ICMP-Umleitungsnachrichten verstehen

Inhalt

Einleitung

Dieses Dokument beschreibt die ICMP-Funktion (Internet Control Message Protocol) zur Paketumleitung.

Voraussetzungen

Anforderungen

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

- Architektur der Nexus 7000-Plattform
- Cisco NX-OS Softwarekonfiguration
- Internet Control Message Protocol, dokumentiert in Request for Comments (RFC) 792

Verwendete Komponenten

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

- Nexus 7000
- Cisco NX-OS-Software

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.

Hintergrundinformationen

In diesem Dokument werden die Paketumleitungsfunktionen des Internet Control Message Protocol (ICMP) behandelt. In diesem Dokument wird erläutert, was das Vorhandensein von ICMP-Umleitungsnachrichten im Netzwerk normalerweise bedeutet und was getan werden kann, um die negativen Nebenwirkungen zu minimieren, die mit Netzwerkbedingungen verbunden sind und die Erzeugung von ICMP-Umleitungsnachrichten verursachen.

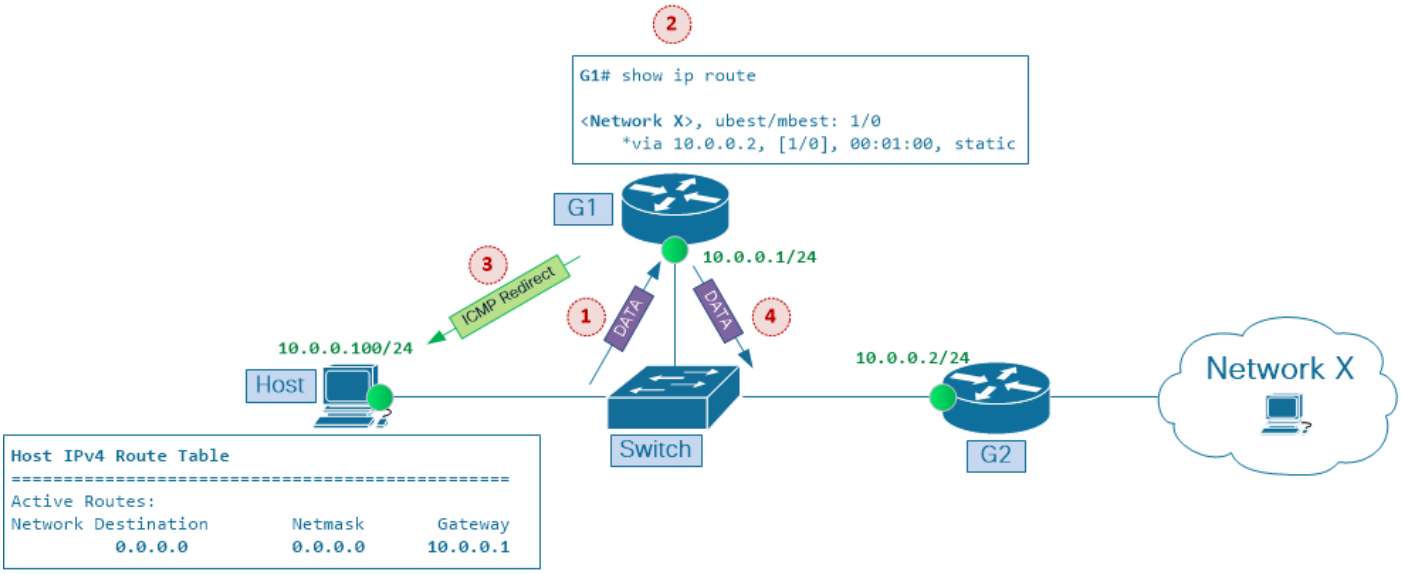
ICMP-Umleitungsnachrichten

Die ICMP-Umleitungsfunktion wird in RFC 792 Internet Control Message Protocol anhand des folgenden Beispiels erläutert:

> Das Gateway sendet in dieser Situation eine Umleitungsnachricht an einen Host.
>
> Ein Gateway G1 empfängt ein Internetdatagramm von einem Host in einem Netzwerk, an das das Gateway angeschlossen ist. Das Gateway G1 überprüft seine Routing-Tabelle und erhält die Adresse des nächsten Gateways G2 auf der Route zum Datagramm-Internet-Zielnetzwerk X
>
> Befinden sich G2 und der durch die Internet-Quelladresse des Datagramms identifizierte Host im gleichen Netzwerk, wird eine Umleitungsnachricht an den Host gesendet. Die Umleitungsnachricht rät dem Host, seinen Datenverkehr für das Netzwerk X direkt an das Gateway G2 zu senden, da dies ein kürzerer Pfad zum Ziel ist.
>
> Das Gateway leitet die ursprünglichen Datagrammdaten an sein Internetziel weiter.

Dieses Szenario ist in Abbildung 1 dargestellt. Host und zwei Router, G1 und G2, sind mit einem gemeinsam genutzten Ethernet-Segment verbunden und haben IP-Adressen im gleichen Netzwerk 10.0.0.0/24

Abbildung 1: ICMP-Umleitungen in Mehrpunkt-Ethernet-Netzwerken



ICMP-Umleitungen in Mehrpunkt-Ethernet-Netzwerken

Der Host hat die IP-Adresse 10.0.0.100. Die Host-Routing-Tabelle enthält einen Standard-Routing-Eintrag, der auf die IP-Adresse 10.0.0.1 des Routers G1 als Standard-Gateway verweist. Router G1 verwendet die IP-Adresse 10.0.0.2 des Routers G2 als nächsten Hop, wenn Datenverkehr an das Zielnetzwerk X weitergeleitet wird.

Dies geschieht, wenn der Host ein Paket an das Zielnetzwerk X sendet:

1. Gateway G1 mit der IP-Adresse 10.0.0.1 empfängt ein Datenpaket vom Host 10.0.0.100 in einem Netzwerk, mit dem es verbunden ist.

2. Das Gateway G1 überprüft seine Routing-Tabelle und erhält die IP-Adresse 10.0.0.2 des nächsten Gateways G2 auf der Route zum Datenpaket-Zielnetzwerk X.

