Fehlerbehebung bei langsamem oder zeitweiligem DHCP auf Catalyst 9000 DHCP Relay Agents

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei langsamen DHCP-Adresszuweisungen (Dynamic Host Configuration Protocol) oder zeitweiligen DHCP-Adresszuweisungsfehlern auf Catalyst Switches der Serie 9000 als DHCP-Relay-Agents beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- DHCP- und DHCP-Relay-Agenten
- Internet Control Message Protocol (ICMP)
- Control Plane Policing (CoPP)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst Switches der Serie 9000
- Cisco IOS XE® Versionen 16.x und 17.x

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Verwandte Produkte

Dieses Dokument kann auch mit folgenden Hardware- und Softwareversionen verwendet werden:

- Catalyst Switches der Serien 3650/3850 mit Cisco IOS XE® 16.x

Hintergrundinformationen

Die Control Plane Policing (CoPP)-Funktion erhöht die Sicherheit auf Ihrem Gerät durch Schutz der CPU vor unnötigem Datenverkehr und Denial-of-Service-Angriffen (DoS). Sie kann außerdem Kontrolldatenverkehr und Verwaltungsdatenverkehr vor Datenverlusten schützen, die durch große Mengen an anderem Datenverkehr mit geringerer Priorität verursacht werden.

Ihr Gerät ist in der Regel in drei Betriebsebenen unterteilt, die jeweils eigene Ziele haben:

- Die Datenebene, auf der die Datenpakete weitergeleitet werden.
- Kontrollebene, um Daten korrekt weiterzuleiten
- die Verwaltungsebene, auf der die Netzwerkelemente verwaltet werden.

Sie können CoPP verwenden, um den Großteil des CPU-gebundenen Datenverkehrs zu schützen und die Routing-Stabilität, Erreichbarkeit und Paketübermittlung sicherzustellen. Am wichtigsten ist, dass Sie CoPP verwenden können, um die CPU vor einem DoS-Angriff zu schützen.

CoPP verwendet die modulare QoS-Kommandozeilenschnittstelle (MQC) und die CPU-Warteschlangen, um diese Ziele zu erreichen. Unterschiedliche Typen von Steuerungsebenen-Datenverkehr werden anhand bestimmter Kriterien zusammengefasst und einer CPU-Warteschlange zugewiesen. Sie können diese CPU-Warteschlangen durch die Konfiguration dedizierter Richtlinien in der Hardware verwalten. Sie können beispielsweise die Policer-Rate für bestimmte CPU-Warteschlangen (Datenverkehrstyp) ändern oder die Policer für einen bestimmten Datenverkehrstyp deaktivieren.

Obwohl die Richtlinien in der Hardware konfiguriert sind, hat CoPP keine Auswirkungen auf die CPU-Leistung oder die Leistung der Datenebene. Da dies jedoch die Anzahl der Pakete begrenzt, die zur CPU geleitet werden, wird die CPU-Last gesteuert. Das bedeutet, dass für Services, die auf Pakete von der Hardware warten, eine kontrollierte Rate der eingehenden Pakete angezeigt wird (diese Rate kann vom Benutzer konfiguriert werden).

Problem

Ein Catalyst 9000-Switch wird als DHCP-Relay-Agent konfiguriert, wenn der Befehl **ip helper-address** auf einer gerouteten Schnittstelle oder SVI konfiguriert wird. Die Schnittstelle, auf der die Hilfsadresse konfiguriert wird, ist in der Regel das Standard-Gateway für Downstream-Clients. Damit der Switch seinen Clients erfolgreiche DHCP-Relay-Dienste bereitstellen kann, muss er in der Lage sein, eingehende DHCP Discover-Nachrichten zu verarbeiten. Dazu muss der Switch die DHCP-Erkennung empfangen und das Paket bis zur CPU durchsuchen, um verarbeitet zu werden. Sobald die DHCP Discover-Nachricht empfangen und verarbeitet wurde, erstellt der

Relay-Agent ein neues Unicast-Paket, das von der Schnittstelle stammt, an der die DHCP Discover-Nachricht empfangen wurde, und an die IP-Adresse gerichtet ist, wie in der Konfiguration **ip helper-address** definiert. Nachdem das Paket erstellt wurde, wird es von der Hardware weitergeleitet und an den DHCP-Server gesendet, wo es verarbeitet und schließlich an den Relay-Agent zurückgesendet werden kann, sodass der DHCP-Prozess für den Client fortgesetzt werden kann.

