Fehlerbehebung bei komplexen OSPF-Fehlermeldungen

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Probleme
Ausgabe 1
Ausgabe 2
Ausgabe 3
Lösungen
Problemlösung 1
Typ-2-LSAs
Typ-3-LSAs
Typ-5-LSAs
Problemlösung 2
Problemlösung 3
Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie Sie OSPF-Fehlermeldungen (Open Shortest Path First) beheben können, die im normalen Netzwerkbetrieb auftreten und die Netzwerkverbindungen beeinträchtigen können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse der OSPF-Grundlagen zu verfügen.

Verwendete Komponenten

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Das OSPF-Protokoll ist ein weit verbreitetes Interior Gateway Protocol (IGP) in Enterprise- und Service Provider-Netzwerken.

Dieses Protokoll wurde entwickelt, weil die Internetgemeinschaft ein hochfunktionales, nicht proprietäres IGP für die TCP/IP-Protokollfamilie einführen muss. Die Diskussionen über die Schaffung eines gemeinsamen interoperablen IGP für das Internet begannen 1988 und wurden erst 1991 formalisiert. Damals forderte die OSPF-Arbeitsgruppe, OSPF für die Weiterentwicklung des Entwurfs eines Internet-Standards in Betracht zu ziehen.

Das OSPF-Protokoll basiert auf der Link-State-Technologie. Dies ist eine Abweichung von den vektorbasierten Bellman-Ford-Algorithmen, die in herkömmlichen Internet-Routing-Protokollen wie Routing Information Protocol (RIP) verwendet werden.

Probleme

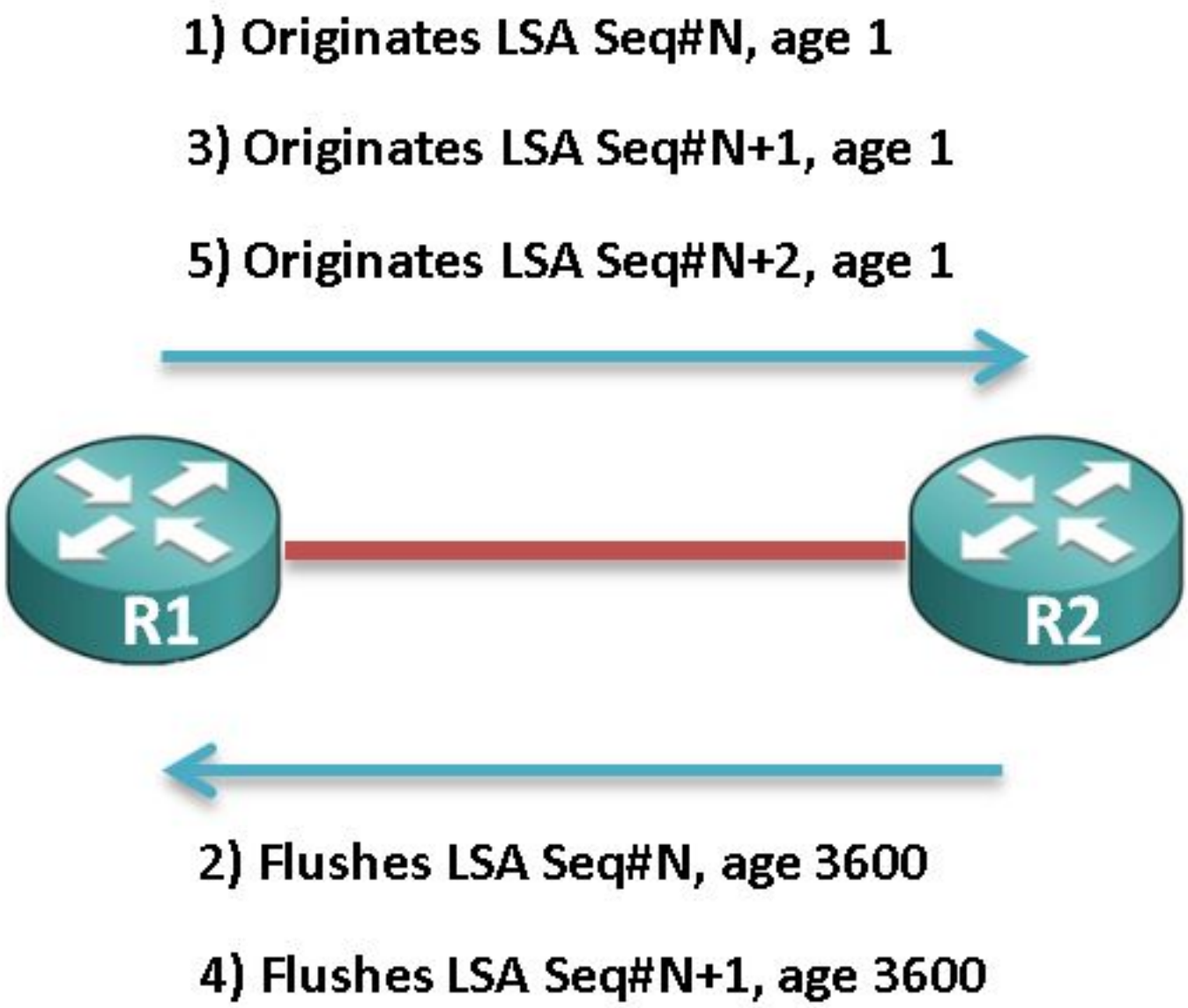
In diesem Abschnitt werden drei OSPF-Probleme beschrieben, die die Netzwerkverbindungen beeinträchtigen könnten.