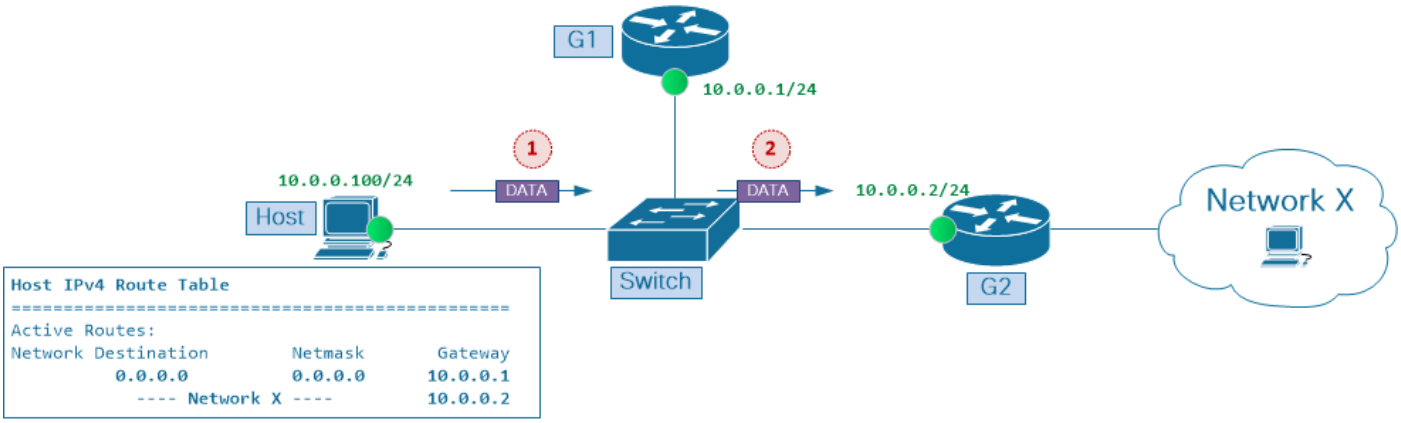
3. Wenn sich G2 und der durch die Quelladresse des IP-Pakets identifizierte Host im gleichen Netzwerk befinden, wird eine ICMP-Umleitungsnachricht an den Host gesendet. Die ICMP-Umleitungsnachricht empfiehlt dem Host, seinen Datenverkehr für das Netzwerk X direkt an das Gateway G2 zu senden, da es sich um einen kürzeren Pfad zum Ziel handelt.

4. Das Gateway G1 leitet das ursprüngliche Datenpaket an sein Ziel weiter.

Abhängig von der Host-Konfiguration kann er festlegen, ob ICMP-Umleitungsnachrichten ignoriert werden sollen, die von G1 an ihn gesendet werden. Wenn der Host jedoch ICMP-Umleitungsnachrichten verwendet, um seinen Routing-Cache anzupassen, und anfängt, nachfolgende Datenpakete direkt an G2 zu senden, werden diese Vorteile in diesem Szenario erreicht

- Optimierung des Datenweiterleitungspfads im Netzwerk Datenverkehr erreicht sein Ziel schneller
- Reduzierung der Auslastung von Netzwerkressourcen wie Bandbreite und Router-CPU-Auslastung

Abbildung 2: Next-Hop G2 im Host-Routing-Cache installiert



Next-Hop G2 im Host-Routing-Cache installiert

Wie in Abbildung 2 gezeigt, werden die folgenden Vorteile im Netzwerk sichtbar, nachdem der Host einen Routen-Cache-Eintrag für Netzwerk X mit G2 als nächstem Hop erstellt hat:

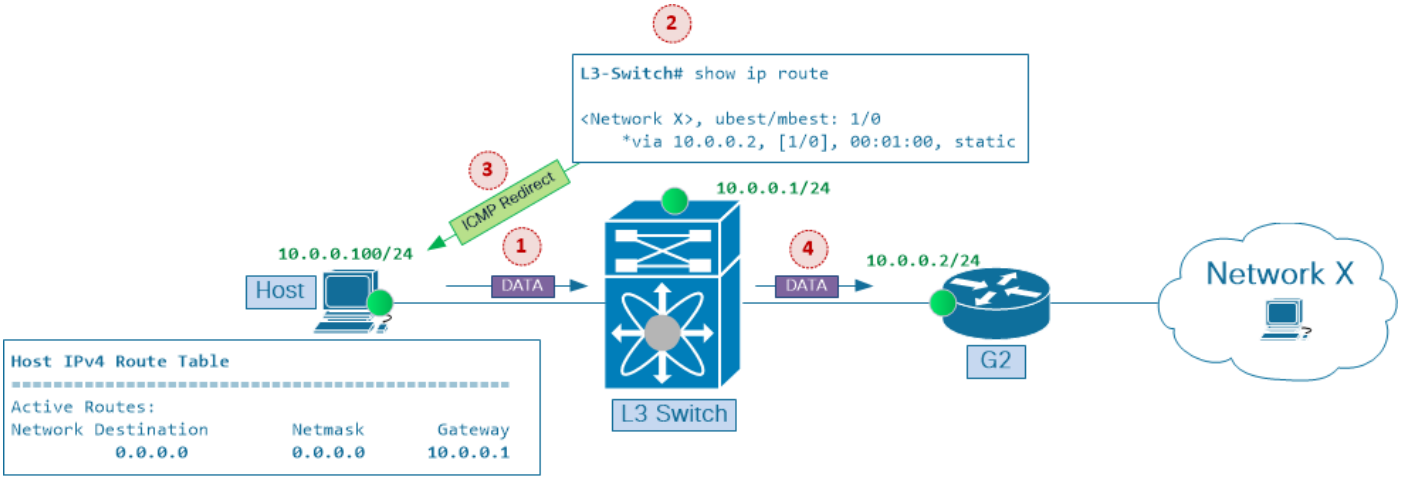
- Die Bandbreitennutzung an der Verbindung zwischen Switch und Router G1 nimmt in beide Richtungen ab.
- Die CPU-Auslastung auf Router G1 nimmt ab, da der Datenfluss von Host zu Netzwerk X diesen Knoten nicht mehr durchläuft.
- End-to-End-Netzwerkverzögerung zwischen Host und Netzwerk X verbessert sich.

