Understand Network Outages Due to VLAN Instance Limit

Contents

Introduction

This document describes potential network outages due to the VLAN instance limit on low-end legacy catalyst switches and their prevention.

Prerequisites

Requirements

Cisco recommends that you have knowledge of basic switching concepts, along with an understanding of the Spanning Tree Protocol (STP) and its features on Cisco Catalyst switches.

Components Used

The information in this document is based on Cisco Catalyst switches, primarily low-end legacy devices, and is applicable across all versions, without being restricted to any specific software or hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The reliability of network infrastructure is critical for organizational operations, and managing the constraints of networking hardware is key to ensuring ongoing stability. Low-end legacy Catalyst switches, which are a staple in many older network environments, often face a limitation that can lead to significant issues like the VLAN instance limit. This limit pertains to the number of STP instances a switch can support concurrently. When an organization reaches the VLAN instance limit on these switches, it cannot enable STP for additional VLANs, which poses a risk of network loops and potential outages.

Understanding VLAN Instance Limit

Each VLAN on a switch that requires STP for loop prevention counts as a separate instance. Low-end and legacy switches have strict limits on the number of concurrent STP instances they can handle. Once the maximum is reached, any additional VLANs operate without STP safeguards, leaving the network vulnerable to loops that can result in broadcast storms and widespread outages.

An example of a Cisco Catalyst 3850 switch operating with more VLANs than it supports:

<#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
```

The switch is operating with the maximum number of supported Spanning Tree instances.

<#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 < -----
```

Risks of Exceeding VLAN Instance Limit

Exceeding the VLAN instance limit on a switch does not typically trigger an immediate outage. Instead, it creates a latent risk that can manifest unexpectedly, often during times of network reconfiguration or when a new connection inadvertently creates a loop. Without STP to detect and block these loops, a single misstep can cascade into a significant network disruption.

Common Symptoms

1. MAC - Flaps:

```
%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. Topology Change Notifications:

<#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. High CPU Utilization Due to Interrupts/ARP Input/STP Processes:

<#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
```

Prevention and Mitigation Techniques

Network administrators can employ several strategies in order to mitigate the risk associated with the VLAN instance limit on low-end legacy Catalyst switches:

1. Consolidate VLANs: Reduce the number of VLANs using STP by combining or resegmenting network traffic where feasible.
2. Implement MSTP: Move from PVST+ or Rapid-PVST+ to Multiple Spanning Tree Protocol (MSTP) to group VLANs into fewer STP instances.
3. Optimize STP Participation: Disable STP on VLANs where loop risks are low or in segments of the network where alternate loop prevention mechanisms are in place.
4. Upgrade Network Infrastructure: Replace older, low-end switches with modern hardware capable of supporting a larger number of STP instances.
5. Redesign the Network: Re-evaluate the network design in order to optimize traffic flows, reduce the number of required VLANs, and better align with the capabilities of the existing hardware.

Conclusion

Reaching the VLAN instance limit on low-end legacy switches is a ticking time bomb that can lead to network outages if not addressed. Proactive network management, including hardware upgrades and strategic network design adjustments, is essential in order to mitigate this risk and ensure the resilience of the network infrastructure in the face of aging technology.