Informazioni sulle interruzioni della rete causate dal limite di istanze della VLAN

Sommario

Introduzione

In questo documento vengono descritte le potenziali interruzioni della rete dovute al limite di istanza della VLAN sugli switch Catalyst legacy di fascia bassa e alla loro prevenzione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei concetti base dello switching, nonché la comprensione dello Spanning Tree Protocol (STP) e delle sue funzionalità sugli switch Cisco Catalyst.

Componenti usati

Le informazioni di questo documento si basano sugli switch Cisco Catalyst, principalmente dispositivi legacy di fascia bassa, e sono applicabili a tutte le versioni, senza restrizioni a versioni software o hardware specifiche.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'affidabilità dell'infrastruttura di rete è fondamentale per le operazioni organizzative e la gestione

dei vincoli dell'hardware di rete è fondamentale per garantire una stabilità costante. Gli switch Catalyst legacy di fascia bassa, che sono la base in molti ambienti di rete meno recenti, spesso devono affrontare un limite che può portare a problemi significativi come il limite di istanza della VLAN. Questo limite si riferisce al numero di istanze STP che uno switch può supportare contemporaneamente. Quando un'organizzazione raggiunge il limite di istanza VLAN su questi switch, non può abilitare il protocollo STP per altre VLAN, il che comporta un rischio di loop di rete e di potenziali interruzioni.

Informazioni sul limite delle istanze VLAN

Ogni VLAN su uno switch che richiede l'STP per la prevenzione del loop viene conteggiata come istanza separata. Gli switch low-end e legacy hanno limiti rigidi sul numero di istanze STP simultanee che possono gestire. Una volta raggiunto il massimo, le VLAN aggiuntive funzionano senza salvaguardie STP, lasciando la rete vulnerabile a loop che possono causare tempeste di trasmissione e interruzioni diffuse.

Ad esempio, su uno switch Cisco Catalyst 3850 che funziona con un numero di VLAN superiore a quello supportato:

<#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

Lo switch funziona con il numero massimo di istanze Spanning Tree supportate.

<#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 < -----
```

Rischi di superamento del limite di istanza della VLAN

Il superamento del limite di istanza della VLAN su uno switch in genere non attiva un'interruzione immediata. Crea invece un rischio latente che può manifestarsi in modo imprevisto, spesso durante i periodi di riconfigurazione della rete o quando una nuova connessione crea inavvertitamente un loop. Senza STP per rilevare e bloccare questi loop, un passaggio errato può causare un'interruzione significativa della rete.

Sintomi comuni

1. MAC - Flap:

```
%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. Notifiche di modifica della topologia:

```
<#root>
VLAN0999 is executing the rstp compatible Spanning Tree protocol
  Number of topology
changes 72413
 last change occurred
0o: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. Utilizzo elevato della CPU dovuto a interrupt/processi di input ARP/STP:

<#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 Hulc 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
```

Tecniche di prevenzione e mitigazione

Gli amministratori di rete possono utilizzare diverse strategie per ridurre il rischio associato al limite delle istanze VLAN sugli switch Catalyst legacy di fascia bassa:

1. Consolidamento delle VLAN: riduzione del numero di VLAN con l'STP attraverso la combinazione o la risegmentazione del traffico di rete, ove possibile.
2. Implementare MSTP: passare da PVST+ o Rapid-PVST+ a Multiple Spanning Tree Protocol (MSTP) per raggruppare le VLAN in meno istanze STP.
3. Ottimizza partecipazione STP: disabilita STP sulle VLAN in cui i rischi di loop sono bassi o in segmenti della rete in cui sono presenti meccanismi alternativi di prevenzione loop.
4. Aggiornamento dell'infrastruttura di rete: sostituzione dei vecchi switch di fascia bassa con hardware moderno in grado di supportare un numero maggiore di istanze STP.
5. Riprogettare la rete: valutare nuovamente la progettazione della rete per ottimizzare i flussi di traffico, ridurre il numero di VLAN richieste e allinearsi meglio alle funzionalità dell'hardware esistente.

Conclusioni

Raggiungere il limite di istanza della VLAN sugli switch legacy di fascia bassa è una bomba a orologeria che può causare interruzioni di rete se non viene risolta. La gestione proattiva della rete, inclusi gli aggiornamenti hardware e gli adeguamenti strategici della progettazione della rete, è essenziale per ridurre questo rischio e garantire la resilienza dell'infrastruttura di rete di fronte all'invecchiamento della tecnologia.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).