Ein häufiges Problem tritt auf, wenn DHCP-Transaktionspakete am Relay-Agent versehentlich durch Datenverkehr beeinträchtigt werden, der an die CPU gesendet wird, da er einem bestimmten ICMP-Szenario unterliegt, z. B. einer ICMP-Umleitung oder einer ICMP-Meldung "Destination Unreachable" (Ziel nicht erreichbar). Dieses Verhalten kann sich dadurch manifestieren, dass Clients nicht in der Lage sind, eine IP-Adresse von DHCP rechtzeitig oder sogar einen vollständigen DHCP-Zuweisungsfehler zu erhalten. In einigen Szenarien kann das Verhalten nur zu bestimmten Tageszeiten beobachtet werden, z. B. zu Spitzenzeiten, wenn die Netzwerkauslastung vollständig maximiert ist.

Wie im Abschnitt "Hintergrund" erwähnt, ist für Catalyst Switches der Serie 9000 eine CoPP-Standardrichtlinie konfiguriert und aktiviert. Diese CoPP-Richtlinie fungiert als Quality of Service (QoS)-Richtlinie, die sich im Pfad des Datenverkehrs befindet, der an den Ports an der Vorderseite empfangen wird und für die Geräte-CPU bestimmt ist. Die Übertragungsrate begrenzt den Datenverkehr auf Basis des Datenverkehrstyps und der vordefinierten Grenzwerte, die in der Richtlinie konfiguriert werden. Einige Beispiele für standardmäßig klassifizierten und eingeschränkten Datenverkehr sind Routing-Control-Pakete (in der Regel mit DSCP CS6 markiert), Topology Control Packets (STP BPDUs) und Low Latency Packets (BFD). Diese Pakete sollten priorisiert werden, da ihre Verarbeitung zu einer stabilen Netzwerkumgebung führt.

Zeigen Sie die CoPP-Richtlinienstatistiken mit dem Befehl **show platform hardware fed switch active qos queue stats internal cpu policer** an.

Die ICMP-Umleitungswarteschlange (Warteschlange 6) und die BROADCAST-Warteschlange (Warteschlange 12) verwenden beide denselben PlcIdx von 0 (Policer-Index). Das bedeutet, dass der Broadcast-Datenverkehr, der von der Geräte-CPU verarbeitet werden muss, z. B. eine DHCP-Erkennung, für den Datenverkehr freigegeben wird, der auch an die Geräte-CPU in der ICMP-Umleitungswarteschlange gerichtet ist. Dies kann zu dem bereits erwähnten Problem führen, bei dem DHCP-Transaktionen fehlschlagen, da der Datenverkehr der ICMP-Umleitungswarteschlange den Datenverkehr verliert, der von der BROADCAST-Warteschlange verarbeitet werden muss, was dazu führt, dass legitime Broadcast-Pakete verworfen werden.

```
9300-Switch#show platform hardware fed switch active qos queue stats internal cpu policer

CPU Queue Statistics
============================================================================================
(default) (set) Queue Queue
QId PlcIdx Queue Name Enabled Rate Rate Drop(Bytes) Drop(Frames)
--------------------------------------------------------------------------------------------
0 11 DOT1X Auth Yes 1000 1000 0 0
1 1 L2 Control Yes 2000 2000 0 0
2 14 Forus traffic Yes 4000 4000 0 0
3 0 ICMP GEN Yes 600 600 0 0
4 2 Routing Control Yes 5400 5400 0 0
5 14 Forus Address resolution Yes 4000 4000 0 0
6    0      ICMP Redirect               Yes     600       600      0            0  <-- Policer
Index 0
7 16 Inter FED Traffic Yes 2000 2000 0 0
8 4 L2 LVX Cont Pack Yes 1000 1000 0 0
```

```
9 19 EWLC Control Yes 13000 13000 0 0
10 16 EWLC Data Yes 2000 2000 0 0
11 13 L2 LVX Data Pack Yes 1000 1000 0 0
12   0      BROADCAST                   Yes     600       600      0            0  <-- Policer
Index 0
13 10 Openflow Yes 200 200 0 0
14 13 Sw forwarding Yes 1000 1000 0 0
15 8 Topology Control Yes 13000 16000 0 0
16 12 Proto Snooping Yes 2000 2000 0 0
17 6 DHCP Snooping Yes 500 500 0 0
18 13 Transit Traffic Yes 1000 1000 0 0
19 10 RPF Failed Yes 250 250 0 0
20 15 MCAST END STATION Yes 2000 2000 0 0
<snip>
```

