使用SNMP，如何检测和清除暂停TCP连接

目录

简介

本文描述如何使用简单网络管理协议(SNMP)检测和清除在Cisco IOS设备的暂停的TCP连接。本文也解释您为此使用的SNMP对象。

部分有资格的， Perl脚本检测和清除暂停TCP连接，提供链路给实现这些说明的Perl脚本。

先决条件

要求

本文档的读者应掌握以下这些主题的相关知识：

- 知道如何查看关于Cisco设备的TCP连接信息
- SNMP一般用途**走**，**获得**，**得到下**和**集**命令
- 知道如何配置在Cisco设备的SNMP

使用的组件

本文适用于Cisco路由器并且交换支持TCP-MIB和CISCO-TCP-MIB模块的运行IOS软件。

注意： 默认情况下CISCO-TCP-MIB模块在NET-SNMP没有装载。如果MIB模块在您的系统没有装

载，您必须使用OID参考对象而不是其名称。

本文档中的信息根据所有IOS软件和硬件版本。

信息根据NET-SNMP此版本：

- NET-SNMP在http://www.net-snmp.org/的版本5.1.2联机

Perl脚本用PERL版本测试：

- 在FreeBSD的5.005_03
- 5.8.0在Solaris 5.8
- 5.005_02 —被发运作为在Microsoft Windows 2000的CiscoWorks SNMS一部分
- 在Microsoft Windows 2000的ActivePerl 5.8.4，在 http://www.activestate.com/Products/ActivePerl/的联机 。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

MIB对象的详细信息—包括对象标识符(OIDs)

这些是您使用的对象：

从CISCO-TCP-MIB模块：

- ciscoTcpConnInBytes， OID .1.3.6.1.4.1.9.9.6.1.1.1.1在此连接输入的字节数。
- ciscoTcpConnInPkts， OID 1.3.6.1.4.1.9.9.6.1.1.1.2信息包输入编号在此连接的。
- ciscoTcpConnOutBytes， OID .1.3.6.1.4.1.9.9.6.1.1.1.3在此连接输出的字节数
- ciscoTcpConnOutPkts， OID .1.3.6.1.4.1.9.9.6.1.1.1.4packets output编号在此连接的。
- ciscoTcpConnRetransPkts， OID .1.3.6.1.4.1.9.9.6.1.1.1.7在此连接重传的数据包数量。
- ciscoTcpConnRto， OID .1.3.6.1.4.1.9.9.6.1.1.1.9此连接的重新传输超时值。

从TCP-MIB模块：

- tcpConnState， OID .1.3.6.1.2.1.6.13.1.1此连接的状态。

有在这些对象的更多详细信息在详细的MIB对象信息。

如果TCP连接暂停，请使用SNMP检测

摘要

这些步骤帮助您确定TCP连接是否暂停：

1. 为了确定是否设备支持ciscoTcpConnRetransPkts和ciscoTcpConnRto对象，请执行在

ciscoTcpConnRto的一Snmp get-next操作并且验证，如果任何对象返回。**注意：** 因为他们两个的支持同时，被添加了您只需要检查一个对象。**注意：** 不是所有的Cisco设备支持最后两个对象(ciscoTcpConnRetransPkts和ciscoTcpConnRto)，但是他们的使用能增加检测的准确性。如果支持ciscoTcpConnRetransPkts和ciscoTcpConnRto对象，请继续对步骤2。如果不支持ciscoTcpConnRetransPkts和ciscoTcpConnRto对象，请继续对步骤3。

2. 支持所有对象。对于每TCP连接请检查这些：ciscoTcpConnOutBytes是0。ciscoTcpConnOutPkts是0。ciscoTcpConnRetransPkts比0极大。ciscoTcpConnRto比20,000极大。**注意：** 可以减少20,000加速检测。一旦暂停，需要一分钟Rto的能到达20,000连接。然而，更加小的值可能减少结果的准确性。如果所有上一个是真的，则暂停此TCP连接并且可以被清除。继续使用SNMP清除暂停的TCP连接。
3. 支持仅前四个对象。对于每TCP连接请检查这些：ciscoTcpConnInBytes比0极大。ciscoTcpConnInPkts是0。ciscoTcpConnOutBytes是0。ciscoTcpConnOutPkts是0。等一些秒钟并且再**获得**对象验证它不是TCP连接在设立过程中。**注意：** 前两检查(输入字节，但是没有输入信息包正数)可能似乎奇怪，但是他们验证许多设备和IOS版本。**注意：** 支持全部六个对象的IOS版本可能不陈列此行为，并且，因此，测验在步骤2不包括这些前两测验。如果所有对象满足两次此TCP连接然后暂停测验并且可以被清除。继续使用SNMP清除暂停的TCP连接。

逐步指导

在本例中的值是：

- 设备主机名a = nms-7206a (支持所有对象)
- 设备主机名b = nms-1605 (支持仅前四个对象)
- ??_末期社区=公共
- 写入公用=私有