Um die Bedeutung des ICMP-Umleitungsmechanismus zu verstehen, sollten Sie bedenken, dass bei den ersten Internet-Router-Implementierungen für die Verarbeitung des Datenverkehrs in erster Linie CPU-Ressourcen erforderlich waren. Daher war es wünschenswert, das Datenverkehrsvolumen, das von einem einzelnen Router verarbeitet werden musste, zu reduzieren und auch die Anzahl der Router-Hops, die ein bestimmter Datenverkehrsfluss auf dem Weg zum Ziel durchlaufen musste, zu minimieren. Gleichzeitig wurde die Layer-2-Weiterleitung (auch als Switching bezeichnet) hauptsächlich in angepassten ASICs (Application-Specific Integrated Circuits) implementiert und war in Bezug auf die Weiterleitungsleistung im Vergleich zur Layer-3-Weiterleitung (auch Routing genannt) relativ "günstig", was wiederum in Prozessoren für allgemeine Zwecke erfolgte.

Neuere ASIC-Generationen können Pakete auf Layer 2 und Layer 3 weiterleiten. Die hardwarebasierte Layer-3-Tabellensuche trägt dazu bei, die mit der Paketverarbeitung durch die Router verbundenen Leistungskosten zu senken. Durch die Integration der Layer-3-Weiterleitungsfunktionen in Layer-2-Switches (die jetzt als Layer-3-Switches bezeichnet werden) wurde die Paketweiterleitung effizienter, sodass keine **einarmigen Router-**Designoptionen (auch **Router on a Stick** genannt) mehr erforderlich waren und die mit solchen Netzwerkkonfigurationen verbundenen Einschränkungen vermieden wurden.

Abbildung 3 baut auf dem Szenario in Abbildung 1 auf. Die Layer-2- und Layer-3-Funktionen, die ursprünglich von zwei separaten Knoten, Switch und Router G1, bereitgestellt wurden, werden in einem einzigen Layer-3-Switch konsolidiert, z. B. einer Plattform der Serie Nexus 7000.

Abbildung 3: Layer-3-Switch ersetzt Konfiguration mit einem Router



Layer-3-Switch ersetzt "One-Arm-Router"-Konfiguration

Dies geschieht, wenn der Host ein Paket an das Ziel Netzwerk X sendet:

1. Gateway-L3-Switch mit IP-Adresse 10.0.0.1 empfängt Datenpaket von einem Host 10.0.0.100 in einem Netzwerk, mit dem er verbunden ist.

2. Das Gateway, L3 Switch, überprüft seine Routing-Tabelle und erhält die Adresse 10.0.0.2 des nächsten Gateways G2 auf der Route zum Datenpaket-Zielnetzwerk X.

3. Wenn sich G2 und der durch die Quelladresse des IP-Pakets identifizierte Host im gleichen Netzwerk befinden, wird eine ICMP-Umleitungsnachricht an den Host gesendet. Die ICMP-Umleitungsnachricht empfiehlt dem Host, seinen Datenverkehr für Netzwerk X direkt an Gateway G2 zu senden, da es sich um einen kürzeren Pfad zum Ziel handelt.

4. Das Gateway leitet das ursprüngliche Datenpaket an sein Ziel weiter.

Da Layer-3-Switches nun sowohl die Layer-2- als auch die Layer-3-Paketweiterleitung auf ASIC-Ebene durchführen können, kann geschlossen werden, dass beide Vorteile der ICMP-Weiterleitungsfunktion, (a) die Verbesserung der Verzögerung durch das Netzwerk und (b) die Verringerung der Netzwerkressourcennutzung, erreicht werden und dass den Pfadoptimierungstechniken in Mehrpunkt-Ethernet-Segmenten nicht mehr viel Aufmerksamkeit gewidmet werden muss.

Bei Aktivierung der ICMP-Umleitungsfunktion an Layer-3-Schnittstellen besteht bei einer suboptimalen Weiterleitung über Multipoint-Ethernet-Segmente jedoch weiterhin ein potenzieller Leistungsengpass, auch wenn dies aus einem anderen Grund geschieht, wie im Abschnitt "Überlegungen zur Nexus-Plattform" weiter unten in diesem Dokument erläutert wird.

> **Anmerkung:** ICMP-Umleitungen sind auf Layer-3-Schnittstellen der Cisco IOS- und Cisco NX-OS-Software standardmäßig aktiviert.

> **Anmerkung:** Zusammenfassung der Bedingungen, unter denen ICMP-Umleitungsnachrichten generiert werden: Der Layer-3-Switch generiert eine ICMP-Umleitungsnachricht zurück zur Quelle des Datenpakets, wenn das Datenpaket von der Layer-3-Schnittstelle, auf der dieses Paket empfangen wird, weitergeleitet werden soll.

Suboptimale Pfade durch Ethernet-Netzwerke

Interior Gateway Protocols (IGP), wie Open Shortest Path First (OSFP) und Cisco Enhanced Interior Gateway Routing Protocol (EIGRP), wurden entwickelt, um Routing-Informationen zwischen Routern zu synchronisieren und ein konsistentes und vorhersehbares Paketweiterleitungsverhalten auf allen Netzwerkknoten bereitzustellen, die diese Informationen berücksichtigen. Wenn beispielsweise bei Multipoint-Ethernet-Netzwerken alle Layer-3-Knoten in einem Segment die gleichen Routing-Informationen verwenden und sich auf den gleichen Ausgangspunkt zum Ziel einigen, ist eine suboptimale Weiterleitung über solche Netzwerke selten der Fall.

Um zu verstehen, was suboptimale Weiterleitungspfade verursacht, sollten Sie bedenken, dass Layer-3-Knoten die Entscheidungen zur Paketweiterleitung unabhängig voneinander treffen. Die von Router B getroffene Entscheidung über die Paketweiterleitung hängt also nicht von der von Router A getroffenen Entscheidung über die Paketweiterleitung ab. Dies ist eines der wichtigsten Prinzipien, das Sie bei der Fehlerbehebung für die Paketweiterleitung über IP-Netzwerke berücksichtigen müssen. Es ist wichtig, dass Sie dieses beachten, wenn Sie den suboptimalen Weiterleitungspfad in Mehrpunkt-Ethernet-Netzwerken untersuchen.

