо использовать точный индекс, который вы определили, был "зависнут" в SNMP Использования, чтобы Обнаружить, если TCP - подключение "Зависает". Знайте, что эта команда разъединяет TCP - подключение без предупреждения.

Подробная информация об объекте MIB

```
.1.3.6.1.4.1.9.9.6.1.1.1.1
ciscoTcpConnInBytes OBJECT-TYPE
        -- FROM CISCO-TCP-MIB
        SYNTAX          Counter
        MAX-ACCESS      read-only
        STATUS          Current
        DESCRIPTION     "Number of bytes that have been input on this TCP
                        connection."
::= { ciscoTcpConnEntry 1 }

.1.3.6.1.4.1.9.9.6.1.1.1.2
ciscoTcpConnOutBytes OBJECT-TYPE
        -- FROM CISCO-TCP-MIB
        SYNTAX          Counter
        MAX-ACCESS      read-only
        STATUS          Current
        DESCRIPTION     "Number of bytes that have been output on this TCP
                        connection."
::= { ciscoTcpConnEntry 2 }

.1.3.6.1.4.1.9.9.6.1.1.1.3
ciscoTcpConnInPkts OBJECT-TYPE
        -- FROM CISCO-TCP-MIB
        SYNTAX          Counter
        MAX-ACCESS      read-only
        STATUS          Current
        DESCRIPTION     "Number of packets that have been input on this TCP
                        connection."
::= { ciscoTcpConnEntry 3 }

.1.3.6.1.4.1.9.9.6.1.1.1.4
ciscoTcpConnOutPkts OBJECT-TYPE
        -- FROM CISCO-TCP-MIB
        SYNTAX          Counter
        MAX-ACCESS      read-only
        STATUS          Current
        DESCRIPTION     "Number of packets that have been output on this TCP
                        connection."
::= { ciscoTcpConnEntry 4 }

.1.3.6.1.4.1.9.9.6.1.1.1.7
ciscoTcpConnRetransPkts OBJECT-TYPE
        -- FROM CISCO-TCP-MIB
        SYNTAX          Counter
        MAX-ACCESS      read-only
        STATUS          Current
        DESCRIPTION     "The total number of packets retransmitted due to a timeout -
                        that is, the number of TCP segments transmitted containing
                        one or more previously transmitted octets."
::= { ciscoTcpConnEntry 7 }

.1.3.6.1.4.1.9.9.6.1.1.1.9
```

```
ciscoTcpConnRto OBJECT-TYPE
        -- FROM CISCO-TCP-MIB
        SYNTAX          Integer
        MAX-ACCESS      read-only
        STATUS          Current
        DESCRIPTION     "The current value used by a TCP implementation for the
                        retransmission timeout."
::= { ciscoTcpConnEntry 9 }

.1.3.6.1.2.1.6.13.1.1
tcpConnState OBJECT-TYPE
        -- FROM RFC1213-MIB
        SYNTAX          Integer { closed(1), listen(2), synSent(3), synReceived(4),
                        established(5), finWait1(6), finWait2(7), closeWait(8), lastAck(9),
                        closing(10), timeWait(11), deleteTCB(12) }
        MAX-ACCESS      read-write
        STATUS          Mandatory
        DESCRIPTION     "The state of this TCP connection.

                        The only value which may be set by a management
                        station is deleteTCB(12).  Accordingly, it is
                        appropriate for an agent to return a `badValue'
                        response if a management station attempts to set
                        this object to any other value.

                        If a management station sets this object to the
                        value deleteTCB(12), then this has the effect of
                        deleting the TCB (as defined in RFC 793) of the
                        corresponding connection on the managed node,
                        resulting in immediate termination of the
                        connection.

                        As an implementation-specific option, a RST

                        segment may be sent from the managed node to the
                        other TCP endpoint (note however that RST segments
                        are not sent reliably)."
::= { tcpConnEntry 1 }
```

Сценарий PERL, чтобы обнаружить и очиститься "завис" TCP - подключения

Эта ссылка предоставляет архивному файлу сценарий PERL и необходимые модули MIB. Щелкните правой кнопкой по ссылке и сохраните файл к вашей системе.

