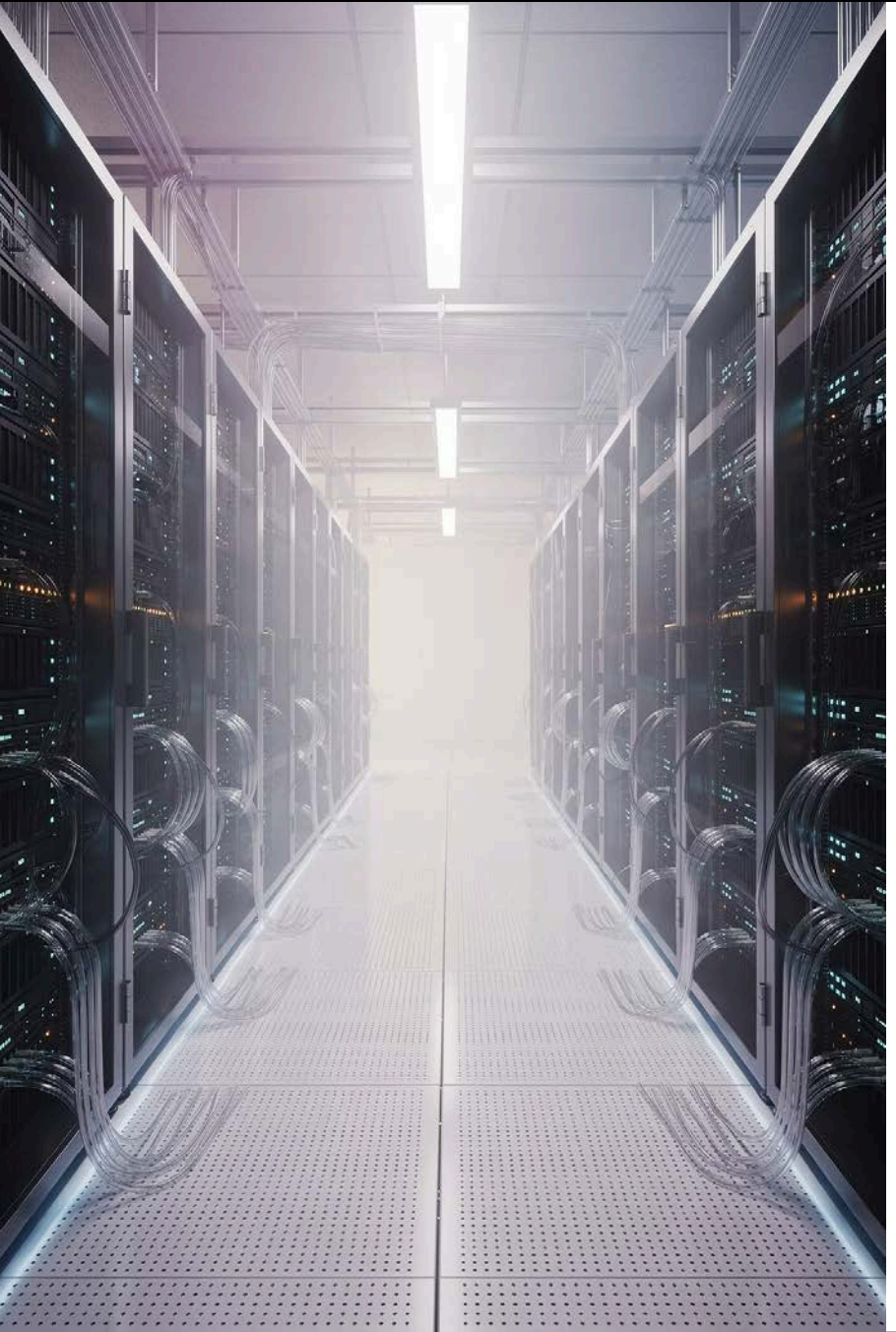


Infrastructure as Code for Enterprise Networks: Automating SD-WAN and Zero Trust

By : Imran Abdul Majeed Qadri
Pace University, New York
Conf42 DevOps 2025

AGENDA

Today's Journey

01

The Network Infrastructure Challenge

Why traditional approaches fail at scale

02

Infrastructure as Code Principles

Applying DevOps methodology to networks

03

SD-WAN Automation

Cisco Viptela and declarative configurations

04

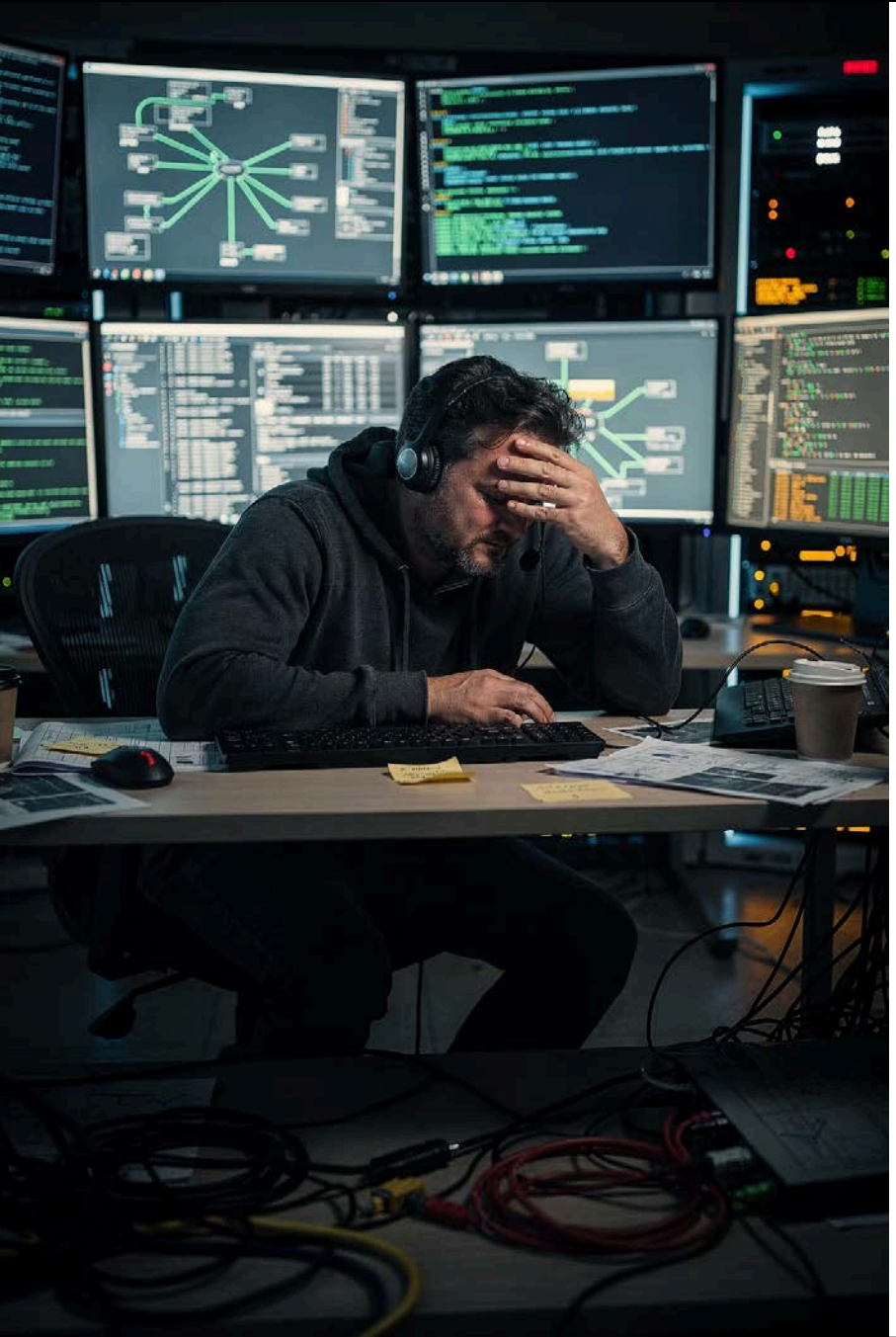
Zero Trust Architecture

Microsegmentation and policy enforcement

05

Practical Implementation

GitOps workflows and continuous validation



The Network Infrastructure Problem

Traditional Approach

- Manual CLI configuration across devices
- Configuration drift and inconsistencies
- Slow change deployment cycles
- Limited rollback capabilities
- Operational silos between teams

Modern Requirements

- Rapid deployment at enterprise scale
- Version-controlled policy management
- Automated compliance validation
- Integrated security architectures
- Cloud-native hybrid connectivity

Infrastructure as Code for Networks

Treating network configuration with the same rigor as application code enables consistency, scalability, and reliability across distributed environments.

Declarative Configuration

Define desired network state rather than procedural commands

Version Control

Git-based workflows for all network policy changes

Automated Validation

Pre-deployment testing and compliance checking

Continuous Deployment

CI/CD pipelines for network infrastructure changes

SD-WAN

Cisco Viptela SD-WAN Architecture

vManage Controller

Centralized management plane for policy orchestration and configuration distribution

vSmart Controller

Control plane providing routing policy enforcement and overlay management protocol

vEdge Routers

Data plane devices at branch and campus locations executing policies

Declarative Network Configuration

Moving from imperative CLI commands to declarative templates enables automated, repeatable deployments across thousands of network devices.