替换社区字符串和主机名在这些命令：

1. 确定是否此设备支持ciscoTcpConnRetransPkts和ciscoTcpConnRto对象：执行在ciscoTcpConnRto的一**Snmp get-next**操作：
   snmpgetnext -c public nms-7206a ciscoTcpConnRto 如果支持对象您看到象这样的一答复：
   ```
   CISCO-TCP-MIB::ciscoTcpConnRto.14.32.100.75.2065.172.18.86.111.23092 =
       INTEGER: 303 milliseconds
   ```
   注意： 用于这些对象的索引，在这种情况下`14.32.100.75.2065.172.18.86.111.23092`，是本地IP地址的串联— 14.32.100.75，本地TCP端口号— 2065，远程IP地址— 172.18.86.111和远程TCP端口号— 23092。返回是为ciscoTcpConnRto。继续执行步骤 2。如果对象不是支持，您看到象这样的一答复：
   snmpgetnext -c public nms-1605 ciscoTcpConnRto `CISCO-FLASH-MIB::ciscoFlashDevicesSupported.0 = INTEGER: 1` 返回不是为ciscoTcpConnRto对象。返回的确切的对象不是重要。继续执行步骤 3。
2. **获得**关于每TCP连接的信息在思科TCP连接表里支持全部六个对象的设备的。执行在ciscoTcpConnOutBytes、ciscoTcpConnOutPkts、ciscoTcpConnRetransPkts和ciscoTcpConnRto的一**Snmp get-next**操作：
   snmpgetnext -c public nms-7206a ciscoTcpConnOutBytes ciscoTcpConnOutPkts ciscoTcpConnRetransPkts ciscoTcpConnRto 您看到象这样的一答复：
   ```
   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
   ```

验证这些：ciscoTcpConnOutBytes是0。ciscoTcpConnOutPkts是0。ciscoTcpConnRetransPkts比0极大。ciscoTcpConnRto比20,000极大。**注意：** 可以减少20,000加速检测。一旦暂停，需要一分钟Rto的能到达20,000连接。然而，更加小的值可能减少结果的准确性。如果所有这些是真的，则暂停此TCP连接并且可以被清除。继续使用SNMP清除暂停的TCP连接。继续**走**TCP连接表。为了执行此，请重复执行一Snmp get-next操作，您检查暂停的连接，使用返回的对象例如这些， ：

```
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请检查每个条目使用前次试验，直到**得到下**操作如此返回对象：

```
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
```

您当前走了在此设备的所有TCP连接，并且您执行。

3. **获得**关于每TCP连接的信息在思科TCP连接表里只支持前四个对象的设备的。执行在ciscoTcpConnInBytes、ciscoTcpConnInPkts ciscoTcpConnOutBytes和ciscoTcpConnOutPkts的一Snmp get-next操作：

```
snmpgetnext -c public nms-1605 ciscoTcpConnInBytes ciscoTcpConnInPkts ciscoTcpConnOutBytes
ciscoTcpConnOutPkts
```

您看到象这样的一答复：

```
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
```

确认这些是否是真的：ciscoTcpConnInBytes比0极大。ciscoTcpConnInPkts是0。ciscoTcpConnOutBytes是0。ciscoTcpConnOutPkts是0。等一些秒钟并且再**获得**对象。验证它不是TCP连接在设立过程中。如果所有在上面**是**真的，则暂停此TCP连接并且可以被清除。继续使用SNMP清除暂停的TCP连接。继续**走**TCP连接表。为了执行此，请重复执行一Snmp get-next操作，您检查暂停的连接，使用返回的对象例如这些， ：

```
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 请检查每个条目使用前次试验，直到**得到下**操作如此返回对象：

```
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
```

您当前走了在此设备的所有TCP连接，并且您执行。

请使用SNMP清除暂停的TCP连接

逐步指导

您能使用SNMP清除一暂停的TCP连接。SNMP命令与**清楚tcp本地<local_ip> <local_port>远程<remote_ip> <remote_port>**命令是等同的。您使用清除线路的对象是**tcpConnState**。

为了清除与SNMP的一暂停的TCP连接，请发出此命令：

```
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)
```

注意： 用于这些对象的索引，在这种情况下`14.32.100.75.2065.172.18.86.111.23092`，是本地IP地址的串联— 14.32.100.75，本地TCP端口号— 2065，远程IP地址— 172.18.86.111和远程TCP端口号— 23092。

注意： 您必须使用您确定是检测的暂停的在使用中的SNMP的确切的索引，如果TCP连接暂停。注意此命令断开一TCP连接，无需警告。

详细的MIB对象信息

```
.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 }
```

检测和清除的Perl脚本暂停TCP连接

此链路提供一份归档文件Perl脚本和必要的MIB模块。用鼠标右键单击链路并且保存文件到您的系统。

- fixTCPhang.tgz

文件在存档是：

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

要解压缩脚本和MIB模块，请使用一个工具例如gzip和tar在类似UNIX的操作系统。例如，抽出文件到假设的**/tmp**归档文件在**/tmp**安置：

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

注意： 您可能需要编辑脚本的第一行指定PERL的位置。

请使用winzip或其他工具在Microsoft Windows操作系统抽出文件。如果抽出文件对**c:\tmp**您然后不必须指定- m选项，当您运行脚本。

调用文件用此命令：

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

对于每个暂停的TCP连接找到您发现一条线路类似此输出：

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

当提供了读写团体串和- f选项指定，脚本清除了连接。注释语句在输出结束时。

脚本支持SNMP版本1， 2c和3。如果指定SNMP版本3，您必须指定所有在- v参数的认证信息。这是用途示例SNMP v3 ：

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

IOS命令配置前一个示例的SNMP v3是：

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

注意： 那里看来是在用于此测试的NET-SNMP windows版本的一bug。bug不允许SHA验证适当地运作。

有您能以此脚本使用的几个其它选项。如果他们不在**/tmp/mibs**，某些脚本选项在哪里在哪里包括查找NET-SNMP命令行实用工具和查找MIB模块。您能也查看那些选项此摘要：

```
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.
```

相关信息

- 技术支持 - Cisco Systems