Ausgabe 1

Sie erhalten die Fehlermeldung **OSPF-4-FLOOD_WAR**. Der OSPF-Hochwasserkrieg tritt ein, wenn der Router wiederholt seine eigene Link State Advertisement (LSA) erhält und diese aus dem Netzwerk entfernt oder eine neue Version davon sendet. Diese Funktion dient zum Erkennen von Problemen mit Typ-2-LSAs, wenn im Netzwerk doppelte IP-Adressen vorhanden sind, oder mit Typ-5-LSAs, wenn in verschiedenen OSPF-Bereichen eine doppelte Router-ID vorhanden ist.

In einem typischen Szenario gibt es einen Router im Netzwerk, der das LSA generiert, und einen zweiten Router, der das LSA leeren soll.

Dieses Bild veranschaulicht die Ursprungs- und Flush-Ereignisse zwischen dem ersten und dem zweiten Router (jeweils mit dem Namen R1 bzw. R2):



Ausgabe 2

Sie erhalten die Fehlermeldung **%OSPF-4-CONFLICTING_LSAID**. Diese Fehlermeldung weist darauf hin, dass eine LSA-Erstellung aufgrund eines Konflikts mit einem aktuellen LSA verhindert wurde, der dieselbe Link-State-ID, aber eine andere *Subnetzmaske* hat.

Der Algorithmus in RFC 2328, Anhang E, wird verwendet, um Konflikte zu lösen, wenn mehrere LSAs mit demselben Präfix und unterschiedlichen Masken angekündigt werden. Wenn dieser Algorithmus verwendet wird und die Hostrouten angekündigt werden, gibt es Situationen, in denen eine Konfliktlösung nicht möglich ist und entweder die Hostroute oder das Präfix, in dem Konflikte nicht angekündigt werden, nicht angegeben wird.

Hier ein Beispiel für einen Ausschnitt der Fehlermeldung:

```
%OSPF-4-CONFLICTING_LSAID: LSA origination prevented by existing LSA with same LSID
but a different mask

Existing Type 5 LSA: LSID 192.168.1.0/31
New Destination: 192.168.1.0/32
```

Ausgabe 3

Sie konfigurieren OSPF, um die Funktion "Fast Hello Packets" zu verwenden, die eine hohe CPU verursacht. Die OSPF-Unterstützung für die Funktion "Fast Hello Packets" ermöglicht Konfigurationen, bei denen die Hello-Pakete in Intervallen von weniger als einer Sekunde gesendet werden. Diese Konfigurationen führen zu einer schnelleren Konvergenz in einem OSPF-Netzwerk.