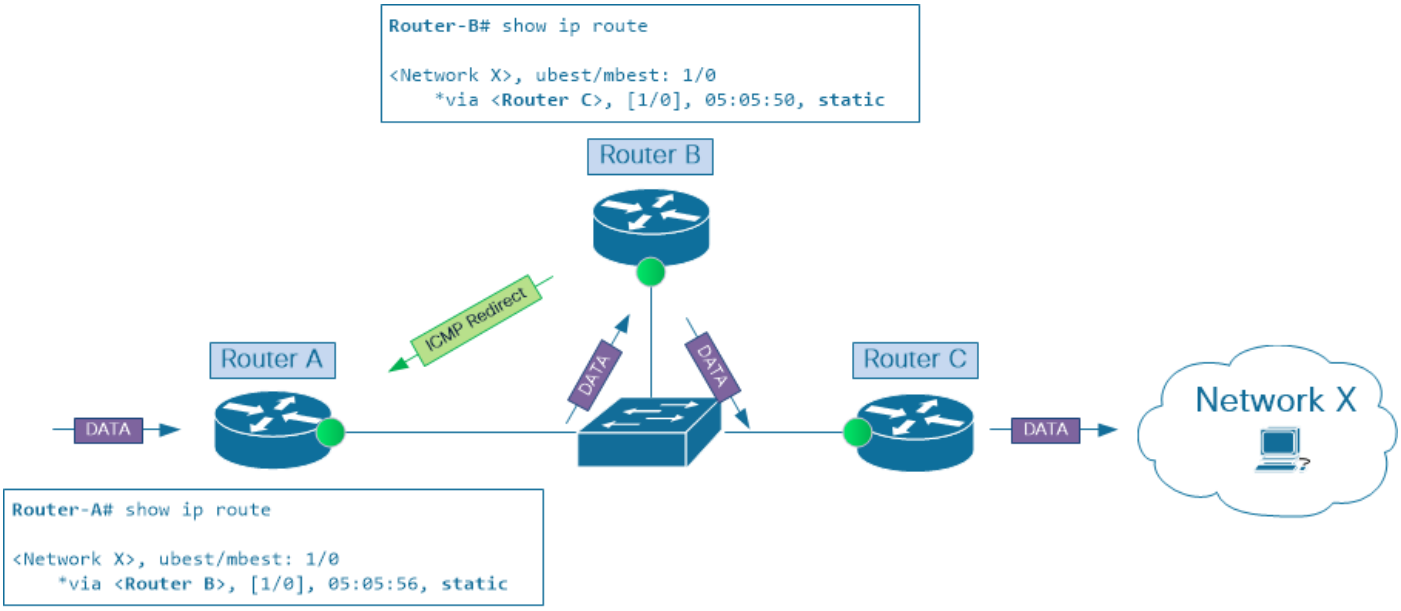
Wie bereits erwähnt, darf es in Netzwerken, in denen alle Router für die Bereitstellung des Datenverkehrs zwischen Endpunkten auf ein einziges dynamisches Routing-Protokoll angewiesen sind, nicht zu einer suboptimalen Weiterleitung über Mehrpunkt-Ethernet-Segmente kommen. In realen Netzwerken ist es jedoch sehr üblich, eine Kombination verschiedener Paketweiterleitungs- und Weiterleitungsmechanismen zu finden. Beispiele für solche Mechanismen sind verschiedene IGPs, statisches Routing und richtlinienbasiertes Routing. Diese Funktionen werden in der Regel gemeinsam verwendet, um die gewünschte Weiterleitung des Datenverkehrs durch das Netzwerk zu erreichen.

Die kombinierte Verwendung dieser Mechanismen kann zwar dazu beitragen, den Datenverkehrsfluss zu optimieren und die Anforderungen eines bestimmten Netzwerkdesigns zu erfüllen, sie übersehen jedoch die Nebenwirkungen, die diese Tools zusammen in Mehrpunkt-Ethernet-Netzwerken verursachen können und die zu einer schlechten Gesamtleistung des Netzwerks führen können.

Statisches Routing

Um dies zu veranschaulichen, betrachten Sie das Szenario in Abbildung 4. Router A hat eine statische Route zu Netzwerk X mit Router B als Next-Hop. Gleichzeitig verwendet Router B Router C als Next-Hop auf statischer Route zu Netzwerk X.

Abbildung 4: Suboptimaler Pfad mit statischem Routing



Suboptimaler Pfad mit statischem Routing

Während der Datenverkehr über Router A in dieses Netzwerk eintritt, es über Router C verlässt und schließlich an das Zielnetzwerk X weitergeleitet wird, müssen Pakete dieses IP-Netzwerk zweimal durchlaufen, um an das Ziel zu gelangen. Dies ist keine effiziente Nutzung von Netzwerkressourcen. Stattdessen würde das direkte Senden von Paketen von Router A an Router C zu denselben Ergebnissen führen, während weniger Netzwerkressourcen benötigt würden.

> **Anmerkung:** Obwohl in diesem Szenario Router A und Router C als Eingangs- und Ausgangs-Layer-3-Knoten für dieses IP-Netzwerksegment verwendet werden, können beide Knoten durch Netzwerkgeräte (z. B. Load Balancer oder Firewalls) ersetzt werden, wenn letztere eine Routing-Konfiguration aufweisen, die zu demselben Paketweiterleitungsverhalten führt.

Richtlinienbasiertes Routing

Policy Based Routing (PBR) ist ein weiterer Mechanismus, der zu suboptimalen Pfaden durch Ethernet-Netzwerke führen kann. Im Gegensatz zu statischem oder dynamischem Routing wird PBR jedoch nicht auf Routing-Tabellenebene ausgeführt. Stattdessen wird die Zugriffskontrollliste (ACL) für die Datenverkehrsumleitung direkt in der Switch-Hardware programmiert. Dies führt dazu, dass bei ausgewählten Datenverkehrsflüssen die Paketweiterleitungssuche auf der Eingangs-Linecard Routing-Informationen umgeht, die über statisches oder dynamisches Routing abgerufen werden.

In Abbildung 4 tauschen Router A und B Routing-Informationen über das Zielnetzwerk X mit einem der dynamischen Routing-Protokolle aus. Beide stimmen darin überein, dass Router B der beste Next-Hop zu diesem Netzwerk ist.