- fixTCPhang.tgz

Файлы в архиве:

- bin/fixTCPhang.pl
- mibs/CISCO-SMI.my
- mibs/CISCO-TCP-MIB.my

Для извлечения сценария и модулей MIB используйте утилиту, такую как gzip и tar на подобные UNIX операционные системы. Например, для извлечения файлов к **/ tmp**, предполагающему, что архивный файл размещен в **/ tmp**:

```
cd /tmp; gzip -dc fixTCPhang.tgz | tar -xvf -
```

Примечание: Вы, возможно, должны отредактировать первую линию сценария для

определения местоположения Perl.

Используйте winzip или другие утилиты на операционных системах Microsoft Windows для извлечения файлов. При извлечении файлов к **c:\tmp** тогда, вы не должны задавать-m опцию при выполнении сценария.

Вызовите файлы с этой командой:

```
fixTCPhang.pl -c public -C private -f nms-7206a
```

Поскольку каждый "завис", TCP - подключения нашли наблюдение линии как эти выходные данные:

```
Found bad TCP connection: Local IP: 14.32.100.75 port 23 Remote IP: 172.18.100.33 port 47878:
CLEARED
```

Поскольку строка имени и пароля для чтения и записи была предоставлена, и-f опция была задана, сценарий очистил соединение. Обратите внимание на оператор `CLEARED` в конце выходных данных.

Сценарий поддерживает версии SNMP 1, 2c, и 3. При определении версии SNMP 3 необходимо задать всю информацию для аутентификации в-v аргументе. Это - пример использования v3 SNMP:

```
fixTCPhang.pl -v "3 -a MD5 -u chelliot -A chelliot -l authNoPriv" -f nms-dmz-ap1200-b
```

Команды IOS для настройки v3 SNMP для предыдущего примера:

```
snmp-server group chelliot-group v3 auth write v1default snmp-server user chelliot chelliot-
group v3 auth md5 chelliot
```

Примечание: Кажется, существует дефект в Версии Windows NET-SNMP, используемого в этом тестировании. Дефект не позволяет аутентификации SHA работать должным образом.

Существует несколько других опций, которые можно использовать с этим сценарием. Некоторые опции сценария включают, где найти служебные программы управляемые с помощью командной строки NET-SNMP и где найти модули MIB, если они не находятся в**/tmp/mibs**. Можно также просмотреть эту сводку тех опций:

```
fixTCPhang.pl fixTCPhang.pl [-dfhV -c <read_community> -C <write_community> -m <mib_directory> -
p <command_path> -t <timeout> -v <snmp_version>] <device> Version 1.2 Detect hung TCP
connections on <device>, optionally clearing them. Options: -c Specify read community string.
Defaults to public. -C Specify the readwrite community string. No default. Must be supplied for
the script to clear hung connections. -d Turn on debug mode. -f Fix or clear any hung TCP
connections found. -h Print this message. -m Specify the directory to find CISCO-SMI.my and
CISCO-TCP-MIB.my. Defaults to /tmp/mibs. -p Where to find the net-snmp utilities. Optional if
the utilities are in the path. -t SNMP Timeout value. Defaults to 5 sec. -v Specify SNMP version
to use: One of 1, 2c, or 3. If 3 is specified then this option must include all of the
authentication information for SNMPv3. For example: "3 -a MD5 -u chelliot -A chelliot -l
authNoPriv" Note: NET-SNMP seems to have a bug with SHA authentication on Windows. See the NET-
SNMP documentation for more information. Defaults to SNMP version 1. -V Print version number.
```

Дополнительные сведения

- Техническая поддержка - Cisco Systems