

Simple Network Management Protocol (SNMP)-Traps

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[SNMP-Traps verwenden](#)

[Beispiele für Traps, die von Cisco IOS gesendet werden](#)

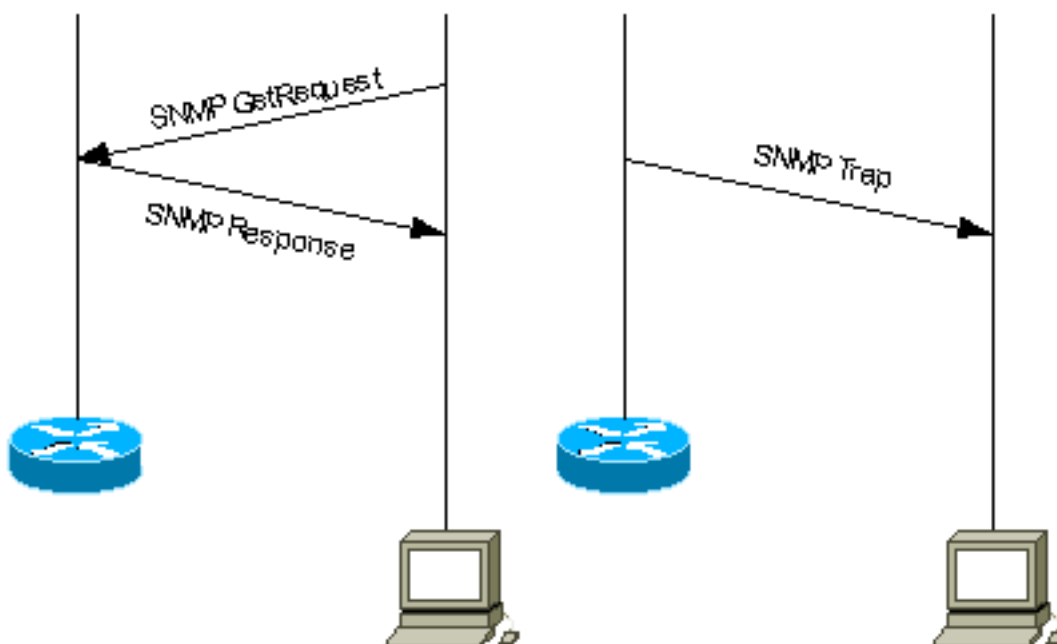
[Zugehörige Informationen](#)

Einführung

Dieses Dokument bietet eine Einführung in SNMP-Traps. Es zeigt, wie SNMP-Traps verwendet werden und welche Rolle sie bei der Verwaltung eines Datennetzwerks spielen.

SNMP-Traps ermöglichen es einem Agenten, die Managementstation über eine nicht angeforderte SNMP-Nachricht über schwerwiegende Ereignisse zu informieren.

In diesem Diagramm zeigt die Konfiguration auf der linken Seite ein Netzwerkmanagementsystem, das Informationen abfragt und eine Antwort erhält. Das Setup auf der rechten Seite zeigt einen Agenten, der ein unerwünschtes oder asynchrones Trap an das Netzwerkmanagementsystem (NMS) sendet.



Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

SNMP-Traps verwenden

SNMPv1 (Simple Network Management Protocol) und SNMPv2c unterstützen zusammen mit der zugehörigen Management Information Base (MIB) eine Trap-gesteuerte Benachrichtigung.

Die Idee hinter einer in einem Trap gesteuerten Benachrichtigung besteht darin, dass der Manager, wenn er für eine große Anzahl von Geräten verantwortlich ist und jedes Gerät über eine große Anzahl von Objekten verfügt, nicht in der Lage ist, Informationen von jedem Objekt auf jedem Gerät abzurufen oder anzufordern. Die Lösung besteht darin, dass jeder Agent auf dem verwalteten Gerät den Manager ohne vorherige Anfrage benachrichtigt. Dazu sendet er eine Meldung, die als Trap des Ereignisses bezeichnet wird.

Nachdem der Manager die Veranstaltung erhalten hat, zeigt der Manager sie an und kann je nach Veranstaltung eine Aktion durchführen. So kann der Manager beispielsweise direkt den Agenten abfragen oder andere zugehörige Geräte-Agenten abfragen, um ein besseres Verständnis der Veranstaltung zu erhalten.

Trap-Directed Notification kann zu erheblichen Einsparungen bei Netzwerk- und Agenten-Ressourcen führen, da keine leichtsinnigen SNMP-Anfragen mehr erforderlich sind. Es ist jedoch nicht möglich, das SNMP-Polling vollständig zu eliminieren. SNMP-Anfragen sind für die Erkennung und Topologieänderungen erforderlich. Außerdem kann ein Agent für verwaltete Geräte kein Trap senden, wenn das Gerät einen katastrophalen Ausfall aufweist.