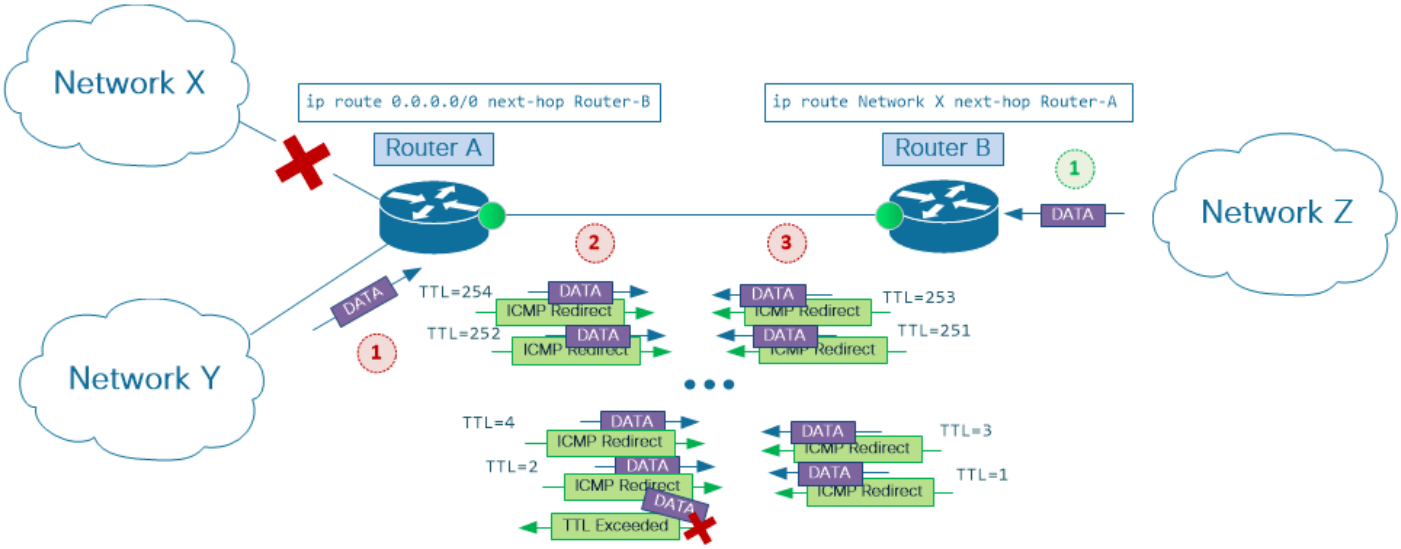
Bei einer PBR-Konfiguration auf Router B, die die vom Routing-Protokoll empfangenen Routing-Informationen überschreibt und Router C als nächsten Hop zu Netzwerk X festlegt, ist die Bedingung zum Auslösen der ICMP-Umleitungsfunktion erfüllt, und das Paket wird zur weiteren Verarbeitung an die CPU von Router B gesendet.

ICMP leitet auf Point-to-Point-Links um

Bisher bezog sich dieses Dokument auf Ethernet-Netzwerke mit drei (oder mehr) verbundenen Layer-3-Knoten, daher der Name "Multipoint Ethernet Networks". Beachten Sie jedoch, dass ICMP-Umleitungsmeldungen auch auf Punkt-zu-Punkt-Ethernet-Verbindungen generiert werden können.

Betrachten wir das Szenario in Abbildung 5. Router A verwendet eine statische Standardroute, um Datenverkehr an Router B zu senden, während Router B eine statische Route zu Netzwerk X hat, die auf Router A verweist.

Abbildung 5 ICMP-Weiterleitungen bei Point-to-Point-Verbindungen



Suboptimaler Pfad mit statischem Routing

Diese Designoption, die auch als Single-Homed-Verbindung bezeichnet wird, ist eine beliebte Option, wenn Sie kleine Benutzerumgebungen mit Service Provider-Netzwerken verbinden. Router B ist ein PE-Gerät (Provider Edge), und Router A ist ein CE-Gerät (User Edge).

Beachten Sie, dass die typische CE-Konfiguration aggregierte statische Routen zu Benutzer-IP-Adressblöcken umfasst, die auf die Null0-Schnittstelle verweisen. Diese Konfiguration ist eine empfohlene Best Practice für die Option mit Single-Homed-CE-PE-Verbindungen mit statischem Routing. Im Rahmen dieses Beispiels wird jedoch davon ausgegangen, dass eine solche Konfiguration nicht vorhanden ist.

Angenommen, Router A verliert die Verbindung zu Netzwerk X, wie in der Abbildung dargestellt. Wenn Pakete vom Benutzer-Netzwerk Y oder Remote-Netzwerk Z versuchen, Netzwerk X zu erreichen, können die Router A und B den Datenverkehr zwischen den Paketen zurückwerfen und das IP-Time-To-Live-Feld in jedem Paket so lange verringern, bis sein Wert 1 erreicht, sodass kein weiteres Routing des Pakets möglich ist.

Während der Datenverkehr zu Netzwerk X zwischen PE- und CE-Routern hin- und herfließt und die Bandbreitennutzung der CE-PE-Verbindungen drastisch (und unnötig) erhöht, verschärft sich das Problem, wenn ICMP-Umleitungen auf einer oder beiden Seiten der Punkt-zu-Punkt-PE-Verbindung aktiviert sind. In diesem Fall wird jedes Paket im an Netzwerk X gerichteten Fluss auf jedem Router mehrmals in CPU verarbeitet, um die ICMP-Umleitungsnachrichten zu generieren.

Überlegungen zur Nexus Plattform

Wenn die ICMP-Umleitung auf der Layer-3-Schnittstelle aktiviert ist und ein eingehendes Datenpaket diese Schnittstelle sowohl zum Ein- als auch zum Ausgang eines Layer-3-Switches verwendet, wird eine ICMP-Umleitungsnachricht generiert. Während die Layer-3-Paketweiterleitung in der Hardware auf der Cisco Nexus 7000-Plattform erfolgt, ist die Switch-CPU weiterhin für die Erstellung der ICMP-Umleitungsnachrichten zuständig. Das visor-Modul benötigt IP-Adressinformationen des Datenflusses, dessen Pfad durch das Netzwerksegment optimiert werden kann. Aus diesem Grund werden Datenpakete von der Eingangs-Linecard an das Supervisor-Modul gesendet.