Datenverkehr, der die standardmäßige Paketrate von 600 pro Sekunde in der CoPP-Richtlinie überschreitet, wird verworfen, bevor er die CPU erreicht.

```
9300-Switch#show platform hardware fed switch active qos queue stats internal cpu policer

CPU Queue Statistics
============================================================================================
(default) (set) Queue Queue
QId PlcIdx Queue Name Enabled Rate Rate Drop(Bytes) Drop(Frames)
--------------------------------------------------------------------------------------------
0 11 DOT1X Auth Yes 1000 1000 0 0
1 1 L2 Control Yes 2000 2000 0 0
2 14 Forus traffic Yes 4000 4000 0 0
3 0 ICMP GEN Yes 600 600 0 0
4 2 Routing Control Yes 5400 5400 0 0
5 14 Forus Address resolution Yes 4000 4000 0 0
6    0      ICMP Redirect               Yes     600       600      3063106173577 3925209161
<-- Dropped packets in queue
7 16 Inter FED Traffic Yes 2000 2000 0 0
8 4 L2 LVX Cont Pack Yes 1000 1000 0 0
9 19 EWLC Control Yes 13000 13000 0 0
10 16 EWLC Data Yes 2000 2000 0 0
11 13 L2 LVX Data Pack Yes 1000 1000 0 0
12   0      BROADCAST                   Yes     600       600      1082560387 3133323
<-- Dropped packets in queue
13 10 Openflow Yes 200 200 0 0
14 13 Sw forwarding Yes 1000 1000 0 0
15 8 Topology Control Yes 13000 16000 0 0
16 12 Proto Snooping Yes 2000 2000 0 0
17 6 DHCP Snooping Yes 500 500 0 0
18 13 Transit Traffic Yes 1000 1000 0 0
19 10 RPF Failed Yes 250 250 0 0
20 15 MCAST END STATION Yes 2000 2000 0 0
<snip>
```

Szenario 1: ICMP-Umleitungen

Betrachten Sie diese Topologie für das erste Szenario:

Die Abfolge der Ereignisse ist wie folgt:

1. Ein Benutzer unter 10.10.10.100 initiiert eine Telnet-Verbindung mit Gerät 10.100.100.100, einem Remote-Netzwerk.

2. Die Ziel-IP-Adresse befindet sich in einem anderen Subnetz, sodass das Paket an das Standardgateway 10.10.10.15 des Benutzers gesendet wird.

3. Wenn der Catalyst 9300 dieses Paket zum Weiterleiten empfängt, sendet er es an seine CPU, um eine ICMP-Umleitung zu generieren.

Die ICMP-Umleitung wird generiert, da es aus Sicht des 9300-Switches für den Laptop effizienter wäre, dieses Paket einfach unter der Adresse 10.10.10.1 direkt an den Router zu senden, da dies sowieso der nächste Hop von Catalyst 9300 ist und sich in demselben VLAN befindet, in dem sich der Benutzer befindet.