Dieser Befehl wird verwendet, um das Intervall festzulegen, in dem mindestens ein Hello-Paket empfangen werden muss, oder der Nachbar wird als ausgefallen eingestuft:

```
ip ospf dead-interval minimal hello-multipliermultiplier
```

Hier ein Beispiel:

```
Router(config-if)# ip ospf dead-interval minimal hello-multiplier 5
```

In diesem Beispiel wird die OSPF-Unterstützung für Fast Hello-Pakete mit der Angabe des **minimalen** Schlüsselworts, des **hello-multiplier-**Schlüsselworts und des Werts aktiviert. Da der Multiplikator auf **5** festgelegt ist, werden pro Sekunde fünf Hello-Pakete gesendet.

Lösungen

In diesem Abschnitt werden einige mögliche Lösungen für die im vorherigen Abschnitt beschriebenen Probleme beschrieben.

Problemlösung 1

Es ist wichtig, dass Sie die Fehlermeldung verstehen, wenn Sie versuchen, Hochwasserkriegsmeldungen zu beheben. Die Meldungen erscheinen auf den Ursprungs- und Flush-Routern anders. Aus diesem Grund ist es wichtig, sich auf den LSA-Typ zu konzentrieren, für den die Meldung zur Flutungskriegsmeldung gemeldet wird, da für jeden LSA-Typ eine andere Fehlerbehebung durchgeführt wird.

Hier ein Beispiel für einen Ausschnitt der OSPF-Hochwasserkriegsmeldung:

```
%OSPF-4-FLOOD_WAR: Process 1 re-originates LSA ID 172.16.254.25 type-2 adv-rtr
172.16.253.1 in area 0

%OSPF-4-FLOOD_WAR: Process 1 flushes LSA ID 172.16.254.25 type-2 adv-rtr
172.16.253.1 in area 0
```

Im Folgenden werden die Nachrichtenkomponenten beschrieben:

- **Prozess** - Dies ist der OSPF-Prozess, der den Fehler meldet.
- **Erneutes Generieren** oder **Spülung** - Dies zeigt an, ob dieser Router LSA *generiert* oder *leeren kann*.
- **LSA-ID** - Dies ist die LSA-ID, für die der Hochwasserkrieg erkannt wird.

- **Typ** - Dies ist der LSA-Typ.
  Hinweis: Der Hochwasserkrieg für jedes LSA hat eine andere Ursache.
- **adv-rtr** - Dies ist der Werberouter, der vom LSA stammt.

- **Area** - Dies ist der Bereich, zu dem das LSA gehört.

Typ-2-LSAs

> **Hinweis**: Weitere Informationen, falls der Hochwasserkrieg für ein Typ-2-LSA gedruckt wird, finden Sie RFC 2328 (Kapitel 13.4, Fall 3).

Wenn ein Router ein LSA für ein Netzwerk vom Typ 2 empfängt, dessen LSA-ID mit der IP-Adresse für eine der Schnittstellen übereinstimmt, die diesem Router zugeordnet sind, muss der Router das LSA leeren. Die Hauptursache in diesem Szenario sind die doppelten IP-Adressen auf den Ursprungs- und Flush-Routern.

Um dieses Problem zu beheben, konfigurieren Sie die IP-Adresse auf einer der Schnittstellen neu oder deaktivieren Sie die Schnittstelle, die die doppelte IP-Adresse hat.

> **Hinweis**: Diese Prüfung auf doppelte IP-Adressen wird auch an ausgefallenen Schnittstellen durchgeführt. Die Schnittstelle muss sich im *Admin-Down*-Modus befinden, um die Prüfung zu umgehen. In einigen Fällen wird der Hochwasserkrieg auch für eine Schnittstelle gemeldet, die vom Administrator geschlossen wurde. Die permanente Lösung besteht also darin, die doppelten IP-Adressen im Netzwerk zu entfernen.

Typ-3-LSAs

Es kommt selten vor, dass bei einem Typ-3-LSA Probleme durch Hochwasserkriege auftreten. Hochwasserkriegsfehlermeldungen für Typ-3-LSAs wurden in Szenarien aufgezeichnet, in denen das IP-Subnetz einer stark flapping-Verbindung in der OSPF-Domäne propagiert wird.