SNMPv1-Traps werden in RFC 1157 definiert, mit den folgenden Feldern:

- *Enterprise*: Identifiziert den Typ des verwalteten Objekts, das das Trap generiert.
- *Agent-Adresse* - Stellt die Adresse des verwalteten Objekts bereit, das das Trap generiert.
- *Generischer Trap-Typ*: Gibt einen von mehreren generischen Trap-Typen an.
- *Spezifischer Trap-Code*: Gibt einen von mehreren spezifischen Trap-Codes an.
- *Zeitstempel* - Liefert die Zeitspanne zwischen der letzten Netzwerkneuinitialisierung und der Generierung des Traps.
- *Variable Bindings* - Das Datenfeld des Traps, das PDU enthält. Jede Variablenbindung ordnet eine bestimmte MIB-Objektinstanz ihrem aktuellen Wert zu.

Standardmäßige generische Traps sind: oldStart, warmStart, linkDown, linkUp,

authenticationFailure, egpNeighborLoss. Für generische SNMPv1-Traps enthält das *Enterprise*-Feld den Wert der [sysObjectID](#) des Geräts, das Trap sendet. Für anbieterspezifische Traps ist das *Feld für generische Trap-Typen* auf enterpriseSpecific(6) festgelegt. Cisco implementierte seine eigenen spezifischen Traps auf unkonventionelle Weise. Anstatt das Trap *Enterprise*-Feld weiterhin die [sysObjectID](#) und den *spezifischen Trap-Code* zur Identifizierung aller spezifischen Traps zu haben, die von allen Cisco Geräten unterstützt werden, implementierte Cisco die Trap-Identifikation mithilfe verschiedener Trap Enterprise- und spezifischer Trap-Code-Felder. Die tatsächlichen Werte werden im [SNMP Object Navigator](#) angezeigt. Darüber hinaus hat Cisco einige generische Traps in der [CISCO-GENERAL-TRAPS MIB](#) neu definiert, indem weitere gebundene Variablen hinzugefügt wurden. Für diese Traps wird der *generische Trap-Typ* gleich gehalten und nicht auf enterpriseSpecific(6) festgelegt.

In SNMPv2c wird Trap als NOTIFICATION definiert und anders als SNMPv1 formatiert. Die Parameter sind wie folgt:

- *sysUpTime*: Dies ist der gleiche Zeitstempel in SNMPv1-Trap.
- [snmpTrapOID](#) —Trap identification-Feld. Für generische Traps sind Werte in RFC 1907 definiert. Für anbieterspezifische Traps ist *snmpTrapOID* im Wesentlichen eine Verkettung des SNMPv1 *Enterprise*-Parameters und zwei zusätzliche Subidentifikatoren, '0', sowie des SNMPv1 *Specific Trap Code*-Parameters.
- *VarBindList*: Dies ist eine Liste von Variablenbindungen.

Damit ein Managementsystem ein Trap verstehen kann, das von einem Agenten an ihn gesendet wird, muss das Managementsystem wissen, was der Objekt-Identifikator (OID) definiert. Daher muss die MIB für dieses Trap geladen sein. Dadurch werden die richtigen OID-Informationen bereitgestellt, sodass das Netzwerkmanagementsystem die an das System gesendeten Traps verstehen kann.

Traps, die von Cisco Geräten in bestimmten MIBs unterstützt werden, finden Sie im [Cisco SNMP Object Navigator](#). Hier werden die für eine bestimmte MIB verfügbaren Traps aufgelistet. Um eine dieser Traps zu erhalten, muss Ihre Cisco IOS® Softwareversion die aufgelistete MIB unterstützen. Um herauszufinden, welche MIBs von Ihrem Cisco Gerät unterstützt werden, besuchen Sie www.cisco.com/go/mibs. Die MIB muss in Ihr Netzwerkmanagementsystem geladen werden. Dies wird häufig als Kompilieren bezeichnet. Informationen zur MIB-Kompilierung auf Ihrer NMS-Plattform finden Sie in Ihrem Network Management System (z. B. HP OpenView oder NetView) Benutzerhandbuch. Weitere Informationen finden Sie unter [SNMP: Häufig gestellte Fragen zu MIBs](#) und [MIB-Compilern sowie zum Laden von MIBs](#).

Darüber hinaus sendet ein Gerät kein Trap an ein Netzwerkmanagementsystem, es sei denn, es ist dafür konfiguriert. Ein Gerät muss wissen, dass es eine Falle senden sollte. Das Trap-Ziel wird normalerweise durch eine IP-Adresse definiert, kann aber ein Hostname sein, wenn das Gerät so eingerichtet ist, dass es einen DNS-Server abfragt. In späteren Versionen der Cisco IOS-Software können Geräteadministratoren auswählen, welche Traps sie senden möchten. Weitere Informationen zum Konfigurieren eines Cisco Geräts für SNMP und zum Senden von Traps finden Sie in den entsprechenden Gerätekonfigurationsanleitungen und dem [grundlegenden NMS-Implementierungsleitfaden](#), den [unterstützten Cisco IOS SNMP-Traps](#) und dem [Konfigurieren dieser](#) und [Anleitungen zur Unterstützung und Konfiguration von Cisco CatalystOS-SNMP-Traps](#).