Das Problem besteht darin, dass der gesamte Fluss an der CPU verarbeitet wird, da er die ICMP-Weiterleitungskriterien erfüllt. Wenn andere Geräte Datenverkehr senden, der das ICMP-Umleitungsszenario erfüllt, wird in dieser Warteschlange noch mehr Datenverkehr an die CPU gesendet, was sich auf die BROADCAST-Warteschlange auswirken kann, da sie die gleiche CoPP-Richtlinie verwenden.

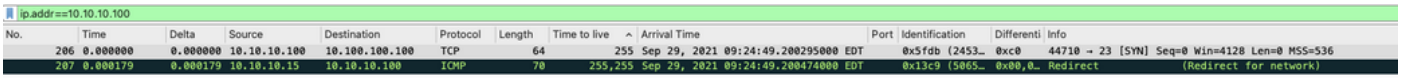
Debuggen Sie ICMP, um das Syslog für die ICMP-Umleitung anzuzeigen.

```
9300-Switch#debug ip icmp       <-- enables ICMP debugs
ICMP packet debugging is on
9300-Switch#show logging | inc ICMP
*Sep 29 12:41:33.217: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE,
dscp 0 topoid 0
*Sep 29 12:41:33.218: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE,
dscp 0 topoid 0
*Sep 29 12:41:33.219: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE,
dscp 0 topoid 0
*Sep 29 12:41:33.219: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE,
dscp 0 topoid 0
*Sep 29 12:43:08.127: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:09.517: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:10.017: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1     <-- ICMP Redirect to use 10.10.10.1 as Gateway
*Sep 29 12:50:14.293: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:19.053: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:23.797: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:28.537: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
```

```
10.10.10.1
*Sep 29 12:50:33.284: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
```

> **Vorsicht**: Aufgrund der Skalierbarkeit wird empfohlen, die Konsolenprotokollierung und die Terminalüberwachung zu deaktivieren, bevor Sie ICMP-Debugging aktivieren.

Eine Embedded Packet Capture auf der CPU der Catalyst Serie 9300 zeigt das anfängliche TCP SYN für die Telnet-Verbindung auf der CPU sowie die generierte ICMP-Umleitung.



Das ICMP-Umleitungspaket stammt von der für den Client bestimmten Catalyst 9300 VLAN 10-Schnittstelle und enthält die ursprünglichen Paket-Header, für die das ICMP-Umleitungspaket gesendet wird.

```
▼ Internet Protocol Version 4, Src: 10.10.10.15, Dst: 10.10.10.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x13c9 (5065)
  ▶ Flags: 0x0000
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x7f75 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.10.15
    Destination: 10.10.10.100
▼ Internet Control Message Protocol
    Type: 5 (Redirect)
    Code: 0 (Redirect for network)
    Checksum: 0x2bec [correct]
    [Checksum Status: Good]
    Gateway address: 10.10.10.1
  ▼ Internet Protocol Version 4, Src: 10.10.10.100, Dst: 10.100.100.100
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
      Total Length: 44
      Identification: 0x5fdb (24539)
    ▶ Flags: 0x0000
      Time to live: 255
      Protocol: TCP (6)
      Header checksum: 0xd7fa [validation disabled]
      [Header checksum status: Unverified]
      Source: 10.10.10.100
      Destination: 10.100.100.100
  ▶ Transmission Control Protocol, Src Port: 44710, Dst Port: 23
```

Lösung

In diesem Szenario können die Pakete, die bis zur CPU durchgelockt werden, verhindert werden, wodurch auch die Generierung des ICMP-Umleitungspakets gestoppt wird.

Moderne Betriebssysteme verwenden keine ICMP-Umleitungsnachrichten, sodass die Ressourcen, die zum Generieren und Senden und Verarbeiten dieser Pakete erforderlich sind, keine effiziente Nutzung von CPU-Ressourcen auf Netzwerkgeräten darstellen.

Sie können auch den Benutzer auffordern, das Standard-Gateway 10.10.10.1 zu verwenden. Eine solche Konfiguration kann jedoch aus einem bestimmten Grund erfolgen und ist nicht Bestandteil des vorliegenden Dokuments.