Wenn Empfänger der ICMP-Umleitungsnachricht diese ignorieren und den Datenverkehr weiterhin an die Layer-3-Schnittstelle des Nexus-Switches weiterleiten, auf der ICMP-Umleitungen aktiviert sind, wird der ICMP-Umleitungsgenerierungsprozess für jedes Datenpaket ausgelöst.

Auf Linecard-Ebene beginnt der Prozess mit einer Ausnahme für die Hardware-Weiterleitung. Auf ASICs werden Ausnahmen ausgelöst, wenn der Paketweiterleitungsvorgang vom Linecard-Modul nicht erfolgreich abgeschlossen werden kann. In diesem Fall müssen Datenpakete zur korrekten Paketbehandlung an das Supervisor-Modul gesendet werden.

> Anmerkung: Die CPU des Supervisor-Moduls generiert nicht nur ICMP-Umleitungsnachrichten, sondern verarbeitet auch viele andere Ausnahmen für die Paketweiterleitung, z. B. IP-Pakete mit einem TTL-Wert (Time To Live) von 1 oder IP-Pakete, die fragmentiert werden müssen, bevor sie an den nächsten Hop gesendet werden.

Nachdem die CPU des Supervisor-Moduls eine ICMP-Umleitungsnachricht an die Quelle gesendet hat, wird die Ausnahmebehandlung abgeschlossen, indem das Datenpaket über das Ausgangs-Linecard-Modul an den nächsten Hop weitergeleitet wird.

Während die Nexus 7000 Supervisor-Module leistungsstarke CPU-Prozessoren verwenden, die große Datenmengen verarbeiten können, ist die Plattform so konzipiert, dass sie den Großteil des Datenverkehrs auf Linecard-Ebene verarbeiten kann, ohne den Supervisor-CPU-Prozessor in den Paketweiterleitungsprozess einbeziehen zu müssen. Auf diese Weise kann sich die CPU auf ihre Kernaufgaben konzentrieren, und der Paketweiterleitungsbetrieb bleibt für dedizierte Hardware-Engines auf den Linecards verfügbar.

In stabilen Netzwerken wird erwartet, dass Ausnahmen bei der Paketweiterleitung, sofern sie auftreten, mit relativ niedrigen Raten erfolgen. Unter dieser Annahme können sie von der Supervisor-CPU behandelt werden, ohne dass ihre Leistung erheblich beeinträchtigt wird. Andererseits können sich bei einer CPU, die mit der Paketweiterleitung befasst ist, Ausnahmen, die mit einer sehr hohen Rate auftreten, negativ auf die Stabilität und Reaktionsfähigkeit des Gesamtsystems auswirken.

Das Design der Nexus 7000-Plattform bietet eine Reihe von Mechanismen zum Schutz der Switch-CPU vor umfangreichen Datenverkehrsmengen. Diese Mechanismen werden an verschiedenen Stellen im System implementiert. Auf Line Card-Ebene gibt es Hardware-Ratenlimitierungen und die Kontrollebene Policing (CoPP). Beide legen Grenzwerte für die Datenverkehrsrate fest, die die Menge des Datenverkehrs steuern, der von jedem Linecard-Modul an den Supervisor weitergeleitet wird.

Diese Schutzmechanismen bevorzugen den Datenverkehr verschiedener Steuerungsprotokolle, die für die Netzwerkstabilität und die Switch-Verwaltbarkeit von entscheidender Bedeutung sind,

wie OSPF, BGP oder SSH, und filtern gleichzeitig aggressiv Datenverkehrstypen, die für die Funktionalität der Kontrollebene des Switches nicht kritisch sind. Der Großteil des Datenverkehrs, der aufgrund von Ausnahmen bei der Paketweiterleitung an die CPU weitergeleitet wird, wird durch solche Mechanismen streng geregelt.

Während Hardware-Ratenlimitierungen und CoPP policing Mechanismen sorgen für die Stabilität der Kontrollebene des Switches und sollten unbedingt immer aktiviert sein. Dies kann einer der Hauptgründe für Datenpaketverluste, Übertragungsverzögerungen und eine insgesamt schlechte Anwendungsleistung im Netzwerk sein. Aus diesem Grund ist es wichtig, die Pfade zu kennen, über die der Datenverkehr das Netzwerk durchläuft, sowie die Verwendung von Tools zur Überwachung der Netzwerkgeräte, die die ICMP-Umleitungsfunktion nutzen können bzw. sollten.

Tools zur Überwachung und Diagnose des Datenverkehrs

show ip traffic

Sowohl Cisco IOS als auch die Cisco NX-OS Software bieten eine Möglichkeit, Statistiken des von der CPU verarbeiteten Datenverkehrs zu überprüfen. Dies wird mit **show ip traffic** aus. Mit diesem Befehl kann der Empfang und/oder die Generierung von ICMP-Umleitungsnachrichten durch einen Switch oder Router auf Layer 3 überprüft werden.

```
Nexus7000#show ip traffic | begin ICMP

ICMP Software Processed Traffic Statistics
----------------------------------------
Transmission:
Redirect: 1000, unreachable: 0, echo request: 0, echo reply: 0,

<output omitted for brevity>

ICMP originate Req: 0, Redirects Originate Req: 1000
Originate deny - Resource fail: 0, short ip: 0, icmp: 0, others: 0
Reception:
Redirect: 0, unreachable: 0, echo request: 0, echo reply: 0,

<output omitted for brevity>

Nexus7000#
```

Ausgeführt show ip traffic einige Male und überprüfen, ob die Zähler für die ICMP-Umleitung inkrementiert werden.