Cisco empfiehlt, beim Cisco Technical Assistance Center (TAC) ein Support-Ticket zu erstellen, wenn Probleme aufgrund von Typ-3-LSAs im Hochwasserkrieg auftreten.

Typ-5-LSAs

Überflutungskriege aufgrund von Typ-5-LSAs treten auf, wenn Router-IDs auf Routern in verschiedenen Bereichen doppelt vorhanden sind. Die Router-ID eines Routers muss geändert werden.

Eine weitere Instanz von Typ-5-Hochwasserkriegen ist, wenn es zwei Router gibt, die über dieselbe Border Gateway Protocol (BGP)-Netzwerkanweisung verfügen und beide Router diese BGP-Netzwerke an OSPF weiterverteilen. Wenn einer dieser BGP-Router das Netzwerk über OSPF erreicht, wird ein OSPF-Hochwasserkrieg aufgrund eines Typ-5-LSAs gemeldet.

Stellen Sie zusammenfassend sicher, dass die Router-IDs nicht identisch sind, und die richtige

Umverteilung der externen LSAs sollte Hochwasserkriegsprobleme aufgrund von Typ-5-LSAs verhindern.

Problemlösung 2

Der erste Schritt, den Sie bei Versuchen unternehmen sollten, die Fehlermeldung **OSPF-CONFLICTING_LSAID** aufzulösen, besteht darin, das Präfix zu suchen, das nicht angekündigt wird, sowie das Präfix, das in Konflikt steht.

Um diese zu finden, geben Sie die Befehle **show ip route** und **show ip ospf database** in die CLI ein. Der Administrator muss den Ursprung des **neuen Ziels**: **192.168.1.0/32**, wie im Beispielfall im Issue 2-Abschnitt beschrieben, und korrigieren Sie die Subnetzmaske des Netzwerks.

Der übliche Fall von miteinander in Konflikt stehenden LSA-IDs wird nach einer kürzlich vorgenommenen Änderung in OSPF protokolliert und behoben, nachdem Sie die Konfiguration der Subnetzmasken in den OSPF-Netzwerkanweisungen korrigiert haben.

Problemlösung 3

Hohe CPU-Fälle werden beim Cisco TAC protokolliert, wenn Kunden OSPF Fast Hellos auf Cisco Catalyst Switches bereitstellen.

> **Hinweis**: Cisco empfiehlt, keine OSPF Fast Hellos zu konfigurieren.

Cisco IOS® wird auf einem nicht präemptiven Modell ausgeführt, und die Funktion "Fast Hello Packet" erfordert, dass die OSPF Hellos häufiger verarbeitet werden als das Dead-Intervall von einer Sekunde. Es kann sein, dass OSPF nicht die erforderlichen Ressourcen auf einem System mit anderen langlaufenden Prozessen bezieht. Abhängig von Ihrer Umgebung und den anderen Protokollen und Anwendungen, die auf dem Router konfiguriert sind, kann die Verwendung dieser Funktion problematisch sein.

Die Alternative von "Hello" in Sekundenbruchteilen wurde durch Bi-Directional Forwarding Detection (BFD) eingeführt, bei der BFD für die schnelle Erkennung von Nachbarn entwickelt wurde. BFD läuft im *Interrupt*-Modus und unterliegt nicht den Problemen, die bei OSPF fast Hellos beobachtet werden. Cisco empfiehlt die Verwendung von BFD für schnellere Konvergenz.

Es gibt zwei bekannte Fehler aufgrund von OSPF fast Hellos:

- Cisco Bug-ID CSCut14044: *WS-C3750X-48/OSPF Fast Hello 333 ms/Adjacency-Drop/15.0(2)SE6*
- Cisco Bug-ID CSCsd17835: *OSPF/HSRP Fast Hello Adjacencies flattern fortlaufend.*

Zugehörige Informationen

- Fehlerbehebung bei doppelten Router-IDs mit OSPF
- Support und Downloads - Cisco Systems

- Technischer Support und Dokumentation - Cisco Systems