Hinweis: Der Manager empfängt in der Regel SNMP-Benachrichtigungen (TRAPS und INFORMs) an UDP-Portnummer 162.

[Beispiele für Traps, die von Cisco IOS gesendet werden](#)

Dieser Abschnitt enthält einige Beispiele für Traps, die von Cisco IOS gesendet wurden und mit dem **Debug-SNMP-Paket** aufgenommen wurden.

SNMPv1 Generic Trap, neu definiert von Cisco:

```
Nov 21 07:44:17: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
4d23h: SNMP: Queuing packet to 172.17.246.162
4d23h: SNMP: V1 Trap, ent products.45, addr 172.17.246.9, gentrap 3, spectrap 0
  ifEntry.1.23 = 23
  ifEntry.2.23 = Loopback1
  ifEntry.3.23 = 24
  lifEntry.20.23 = up
```

Diese Ausgabe zeigt das neu definierte linkUp-Trap von Cisco aus der [CISCO-GENERAL-TRAPS](#) MIB mit vier gebundenen Variablen. Es hat folgende Felder:

- *Enterprise* = products.45 ([sysObjectID](#) des Geräts, das Trap sendet, in diesem Beispiel ist es c7507-Router)
- *Generischer Trap-Typ* = 3 (linkUp)
- *Spezifischer Trap-Code* = 0

SNMPv1 Cisco spezifisches Trap:

```
4d23h: SNMP: Queuing packet to 172.17.246.162
4d23h: SNMP: V1 Trap, ent ciscoSyslogMIB.2, addr 172.17.246.9, gentrap 6, spectrap 1
  clogHistoryEntry.2.954 = LINK
  clogHistoryEntry.3.954 = 4
  clogHistoryEntry.4.954 = UPDOWN
  clogHistoryEntry.5.954 = Interface Loopback1, changed state to up
  clogHistoryEntry.6.954 = 43021184
```

Diese Ausgabe zeigt das Cisco spezifische clogMessageGenerated-Trap von [CISCO-SYSLOG-MIB](#) mit fünf gebundenen Variablen. Es hat folgende Felder:

- *Enterprise* = Enterprise-Wert von clogMessageGenerated trap
- *Generischer Trap-Typ* = 6 (EnterpriseSpecific)
- *Spezifischer Trap-Code* = 1 (spezifischer Trap-Code von clogMessageGenerated)

SNMPv2c Cisco spezifisches Trap:

```
4d23h: SNMP: Queuing packet to 172.17.246.162
4d23h: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
  sysUpTime.0 = 43053404
  snmpTrapOID.0 =
  clogHistoryEntry.2.958 = SYS
  clogHistoryEntry.3.958 = 6
  clogHistoryEntry.4.958 = CONFIG_I
  clogHistoryEntry.5.958 = Configured from console by vty0 (10.10.10.10)
  clogHistoryEntry.6.958 = 43053403
```

Diese Ausgabe zeigt die SNMPv2c-Benachrichtigung [von](#) Cisco [ConfigManEvent](#) von [CISCO-CONFIG-MAN-MIB](#) mit drei gebundenen Variablen:

- [ccmHistoryEventCommandSource](#)
- [ccmHistoryEventConfigSource](#)
- [ccmHistoryEventConfigDestination](#)

Dieses Trap kann verwendet werden, wenn Änderungen an der Gerätekonfiguration

vorgenommen wurden. Die Werte der letzten beiden Komponenten bestimmen, ob ein Befehl **show** ausgegeben wurde oder ob die Konfiguration berührt wurde.

```
6506E#term mon
6506E#debug snmp packet
SNMP packet debugging is on

6506E#sh run
Building configuration...
...
6506E#
19:24:18: SNMP: Queuing packet to 10.198.28.80
19:24:18: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 6981747
snmpTrapOID.0 = ciscoConfigManMIB.2.0.1
ccmHistoryEventEntry.3.100 = 1
!--- 1 -> commandLine. Executed via CLI. ccmHistoryEventEntry.4.100 = 3 !--- 3 -> running
ccmHistoryEventEntry.5.100 = 2 !--- 2 -> commandSource. Show command was executed.
```

```
6506E#term mon
6506E#debug snmp packet
SNMP packet debugging is on

6506E#conf t
Enter configuration commands, one per line. End with CNTL/Z.
6506E(config)#exit

22:57:37: SNMP: Queuing packet to 10.198.28.80
22:57:37: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 8261709
snmpTrapOID.0 = ciscoConfigManMIB.2.0.1
ccmHistoryEventEntry.3.108 = 1
!--- 1 -> commandLine. Executed via CLI. ccmHistoryEventEntry.4.108 = 2 !--- 2 -> commandSource
ccmHistoryEventEntry.5.108 = 3 !--- 3 -> running. Change was destined to the running
configuration.
```

Zugehörige Informationen

- [Technischer Support und Dokumentation - Cisco Systems](#)