Ethanalyzer

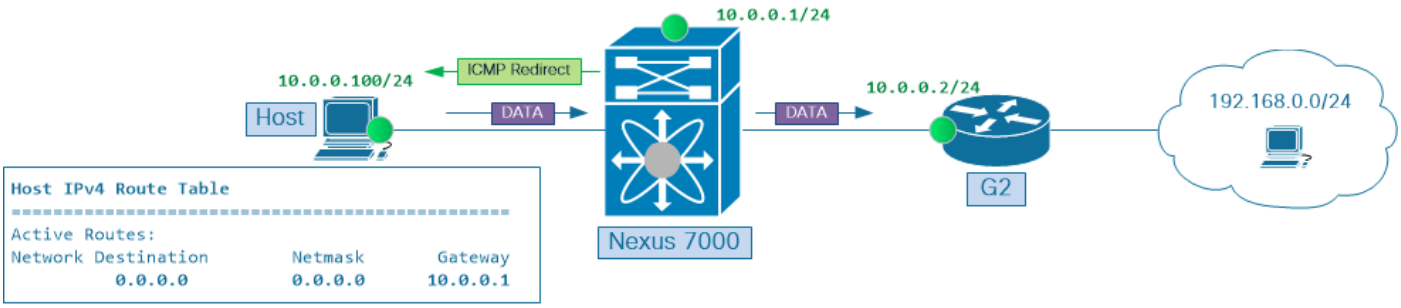
Die Cisco NX-OS Software verfügt über ein integriertes Tool zur Erfassung des Datenverkehrs flowing zwischen Switch-CPUs (auch als Ethanalyzer bekannt).

Anmerkung: Weitere Informationen zu Ethanalyzer finden Sie im Ethanalyzer auf Nexus

7000 Troubleshooting Guide.

Abbildung 6 zeigt ein ähnliches Szenario wie in Abbildung 3. Hier wird Netzwerk X durch das Netzwerk 192.168.0.0/24 ersetzt.

Abbildung 6: Ethanalyzer-Erfassung ausführen



Ethanalyzer Capture ausführen

Der Host 10.0.0.100 sendet einen kontinuierlichen Strom von ICMP-Echoanfragen an die Ziel-IP-Adresse 192.168.0.1. Der Host verwendet die Switch Virtual Interface (SVI) 10 des Nexus 7000-Switches als nächsten Hop zum Remote-Netzwerk 192.168.0.0/24. Zu Demonstrationszwecken ist der Host so konfiguriert, dass er ICMP-Umleitung ignoriert. Nachrichten.

Mit diesem nächsten Befehl können Sie den von der Nexus 7000 CPU empfangenen und gesendeten ICMP-Datenverkehr erfassen:

```
Nexus7000#ethanalyzer local interface inband capture-filter icmp limit-captured-frames 1000

Capturing on inband
2018-09-15 23:45:40.124077   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.124477     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.124533   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.126344   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.126607     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.126655   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
    2018-09-15 23:45:40.128348   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
    2018-09-15 23:45:40.128611     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
    2018-09-15 23:45:40.128659   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.130362   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.130621     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.130669   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.132392   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.132652     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.132700   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.134347   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.134612     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.134660   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.136347   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.136598     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.136645   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.138351   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.138607     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.138656   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request

...
```

Zeitstempel in der vorherigen Ausgabe weisen darauf hin, dass drei Pakete, die in diesem Beispiel hervorgehoben wurden, gleichzeitig erfasst wurden, 2018-09-15 23:45:40.128. Der nächste ist

eine Paketaufschlüsselung dieser Paketgruppe

- Das erste Paket ist das Eingangsdatenpaket, in diesem Beispiel eine ICMP-Echo-Anforderung.
  2018-09-15 23:45:40.128348 10.0.0.100 -> 192.168.0.1 ICMP-Echo (Ping)-Anfrage

- Das zweite Paket ist ein vom Gateway generiertes ICMP-Umleitungspaket. Dieses Paket wird zurück an den Host gesendet.
  2018-09-15 23:45:40.128611 10.0.0.1 -> 10.0.0.100 ICMP Redirect (Redirect for host)

- Das dritte Paket ist das Datenpaket, das nach dem Routing durch die CPU in Egress-Richtung erfasst wird. Die IP-TTL dieses Pakets wurde dekrementiert und die Prüfsumme neu berechnet, obwohl dies zuvor nicht gezeigt wurde.
  2018-09-15 23:45:40.128659 10.0.0.100 -> 192.168.0.1 ICMP-Echo (Ping)-Anfrage

Während Sie durch große Ethianalyzer-Aufnahmen navigieren, die viele Pakete unterschiedlicher Art und Ströme enthalten, kann es schwierig sein, ICMP-Umleitungsnachrichten mit dem Datenverkehr zu korrelieren, der ihnen entspricht.

Konzentrieren Sie sich in diesen Fällen auf ICMP-Umleitungsnachrichten, um Informationen über nicht optimal weitergeleitete Datenverkehrsflüsse abzurufen. ICMP-Umleitungsnachrichten enthalten den Internet-Header sowie die ersten 64 Bit der ursprünglichen Datagrammdaten. Diese Daten werden von der Quelle des Datagramms verwendet, um die Nachricht dem entsprechenden Prozess zuzuordnen.

Verwenden Sie das Paket-Erfassungstool Ethanalyzer mit einem **detaillierten** Schlüsselwort, um den Inhalt von ICMP-Umleitungsnachrichten anzuzeigen und nach IP-Adressinformationen des Datenflusses zu suchen, die nicht optimal weitergeleitet werden.

```
Nexus7000#ethanalyzer local interface inband capture-filter icmp limit-captured-frames 1000
detail

...
Frame 2 (70 bytes on wire, 70 bytes captured)
Arrival Time: Sep 15, 2018 23:54:04.388577000
[Time delta from previous captured frame: 0.000426000 seconds]
[Time delta from previous displayed frame: 0.000426000 seconds]
[Time since reference or first frame: 0.000426000 seconds]
Frame Number: 2
Frame Length: 70 bytes
Capture Length: 70 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:icmp:ip:icmp:data]
Ethernet II, Src: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf), Dst: 00:0a:00:0a:00:0a
(00:0a:00:0a:00:0a)
Destination: 00:0a:00:0a:00:0a (00:0a:00:0a:00:0a)
Address: 00:0a:00:0a:00:0a (00:0a:00:0a:00:0a)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
Source: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf)
Address: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.100 (10.0.0.100)
```

```
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 56
Identification: 0xf986 (63878)
Flags: 0x00
0.. = Reserved bit: Not Set
.0. = Don't fragment: Not Set
..0 = More fragments: Not Set
Fragment offset: 0
Time to live: 255
Protocol: ICMP (0x01)
Header checksum: 0xadd9 [correct]
[Good: True]
[Bad : False]
Source: 10.0.0.1 (10.0.0.1)
Destination: 10.0.0.100 (10.0.0.100)
Internet Control Message Protocol
 Type: 5 (Redirect)
 Code: 1 (Redirect for host)
Checksum: 0xb8e5 [correct]
Gateway address: 10.0.0.2 (10.0.0.2)
Internet Protocol, Src: 10.0.0.100 (10.0.0.100), Dst: 192.168.0.1 (192.168.0.1)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 84
Identification: 0xf986 (63878)
Flags: 0x00
0.. = Reserved bit: Not Set
.0. = Don't fragment: Not Set
..0 = More fragments: Not Set
Fragment offset: 0
Time to live: 254
Protocol: ICMP (0x01)
Header checksum: 0xa8ae [correct]
[Good: True]
[Bad : False]
Source: 10.0.0.100 (10.0.0.100)
Destination: 192.168.0.1 (192.168.0.1)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0 ()
Checksum: 0x02f9 [incorrect, should be 0xcae1]
Identifier: 0xa01d
Sequence number: 36096 (0x8d00)

...
```

