Cómo detectar y conexiones TCP claramente colgadas usando el SNMP

Contenido

Introducción

Este documento describe cómo utilizar el Simple Network Management Protocol (SNMP) para detectar y las conexiones TCP claramente colgadas en un dispositivo Cisco IOS. El documento también explica el SNMP se opone que usted utiliza el para este propósito.

La sección titulada, la secuencia de comandos Perl para detectar y las conexiones TCP claramente colgadas, proporciona un link a una secuencia de comandos Perl que implemente estas instrucciones.

prerrequisitos

Requisitos

Quienes lean este documento deben tener conocimiento de los siguientes temas:

- Entienda cómo ver la información de la conexión TCP sobre los dispositivos de Cisco
- Uso general del **paseo** SNMP, **comandos get, get-next, y set**
- Entienda cómo configurar el SNMP en un dispositivo de Cisco

Componentes Utilizados

Este documento se aplica a los routeres Cisco y al Switches que funcionan con el software IOS que soporta el TCP-MIB y los módulos CISCO-TCP-MIB.

Nota: El módulo CISCO-TCP-MIB no se carga por abandono en el NET-SNMP. Si el módulo MIB no se carga en su sistema, usted debe utilizar el OID para referirse a un objeto en vez de su nombre.

La información en este documento se basa en todo el software IOS y versiones de hardware.

La información se basa sobre esta versión del NET-SNMP:

- Versión 5.1.2 NET-SNMP disponible en http://www.net-snmp.org/

La secuencia de comandos Perl fue probada con las versiones de PERL:

- 5.005_03 en FreeBSD
- 5.8.0 en Solaris 5.8
- 5.005_02 — enviado como parte de los CiscoWorks SNM en el Microsoft Windows 2000
- ActivePerl 5.8.4 en el Microsoft Windows 2000, disponible en http://www.activestate.com/Products/ActivePerl/ .

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Antecedentes

Detalles de los objetos de MIB — Incluye los identificadores de objeto (los OID)

Éstos son los objetos que usted utiliza:

Del módulo CISCO-TCP-MIB:

- ciscoTcpConnInBytes, OID .1.3.6.1.4.1.9.9.6.1.1.1.1La cantidad de bytes entrada en esta conexión.
- ciscoTcpConnInPkts, OID 1.3.6.1.4.1.9.9.6.1.1.1.2El número de paquetes entrados en esta conexión.
- ciscoTcpConnOutBytes, OID .1.3.6.1.4.1.9.9.6.1.1.1.3La cantidad de bytes hecha salir en esta conexión
- ciscoTcpConnOutPkts, OID .1.3.6.1.4.1.9.9.6.1.1.1.4El número de paquetes hechos salir en esta conexión.
- ciscoTcpConnRetransPkts, OID .1.3.6.1.4.1.9.9.6.1.1.1.7El número de paquetes retransmitidos en esta conexión.

- ciscoTcpConnRto, OID .1.3.6.1.4.1.9.9.6.1.1.1.9El valor de agotamiento del tiempo de la retransmisión para esta conexión.

Del módulo TCP-MIB:

- tcpConnState, OID .1.3.6.1.2.1.6.13.1.1El estatus para esta conexión.

Hay más detalles en estos objetos en la información detallada del objeto de MIB.

Utilice el SNMP para detectar si una conexión TCP cuelga

Resumen

Estos pasos le ayudan a determinar si una conexión TCP cuelga:

1. Para determinar si el ciscoTcpConnRetransPkts y los objetos del ciscoTcpConnRto se soportan en el dispositivo, realizan una operación del **Get Next** SNMP en el ciscoTcpConnRto y la verifican si se vuelven algunos objetos.**Nota:** Usted necesita solamente marcar un objeto porque el soporte para ambos ellos fue agregado al mismo tiempo.**Nota:** No todos los dispositivos de Cisco soportan los dos objetos más recientes (ciscoTcpConnRetransPkts y ciscoTcpConnRto), pero su uso puede aumentar la exactitud de la detección.Si se soportan el ciscoTcpConnRetransPkts y los objetos del ciscoTcpConnRto, proceda al paso 2.Si el ciscoTcpConnRetransPkts y los objetos del ciscoTcpConnRto no se soportan, proceda al paso 3.
2. Se soportan todos los objetos. Para cada control de la conexión TCP éstos:los ciscoTcpConnOutBytes son 0.los ciscoTcpConnOutPkts son 0.el ciscoTcpConnRetransPkts es mayor de 0.el ciscoTcpConnRto es mayor de 20,000.**Nota:** Los 20,000 se pueden reducir para acelerar la detección. Tarda un minuto o para que Rto alcance tan 20,000 una vez que se cuelga la conexión. Sin embargo, valores más pequeños pueden reducir la exactitud del resultado.Si todos los anteriores son verdades, después esta conexión TCP se cuelga y puede ser borrada. Proceda a utilizar el SNMP para borrar una conexión TCP que cuelgue.
3. Solamente se soportan los primeros cuatro objetos. Para cada control de la conexión TCP éstos:el ciscoTcpConnInBytes es mayor de 0.los ciscoTcpConnInPkts son 0.los ciscoTcpConnOutBytes son 0.los ciscoTcpConnOutPkts son 0.Espere algunos segundos y **consiga los** objetos otra vez para verificar que no era una conexión TCP en curso de establecimiento.**Nota:** Los primeros dos controles (un número positivo de bytes de la entrada pero de ningunos paquetes de entrada) pueden parecer extraños, pero ellos fueron verificados contra los varios dispositivos y las versiones de IOS.**Nota:** Las versiones de IOS que soportan los seis objetos pueden no exhibir este comportamiento y, por lo tanto, la prueba en el paso 2 no incluyen estas primeras dos pruebas.Si toda la reunión de los objetos las pruebas ambas veces después esta conexión TCP se cuelga y puede ser borrada. Proceda a utilizar el SNMP para borrar una conexión TCP que cuelgue.

Instrucciones Paso a Paso

Los valores en este ejemplo son:

- Nombre del host del dispositivo a = nms-7206a (soporta todos los objetos)
- Nombre del host del dispositivo b = nms-1605 (soportes solamente los primeros cuatro

objetos)
- Comunidad de lectura = público
- Escribir comunidad = soldado

Substituya las cadenas de comunidad y el nombre de host en estos comandos:

1. Determine si este soportes de dispositivo el ciscoTcpConnRetransPkts y los objetos del ciscoTcpConnRto:Realice una operación del **Get Next SNMP** en el ciscoTcpConnRto: **`snmpgetnext -c public nms-7206a ciscoTcpConnRto`** Si se soportan los objetos usted ve una respuesta como esto:
```
CISCO-TCP-MIB::ciscoTcpConnRto.14.32.100.75.2065.172.18.86.111.23092 =
     INTEGER: 303 milliseconds
```
Nota: El índice usado para estos objetos, en este caso `14.32.100.75.2065.172.18.86.111.23092`, es una concatenación del IP Address local — 14.32.100.75, el número del puerto TCP local — 2065, el IP Address remoto — 172.18.86.111, y el número del puerto TCP remoto — 23092.La vuelta está para el ciscoTcpConnRto. Continúe en el paso 2.Si los objetos no son soporte, usted ve una respuesta como esto:
`snmpgetnext -c public nms-1605 ciscoTcpConnRto` `CISCO-FLASH-MIB::ciscoFlashDevicesSupported.0 = INTEGER: 1` La vuelta no está para el objeto del ciscoTcpConnRto. El objeto exacto vuelto no es importante. Proceda al paso 3.
2. **Consiga la** información sobre cada conexión TCP para dispositivos que soporta los seis objetos en la tabla de la conexión TCP de Cisco.Realice una operación del **Get Next SNMP** en los ciscoTcpConnOutBytes, los ciscoTcpConnOutPkts, el ciscoTcpConnRetransPkts, y el ciscoTcpConnRto:
`snmpgetnext -c public nms-7206a ciscoTcpConnOutBytes ciscoTcpConnOutPkts ciscoTcpConnRetransPkts ciscoTcpConnRto` Usted ve una respuesta como esto:
```
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
```
Verifique éstos:los ciscoTcpConnOutBytes son 0.los ciscoTcpConnOutPkts son 0.el ciscoTcpConnRetransPkts es mayor de 0.el ciscoTcpConnRto es mayor de 20,000.**Nota:** Los 20,000 se pueden reducir para acelerar la detección. Tarda un minuto o para que Rto alcance tan 20,000 una vez que se cuelga la conexión. Sin embargo, valores más pequeños pueden reducir la exactitud del resultado.Si todos los éstos son verdades, después esta conexión TCP se cuelga y puede ser borrada. Proceda a utilizar el SNMP para borrar una conexión TCP que cuelgue.Continúe **recorriendo la** tabla de la conexión TCP. Para hacer esto, realice una operación del **Get Next** SNMP en varias ocasiones como usted marca para saber si hay conexiones colgadas, usando los objetos vueltos tales como éstos:
`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`Marque cada entrada usando la prueba anterior hasta que la operación del **Get Next** vuelva los objetos de este modo:
```
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
```
Usted ahora ha recorrido todas las conexiones TCP en este dispositivo y le hacen.
3. **Consiga la** información sobre cada conexión TCP para dispositivos que soporta solamente

los primeros cuatro objetos en la tabla de la conexión TCP de Cisco.Realice una operación del **Get Next** SNMP en el ciscoTcpConnInBytes, los ciscoTcpConnOutBytes de los ciscoTcpConnInPkts, y los ciscoTcpConnOutPkts:

snmpgetnext -c public nms-1605 ciscoTcpConnInBytes ciscoTcpConnInPkts ciscoTcpConnOutBytes ciscoTcpConnOutPkts Usted ve una respuesta como esto:

```
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
```