Deaktivieren Sie ICMP-Umleitungen einfach über die CLI **no ip redirects**.

```
9300-Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
9300-Switch(config)#interface vlan 10
9300-Switch(config-if)#no ip redirects       <-- disable IP redirects
9300-Switch(config-if)#end
```

Stellen Sie sicher, dass die ICMP-Umleitungen auf einer Schnittstelle deaktiviert sind.

```
9300-Switch#show ip interface vlan 10
Vlan10 is up, line protocol is up
Internet address is 10.10.10.15/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.102
Outgoing Common access list is not set
Outgoing access list is not set
Inbound Common access list is not set
Inbound access list is BLOCK-TELNET
Proxy ARP is disabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are never sent       <-- redirects disabled
ICMP unreachables are never sent
ICMP mask replies are never sent
IP fast switching is enabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF switching turbo vector
<snip>
```

Weitere Informationen zu ICMP-Umleitungen und dem Zeitpunkt ihrer Versendung finden Sie unter folgendem Link: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13714-43.html

Szenario 2: ICMP nicht erreichbar

Stellen Sie sich dieselbe Topologie vor, in der der Benutzer unter 10.10.10.100 eine Telnet-Verbindung mit 10.100.100.100 initiiert. Diesmal wurde eine eingehende Zugriffsliste für die VLAN 10-SVI konfiguriert, die Telnet-Verbindungen blockiert.


```
9300-Switch#show running-config interface vlan 10
Building Configuration..

Current Configuration : 491 bytes
!
interface Vlan10
ip address 10.10.10.15 255.255.255.0
no ip proxy-arp
ip access-group BLOCK-TELNET in              <-- inbound ACL
end
9300-Switch#
9300-Switch#show ip access-list BLOCK-TELNET
Extended IP access list BLOCK-TELNET
10 deny tcp any any eq telnet            <-- block telnet
20 permit ip any any
9300-Switch#
```

Die Abfolge der Ereignisse ist wie folgt:

1. Der Benutzer unter 10.10.10.100 initiiert eine Telnet-Verbindung mit Gerät 10.100.100.100.

2. Die Ziel-IP-Adresse befindet sich in einem anderen Subnetz, sodass das Paket an das Standard-Gateway des Benutzers gesendet wird.

3. Wenn der Catalyst 9300 dieses Paket empfängt, wird es anhand der eingehenden ACL ausgewertet und blockiert.

4. Da das Paket blockiert ist und IP Unreachables auf der Schnittstelle aktiviert sind, wird das Paket an die CPU gesendet, sodass das Gerät ein nicht erreichbares ICMP-Zielpaket generieren kann.

