

VLANインスタンスの制限によるネットワーク停止について

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[VLANインスタンスの制限について](#)

[VLANインスタンスの制限を超えるリスク](#)

[一般的な症状](#)

[予防と緩和のテクニック](#)

[結論](#)

はじめに

このドキュメントでは、ローエンドレガシーCatalystスイッチのVLANインスタンス制限によるネットワーク停止の可能性と、その防止について説明します。

前提条件

要件

シスコでは、スパニングツリープロトコル(STP)とCisco Catalystスイッチの機能に関する知識に加えて、基本的なスイッチングの概念に関する知識があることを推奨しています。

使用するコンポーネント

このドキュメントの情報は、主にローエンドレガシーデバイスであるCisco Catalystスイッチに基づくもので、特定のソフトウェアやハードウェアのバージョンに限定されることなく、すべてのバージョンに適用できます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ネットワークインフラストラクチャの信頼性は組織の運用にとって重要であり、ネットワークハ

ードウェアの制約を管理することは、継続的な安定性を確保する鍵となります。ローエンドレガシーのCatalystスイッチは、多くの古いネットワーク環境に欠かせないものですが、多くの場合、VLANインスタンスの制限などの重大な問題を引き起こす可能性のある制限に直面します。この制限は、スイッチが同時にサポートできるSTPインスタンスの数に関係します。これらのスイッチでVLANインスタンスの上限に達すると、追加のVLANに対してSTPを有効にすることができなくなり、ネットワークループや機能停止のリスクが生じます。

VLANインスタンスの制限について

ループ防止用にSTPを必要とするスイッチ上の各VLANは、個別のインスタンスとしてカウントされます。ローエンドスイッチおよびレガシースイッチには、処理できる同時STPインスタンスの数に対して厳密な制限があります。最大値に達すると、追加のVLANはSTPセーフガードなしで動作するため、ネットワークはブロードキャストストームや広範な停止を引き起こす可能性があるループに対して脆弱になります。

サポートする数よりも多くのVLANで動作するCisco Catalyst 3850スイッチの例：

```
<#root>
```

```
Switch#show run | i span
```

```
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree extend system-id
```

```
no spanning-tree vlan 43,125,402,404,406,409,412,414-415,418-420,422-424,426 < ----- STP disabled on the
```

```
no spanning-tree vlan 427,430
```

```
spanning-tree vlan 1-1005 priority 40960
```

スイッチは、サポートされているスパンニングツリーインスタンスの最大数で動作しています。

```
<#root>
```

```
Switch#show spannig-tree summary totals
```

```
Name          Blocking Listening Learning Forwarding STP Active
```

```
-----
```

```
128 vlans < -----
```

```
          29          0          0         1481         1510
```

```
Switch#show spanning-tree instances
```

MAX STP instances supported is 128 < -----

VLANインスタンスの制限を超えるリスク

スイッチ上のVLANインスタンスの制限を超えても、通常はただちに停止することはありません。その代わりに、ネットワークの再設定時や新しい接続が誤ってループを作成する際に、予期せぬ潜在的なリスクが発生する可能性があります。これらのループを検出してブロックするSTPがなければ、1回の手順ミスがネットワークの重大な中断に連鎖する可能性があります。

一般的な症状

1. MAC – フラップ :

```
%MAC_MOVE-SW1-4-NOTIF: Host xxxx.xxxx.xxxx in vlan <> is flapping between port (1) and port (2)
%MAC_MOVE-SW1-4-NOTIF: Host yyyy.yyyy.yyyy in vlan <> is flapping between port port (1) and port (2)
%MAC_MOVE-SW1-4-NOTIF: Host zzzz.zzzz.zzzz in vlan <> is flapping between port (1) and port (2)
```

2. トポロジ変更通知 :

<#root>

```
VLAN0999 is executing the rstp compatible Spanning Tree protocol
  Number of topology
```

```
changes 72413
```

```
  last change occurred
```

```
00:00:05 ago
```

```
      from TenGigabitEthernet1/1/1
```

```
VLAN0608 is executing the rstp compatible Spanning Tree protocol
  Number of topology
```

```
changes 1106
```

```
  last change occurred
```

```
00:07:53 ago
```

```
      from TenGigabitEthernet1/1/1
```

```
VLAN0301 is executing the rstp compatible Spanning Tree protocol
  Number of topology
```

changes 25824

last change occurred

00:03:13 ago

from Port-channel21

3. 割り込み/ARP入力/STPプロセスが原因の高いCPU使用率：

<#root>

CPU utilization for

five seconds: 99%/5%;

one minute: 98%; five minutes: 97%

PID	Runtime(ms)	Invoked	uSecs	5Sec	1Min	5Min	TTY	Process
-----	-------------	---------	-------	------	------	------	-----	---------

11	48417100	4048595	11957	28.47%	27.55%	27.15%	0	ARP Input < ----- High CPU due to ARP Inp
130	2296685	1887488	1216	21.19%	20.49%	20.01%	0	Spanning Tree
205	12387701	1054338	11749	8.91%	9.02%	9.10%	0	Hu1c LED Process
88	3036802	283172	10723	6.71%	6.98%	6.85%	0	IP Input
44	867032	754781	1148	4.27%	4.45%	4.35%	0	Interrupts

予防と緩和のテクニック

ローエンドのレガシーCatalystスイッチでのVLANインスタンスの制限に関連するリスクを軽減するために、ネットワーク管理者はいくつかの戦略を採用できます。

1. VLANの統合：可能な場合はネットワークトラフィックを結合または再セグメント化することにより、STPを使用してVLANの数を削減します。
2. MSTPの実装：PVST+またはRapid-PVST+からMultiple Spanning Tree Protocol(MSTP)に移行して、VLANをより少ない数のSTPインスタンスにグループ化します。
3. STPへの参加の最適化：ループのリスクが低いVLAN上、または代替のループ防止メカニズムが導入されているネットワークのセグメントでSTPを無効にします。
4. ネットワークインフラストラクチャのアップグレード：古いローエンドスイッチを、より多くのSTPインスタンスをサポートできる最新のハードウェアに置き換えます。
5. ネットワークの再設計：トラフィックフローを最適化し、必要なVLANの数を削減し、既存のハードウェアの機能とより適切に連携するために、ネットワーク設計を再評価します。

結論

ローエンドのレガシースイッチでVLANインスタンスの上限に達することは、対処しなければネットワークの停止につながるタイムボムとなり得ます。このリスクを軽減し、老朽化したテクノロジーに直面したネットワークインフラストラクチャの復元力を確保するには、ハードウェアの

アップグレードや戦略的なネットワーク設計の調整など、プロアクティブなネットワーク管理が不可欠です。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。