Sperrung ICMP adressiert um

Wenn beim Netzwerkdesign der Datenverkehrsfluss von derselben Layer-3-Schnittstelle, auf der er den Switch oder Router betreten hat, geroutet werden muss, kann verhindert werden, dass der Datenverkehrsfluss durch die CPU geleitet wird, wenn Sie die entsprechende ICMP-

Umleitungsfunktion auf der Layer-3-Schnittstelle deaktivieren.

Für die meisten Netzwerke empfiehlt es sich, die ICMP-Umleitungen auf allen Layer 3-Schnittstellen proaktiv zu deaktivieren, sowohl physisch (wie bei der Ethernet-Schnittstelle) als auch virtuell (wie bei Port-Channel- und SVI-Schnittstellen). Verwenden Sie no ip redirects Befehl auf Schnittstellenebene von Cisco NX-OS zum Deaktivieren von ICMP-Umleitungen auf einer Layer-3-Schnittstelle. So überprüfen Sie, ob die ICMP-Umleitungsfunktion deaktiviert ist:

- Sicher**no ip redirects**-Befehl wird zur Schnittstellenkonfiguration hinzugefügt.

```
Nexus7000#show run interface vlan 10

interface Vlan10
no shutdown no ip redirects
  ip address 10.0.0.1/24
```

- Stellen Sie sicher, dass der Status von "ICMP Redirects" auf der Schnittstelle "disabled" (deaktiviert) anzeigt.

```
Nexus7000#show ip interface vlan 10 | include redirects
  IP icmp redirects: disabled
```

- Stellen Sie sicher, dass die Softwarekomponente Cisco NX-OS, die die Schnittstellenkonfiguration vom Switch-Supervisor auf eine oder mehrere Linecards überträgt, das Aktivieren/Deaktivieren der ICMP-Umleitung auf **0** setzt.

```
Nexus7000#show system internal eltm info interface vlan 10 | i icmp_redirect
  per_pkt_ls_en = 0, icmp_redirect = 0, v4_same_if_check = 0
```

- Stellen Sie sicher, dass das Aktivieren/Deaktivieren-Flag für die ICMP-Umleitung für eine bestimmte Layer-3-Schnittstelle auf einer oder mehreren Linecards auf **0** festgelegt ist.

```
Nexus7000#attach module 7
Attaching to module 7 ...
To exit type 'exit', to abort type '$.'
Last login: Wed Sep 15 23:56:25 UTC 2018 from 127.1.1.1 on pts/0
module-7#

!--- Optionally, jump to non-admin Virtual Device Context (VDC) if verification needs to be done
in one of the custom VDCs
module-7#vdc 6

module-7#show system internal iftmc info interface vlan 10 | include icmp_redirect
icmp_redirect : 0x0 ipv6_redirect : 0x1
```

Zusammenfassung

Der in RFC 792 beschriebene ICMP-Umleitungsmechanismus wurde zur Optimierung des Weiterleitungspfads über Multipoint-Netzwerksegmente entwickelt. Zu Beginn des Internets trug eine solche Optimierung dazu bei, teure Netzwerkressourcen wie Verbindungsbandbreite und CPU-Zyklen der Router zu schützen. Da die Netzwerkbandbreite erschwinglicher wurde und sich relativ langsames CPU-basiertes Paketrouting zu schnellerer Layer-3-Paketweiterleitung in dedizierten Hardware-ASICs entwickelte, verringerte sich die Bedeutung einer optimalen Datenübertragung durch Multipoint-Netzwerksegmente. Standardmäßig ist die ICMP-

Weiterleitungsfunktion auf jeder Layer-3-Schnittstelle aktiviert. Die Versuche, Netzwerkknoten in Mehrpunkt-Ethernet-Segmenten über optimale Weiterleitungspfade zu informieren, werden jedoch nicht immer vom Netzwerkpersonal verstanden und darauf reagiert. In Netzwerken mit kombinierter Verwendung verschiedener Weiterleitungsmechanismen, wie z. B. statisches Routing, dynamisches Routing und richtlinienbasiertes Routing, kann dies zu einer unerwünschten Verwendung der Transitknoten-CPU zur Verarbeitung des Produktionsdatenverkehrs führen, wenn die ICMP-Umleitungsfunktion aktiviert ist und nicht ordnungsgemäß überwacht wird. Dies wiederum kann erhebliche Auswirkungen auf den Produktionsdatenverkehr und die Stabilität der Netzwerkinfrastruktur auf der Kontrollebene haben.

Für die meisten Netzwerke wird es als Best Practice erachtet, die ICMP-Umleitungsfunktion auf allen Layer-3-Schnittstellen in der Netzwerkinfrastruktur proaktiv zu deaktivieren. Dadurch können Szenarien mit Produktionsdatenverkehr vermieden werden, der in der CPU von Layer-3-Switches und -Routern verarbeitet wird, wenn ein besserer Weiterleitungspfad durch Multipoint-Netzwerksegmente vorhanden ist.

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.