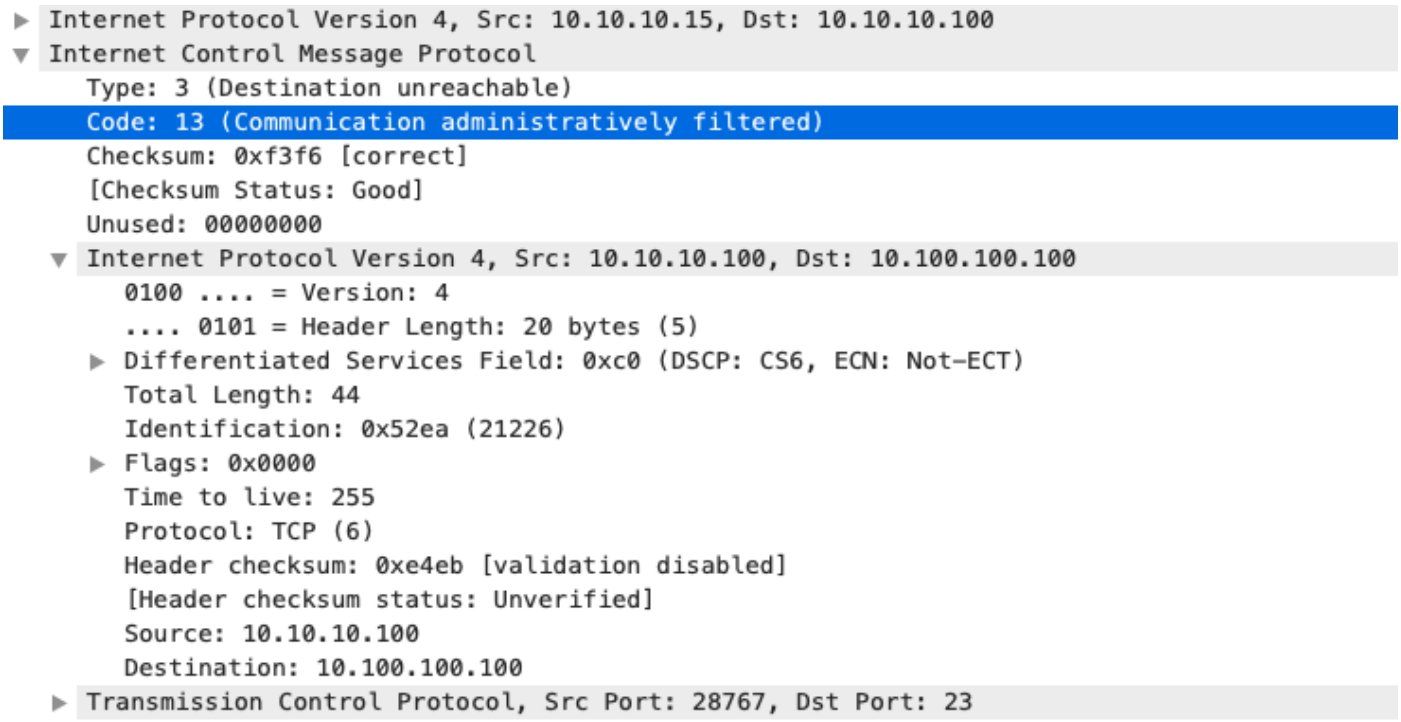
Debuggen Sie ICMP, um das nicht erreichbare ICMP-Ziel-Syslog anzuzeigen.

```
9300-Switch#debug ip icmp              <-- enables ICMP debugs
ICMP packet debugging is on
9300-Switch#show logging | include ICMP
<snip>
*Sep 29 14:01:29.041: ICMP: dst (10.100.100.100) administratively prohibited unreachable sent to
10.10.10.100    <-- packet blocked and ICMP message sent to client
```

> **Vorsicht**: Aufgrund der Skalierbarkeit wird empfohlen, die Konsolenprotokollierung und die Terminalüberwachung zu deaktivieren, bevor Sie ICMP-Debugging aktivieren.

Eine Embedded Packet Capture auf der CPU der Catalyst Serie 9300 zeigt das anfängliche TCP SYN für die Telnet-Verbindung auf der CPU sowie das gesendete ICMP Destination Unreachable.

Das Paket "ICMP Destination Unreachable" stammt von der für den Client bestimmten Catalyst 9300 VLAN 10-Schnittstelle und enthält die ursprünglichen Paket-Header, für die das ICMP-Paket gesendet wird.



Lösung

Deaktivieren Sie in diesem Szenario das Verhalten, bei dem blockierte Pakete durch eine ACL blockiert werden, um die Meldung "ICMP Destination Unreachable" (ICMP-Ziel nicht erreichbar) zu generieren.

