State Of Data Center Network Operations Report

Most common issues plaguing customer fabrics

Statistics below show the top five categories of issues found in customer fabrics.



The study found majority of customers struggle to correctly configure logical routers

Fabric external connectivity



as per the controller's policy model. Top 3 issues found in customer fabrics

at the fabric boundary (L3Out in ACI parlance). The likely reason is non-uniform SDN

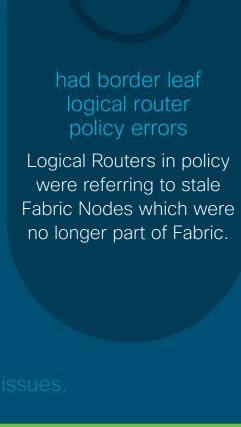
experience across the networking team with all the necessary configurations required

18%





misconfiguration.



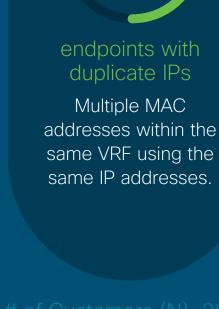
IP and routing management issues

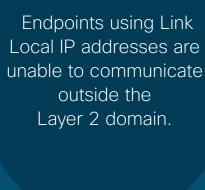
Customers vary in their sophistication using IP address and routing management solutions. A comprehensive and continuous verification across configuration dynamic state is critical to ensure consistency of IP address allocation across end-points and subnets.



54%

Top 4 issues found in customer fabrics

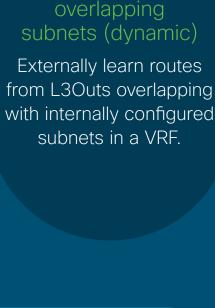




DHCP failure



overlapping

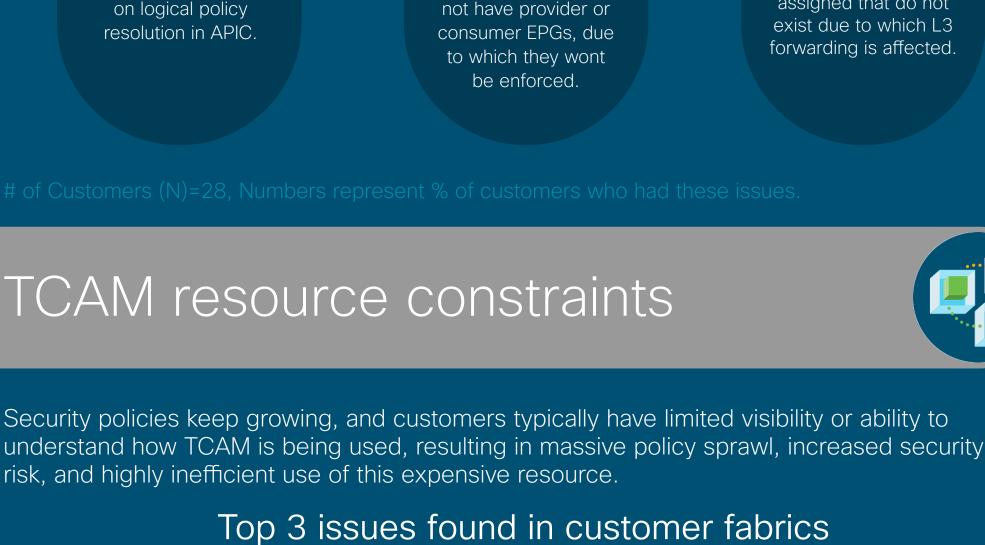


Drift is a reality in every software platform and pervasive across all customer fabrics analyzed in this study. A proactive approach to minimizing configuration drift and policy sprawl is critical

to managing risk in modern software driven networks.

Stale configuration and policy drift

Top 3 issues found in customer fabrics

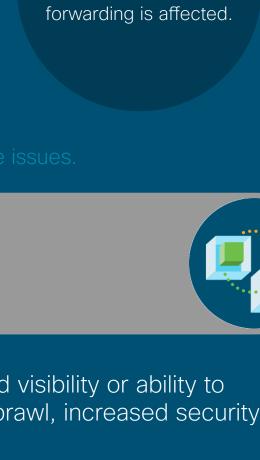


Application EPG did

not get deployed based



Existing contracts do



BDs do not have a VRF

configured, or have VRFs

assigned that do not

exist due to which L3



had contracts with

scope mismatch

Incorrectly defined

contracts where the

Provider or Consumer

EPGs specified do not

fall within the defined

contract scope.

had highly imbalanced

TCAM utilization

Over a third of customers

had huge min-max range

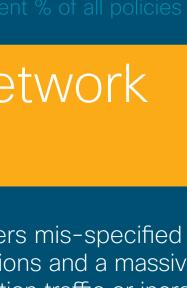
(> 50%) of TCAM utilization

across fabric leaf switches.

A few hot spots can create

deployment issues

in the fabric.



unused

TCAM policies

Across all customers

analyzed, on average,

67% of policies were

unused (zero hit count),

indicating significant room for TCAM

optimization.



had inconsistent VRF

enforcement policies

Application or external

EPG is attached to a

contract but the VRF

is not in enforced

mode, resulting in open communication

had shadow policies

These customers had 2-8% permit policies

that were shadowed

representing latent

security risk

The study found almost 1 of 2 customers mis-specified security policies in the network. With multiple security policy configurations and a massive security policy set, security intent is often broken either denying expected application traffic or increasing the risk of a potential security breach. Top 3 issues found in customer fabrics

29%

had shadowed

permit policies

Duplicate intent with

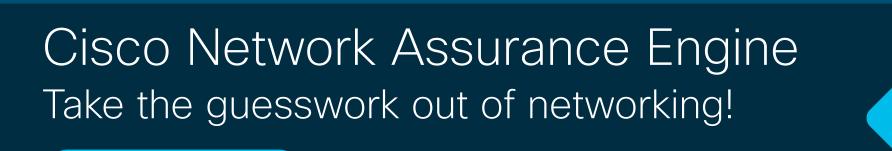
multiple aliased permit

policies between the

same EPGs, increasing

security risk.

inconsistent with intent.



Predict

the impact

of changes.

Request Demo



Assure network

security policy

and compliance.

Make Data Center Network Operations

Proactively verify

network-wide

behavior.

fundamentally more proactive. Watch Video: The Power to Predict