Marque para ver si éstos son verdades:el ciscoTcpConnInBytes es mayor de 0.los ciscoTcpConnInPkts son 0.los ciscoTcpConnOutBytes son 0.los ciscoTcpConnOutPkts son 0.Espere algunos segundos y **consiga los** objetos otra vez. Verifique que no fuera una conexión TCP en curso de establecimiento.Si todos los antedichos **son** verdades, después esta conexión TCP se cuelga y puede ser borrada. Proceda a utilizar el SNMP para borrar una conexión TCP que cuelgue.Continúe **recorriendo la** tabla de la conexión TCP. Para hacer esto, realice una operación del **Get Next** SNMP en varias ocasiones como usted marca para saber si hay conexiones colgadas, usando los objetos vueltos tales como éstos:

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 Marque cada entrada usando la prueba anterior hasta que la operación del **Get Next** vuelva los objetos de este modo:

```
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
```

Usted ahora ha recorrido todas las conexiones TCP en este dispositivo y le hacen.

Utilice el SNMP para borrar una conexión TCP que cuelgue

Instrucciones Paso a Paso

Usted puede utilizar el SNMP para borrar una conexión TCP colgada. El comando SNMP es equivalente al **comando clear tcp local <local_ip> <local_port> remote <remote_ip> <remote_port>**. El objeto que usted utiliza para borrar una línea es **tcpConnState**.

Para borrar una conexión TCP colgada con el SNMP, publique este comando:

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)`

Nota: El índice usado para estos objetos, en este caso `14.32.100.75.2065.172.18.86.111.23092`, es una concatenación del IP Address local — 14.32.100.75, el número del puerto TCP local — 2065, el IP Address remoto — 172.18.86.111, y el número del puerto TCP remoto — 23092.

Nota: Usted debe utilizar el índice exacto que usted determinó era SNMP funcionando colgado para detectar si una conexión TCP cuelga. Sea consciente que este comando desconecta una conexión TCP sin el cuidado.

Información detallada del objeto de 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 }
```

Secuencia de comandos Perl a detectar y conexiones TCP claramente colgadas

Este link proporciona un archivo con una secuencia de comandos Perl y los módulos MIB necesarios. Haga clic con el botón derecho del ratón el link y salve el archivo a su sistema.

- fixTCPhang.tgz

Los archivos en el archivo son:

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

Para extraer el script y los módulos MIB, utilice una utilidad tal como gzip y alquitrán en a Unix-como los sistemas operativos. Por ejemplo, extraer los archivos a **/tmp** si se asume que el archivo está puesto en **/tmp**:

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

Nota: Usted puede necesitar editar la primera línea del script para especificar la ubicación del Perl.

Utilice el winzip u otras utilidades en los sistemas operativos de Microsoft Windows para extraer los archivos. Si usted extrae los archivos a **c:\tmp** entonces que usted no tiene que especificar -opción m cuando usted ejecuta el script.

Invoque los archivos con este comando:

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

Para cada las conexiones TCP colgadas encontradas le consideran una línea como esta salida:

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

Mientras que la cadena de comunidad de lectura/escritura fue suministrada y - la opción f fue especificada, el script borró la conexión. Observe la declaración BORRADA en el extremo de la salida.

El script soporta las versiones de SNMP 1, 2c, y 3. Si usted especifica el SNMP versión 3, usted debe especificar toda la información de autenticación en - el argumento v. Éste es un ejemplo del v3 SNMP que usa:

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

Los comandos ios de configurar el v3 SNMP para el ejemplo anterior son:

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

Nota: Aparece ser un bug en la versión de Windows del NET-SNMP usada en esta prueba. El bug no permite que la autenticación del SHA trabaje correctamente.

Hay varias otras opciones que usted puede utilizar con este script. Algunas de las opciones del script incluyen donde encontrar las utilidades de línea de comando NET-SNMP y donde encontrar los módulos MIB si no están en **/tmp/mibs**. Usted puede también ver este resumen de esas opciones:

```
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.
```

Información Relacionada

- Soporte Técnico - Cisco Systems