Die Funktion "IP Unreachable" ist auf gerouteten Schnittstellen der Catalyst Switches der Serie 9000 standardmäßig aktiviert.

```
9300-Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
9300-Switch(config)#interface vlan 10
9300-Switch(config-if)#no ip unreachables      <-- disable IP unreachables
```

Stellen Sie sicher, dass sie für die Schnittstelle deaktiviert sind.

```
9300-Switch#show ip interface vlan 10
Vlan10 is up, line protocol is up
Internet address is 10.10.10.15/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.102
Outgoing Common access list is not set
Outgoing access list is not set
Inbound Common access list is not set
```

```
Inbound access list is BLOCK-TELNET
Proxy ARP is disabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are never sent
ICMP unreachables are never sent     <-- IP unreachables disabled
ICMP mask replies are never sent
IP fast switching is enabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF switching turbo vector
<snip>
```

Szenario 3: ICMP-TTL überschritten

Berücksichtigen Sie die Topologie, die zuvor für die beiden vorherigen Szenarien verwendet wurde. Diesmal versucht der Benutzer unter 10.10.10.100, eine Ressource in einem Netzwerk zu erreichen, das seit der Außerbetriebnahme beendet wurde. Aus diesem Grund sind die SVI und das VLAN, die zum Hosten dieses Netzwerks verwendet wurden, auf dem Catalyst 9300 nicht mehr vorhanden. Der Router verfügt jedoch weiterhin über eine statische Route, die als nächster Hop für dieses Netzwerk auf die Catalyst 9300 VLAN 10-Schnittstelle verweist.

Da dieses Netzwerk für den Catalyst 9300 nicht mehr konfiguriert ist, wird es nicht als direkt verbunden angezeigt, und der Catalyst 9300 leitet Pakete, für die er keine spezifische Route für besitzt, an seine statische Standardroute weiter, die unter 10.10.10.1 auf den Router verweist.

Dieses Verhalten führt zu einer Routing-Schleife im Netzwerk, wenn der Benutzer versucht, eine Verbindung zu einer Ressource im Adressbereich 192.168.10.0/24 herzustellen. Das Paket wird zwischen dem Router der Serie 9300 und dem Router in Schleifen übertragen, bis die TTL abläuft.

1. Benutzer versucht, eine Verbindung zu einer Ressource im Netzwerk 192.168.10/24 herzustellen.

2. Das Paket wird von Catalyst 9300 empfangen und mit dem nächsten Hop 10.10.10.1 auf die Standardroute geroutet, und der TTL wird um 1 herabgesetzt.

3. Der Router empfängt dieses Paket und überprüft die Routing-Tabelle, um eine Route für dieses Netzwerk mit dem nächsten Hop 10.10.10.15 zu finden. Er setzt den TTL um 1 herab und leitet das Paket zurück an den 9300.

4. Catalyst 9300 empfängt das Paket und leitet es erneut an 10.10.10.1 zurück. Die TTL wird um 1 herabgesetzt.

Dieser Prozess wird wiederholt, bis die IP-TTL den Wert 0 erreicht.

Wenn der Catalyst das Paket mit der IP TTL = 1 empfängt, sendet er das Paket an die CPU und

generiert eine ICMP-Meldung über eine Überschreitung der TTL.

Der ICMP-Pakettyp ist 11 mit Code 0 (bei der Übertragung ist die TTL abgelaufen). Dieser Pakettyp kann nicht über CLI-Befehle deaktiviert werden.

Das Problem mit dem DHCP-Datenverkehr kommt in diesem Szenario ins Spiel, da die Pakete, die in Loops zusammengefasst werden, der ICMP-Umleitung unterliegen, da sie dieselbe Schnittstelle auslassen, auf der sie empfangen wurden.

Die vom Benutzer gesendeten Pakete unterliegen ebenfalls der ICMP-Umleitung. In diesem Szenario kann der DHCP-Datenverkehr aus der BROADCAST-Warteschlange entfernt werden. Bei einer Skalierung wäre dieses Szenario aufgrund der Anzahl der Pakete, die in die Umleitungswarteschlange gestellt werden, noch schlimmer.

