MCP Issues and mitigation [William PowerPoint make now]

Contents

[Introduction: 1](#_Toc156464244)

[Known Hotspots Analysis 1](#_Toc156464245)

[Background Analysis 1](#_Toc156464246)

[Long-Term Strategies 1](#_Toc156464247)

[IAAS Team Consultation: 1](#_Toc156464248)

[Consideration of ACI 6.0x Upgrade: 1](#_Toc156464249)

[Short-Term Strategies 1](#_Toc156464250)

[EPG Management: 1](#_Toc156464251)

[Communication Plan 1](#_Toc156464252)

[To Management: 1](#_Toc156464253)

[To Cisco: 1](#_Toc156464254)

[R&D and Infrastructure 1](#_Toc156464255)

[Architecture Redesign: 1](#_Toc156464256)

[Risk Management: 1](#_Toc156464257)

[Risk Acceptance: 1](#_Toc156464258)

[Conclusion 1](#_Toc156464259)

# Introduction:

The network environment faces several challenges related to MCP issues, especially after the ACI 5.2(8e) upgrade. Addressing these issues requires a strategic approach incorporating short-term and long-term solutions.

# Known Hotspots Analysis

The table shows specific hotspots in the network, which are crucial for targeting MCP mitigation efforts. Each switch ID and port channel number, paired with the respective host, indicates areas where vulnerabilities may exist.  
Flexpod hot spots

|  |  |  |
| --- | --- | --- |
| **Switch ID** | **Port channel number** | **Host** |
| 221 | Po2, Po3 | ufceid007 |
| 222 | Po2, Po4 |
| 311 | Po15, Po17 | ufceid005 |
| 312 | Po16, Po20 |
| 407 | Po5, Po8 | ufceid006 |
| 408 | Po17, Po30 |
| 415 | Po12, Po8 | ufceid004 |
| 416 | Po10, Po16 |
| 803 | Po1, Po2 | ufceid009 |
| 804 | Po1, Po2 |

# Background Analysis

Post-Upgrade Emergence of Issues: The visibility of MCP issues following the upgrade to ACI 5.2(8e) suggests that these issues were latent in the system and previously masked by older versions.  
 This upgrade surfaced these existing challenges.

# Long-Term Strategies

## IAAS Team Consultation:

Collaboration with the IAAS team, including TSC Thiyagu etc., under the coordination of cross-team leads like Niels and David is essential.

Such collaboration will be vital for holistic problem-solving and for developing a sustainable network architecture.

## Consideration of ACI 6.0x Upgrade:

Though upgrading to ACI 6.0x was not recommended previously. It's crucial to reassess this option with current data.

Engage in a bug scrub for the 6.0x image and consult Cisco via NTT OPS for recommendations on stable releases. **Deciding who will take the initiative for this is key**.

## Short-Term Strategies

#### Cleanup of Unused Trunks and VLANs:

The customer should focus on cleaning up unused trunks or pruning trunked VLANs, particularly in the identified hotspots. This will help in reducing complexity and potential MCP triggers.

## EPG Management:

Address EPGs without endpoints but configured with static VLANs.   
Decide owners and possibly change the deployment model from Immediate to On-Demand for empty EPGs.

Review and potentially revise these deployments' default settings (manual vs automated).

## Communication Plan

To Management:   
Recommend decommissioning unused EPGs to streamline the network and mitigate risks.   
Long-term solution – redesign some workloads   
Optimize design by configurating on demand vlan provisioning as a standard deployment model  
Upgrade to a software with higher MCP scalability numbers

To Cisco:   
**Express concerns about waiting for the 6.0 release and seek their input or recommendations**.

## R&D and Infrastructure

## Architecture Redesign:

Task R&D (Platform) with redesigning the architecture. Niels, as the owner of the P&T segment, plays a critical role here.

Address pending changes from P&T R&D and software, focusing on dedicated infrastructure elements **like HP and Blades Server C3600.**

# Risk Management: Address pending changes by either accepting the risk for some workloads.

Prepare for largest scenarios like restarting the leaf.

Tackle issues related to tagged 256 interfaces that transcend broadcast domains, requiring impactful mitigation strategies.

## Risk Acceptance:

Acknowledge and accept the risk of MCP faults and warnings until an upgrade to a more capable software version is possible.  
Including that customer requests are implemented with the RISK that switches may restart, however the problem existed on that the software before upgrade was not monitoring MCP utilization.

## Conclusion

We will work on the short-term effort and there is already a demand raised via change management to change the VLAN deployment model to ON DEMAND  
David, PO will engage cross team efforts in a BID to explore the redesign, decommissioning (LCM) or pruning unused trunks.  
We have also discussed other design optimization we will present to compute teams (like VMM domains to control VLAN ranges automatically)   
Future scenario is software upgrades but we belief that the underlying issues need to be tackled and solved