Hier werden CoPP-Drops durch 1000 Pings zum Netzwerk 192.168.10.0/24 mit einer Zeitüberschreitung von 0 Sekunden zwischen jedem Ping demonstriert. Die CoPP-Statistiken auf dem 9300 werden gelöscht und bei null Byte verworfen, bevor die Pings gesendet werden.

```
9300-Switch#clear platform hardware fed switch active qos statistics internal cpu policer
<-- clear CoPP stats

9300-Switch#show platform hardware fed switch active qos queue stats internal cpu policer | i
Redirect|Drop   <-- verify 0 drops
QId PlcIdx Queue Name Enabled Rate Rate Drop(Bytes) Drop(Frames)
6 0 ICMP Redirect Yes 600 600 0               0                        <-- bytes dropped 0
<snip>
```

Benutzer sendet Datenverkehr an entferntes Netzwerk.

```
User#ping 192.168.10.10 timeout 0 rep 1000   <-- User sends 1000 pings
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 192.168.10.10, timeout is 0 seconds:
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................
Success rate is 0 percent (0/1000)
```

Die ICMP-Debugs zeigen die durch die Routing-Schleife bedingten Redirect-Syslogs und TTL-Exceeded-Syslogs.

```
9300-Switch#debug ip icmp
ICMP packet deubgging is on
*Sep 29 16:33:22.676: ICMP: redirect sent to 10.10.10.100 for dest 192.168.10.10, use gw
10.10.10.1    <-- redirect sent
*Sep 29 16:33:22.678: ICMP: time exceeded (time to live) sent to 10.10.10.100 (dest was
```

```
192.168.10.10), topology BASE, dscp 0 topoid 0    <-- TTL exceeded observed
*Sep 29 16:33:22.678: ICMP: time exceeded (time to live) sent to 10.10.10.100 (dest was
192.168.10.10), topology BASE, dscp 0 topoid 0
*Sep 29 16:33:22.678: ICMP: time exceeded (time to live) sent to 10.10.10.100 (dest was
192.168.10.10), topology BASE, dscp 0 topoid 0
<snip>
```

> **Vorsicht**: Aufgrund der Skalierbarkeit wird empfohlen, die Konsolenprotokollierung und die Terminalüberwachung zu deaktivieren, bevor Sie ICMP-Debugging aktivieren.

CoPP-Drops werden aufgrund des Datenverkehrs erkannt, der zur Umleitung an die CPU geleitet wird. Beachten Sie, dass dies nur für einen einzelnen Client gilt.

```
9300-Switch#show platform hardware fed switch active qos queue stats internal cpu policer

CPU Queue Statistics
============================================================================================
(default) (set) Queue Queue
QId PlcIdx Queue Name Enabled Rate Rate Drop(Bytes) Drop(Frames)
--------------------------------------------------------------------------------------------
0 11 DOT1X Auth Yes 1000 1000 0 0
1 1 L2 Control Yes 2000 2000 0 0
2 14 Forus traffic Yes 4000 4000 0 0
3 0 ICMP GEN Yes 600 600 0 0
4 2 Routing Control Yes 5400 5400 0 0
5 14 Forus Address resolution Yes 4000 4000 0 0
6    0      ICMP Redirect               Yes     600       600      15407990     126295    <--
drops in redirect queue
7 16 Inter FED Traffic Yes 2000 2000 0 0
8 4 L2 LVX Cont Pack Yes 1000 1000 0 0
<snip>
```

Lösung

Die Lösung in diesem Szenario ist die Deaktivierung von ICMP-Umleitungen, wie in Szenario 1. Die Routing-Schleife ist ebenfalls ein Problem, die Intensität wird jedoch noch erhöht, da die Pakete auch für die Umleitung analysiert werden.

ICMP-Pakete mit TTL-Überschreitung werden auch bei einem TTL-Wert von 1 gesendet. Diese Pakete verwenden jedoch einen anderen CoPP Policer-Index und verwenden keine Warteschlange für BROADCAST, sodass der DHCP-Datenverkehr nicht beeinträchtigt wird.

Deaktivieren Sie die ICMP-Umleitungen über die CLI no ip redirects.

```
9300-Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
9300-Switch(config)#interface vlan 10
9300-Switch(config-if)#no ip redirects        <-- disable IP redirects
9300-Switch(config-if)#end
```

Zugehörige Informationen

- Konfigurieren der eingebetteten Paketerfassung
- Verständnis von ICMP-Umleitungen
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.