Define Templates

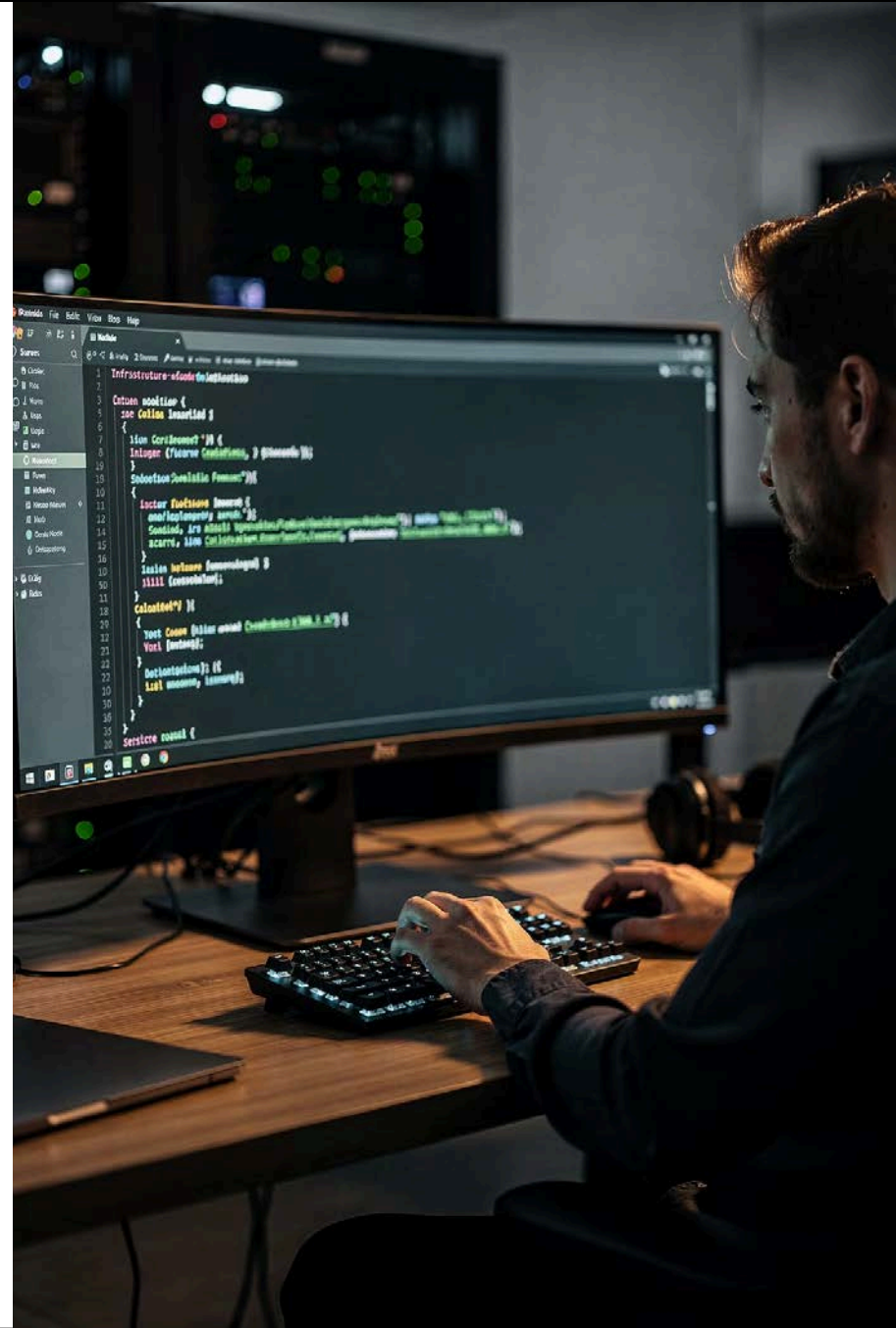
Create reusable configuration templates with variables for device-specific parameters

Store in Git

Version control all network policies and templates with change tracking

Automated Deployment

CI/CD pipeline validates and deploys configurations to target devices



GitOps Workflow Implementation

1

Pull Request

Network engineer submits configuration change via Git PR

2

Automated Testing

Syntax validation, policy compliance, and simulation testing

3

Peer Review

Senior engineers review changes and approve deployment

4

Staged Rollout

Canary deployment to test sites before full production

5

Production Deploy

Automated deployment with continuous monitoring

ZERO TRUST

Zero Trust Network Architecture

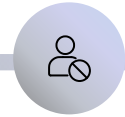
Zero trust principles eliminate implicit trust, requiring continuous verification and microsegmentation to protect critical infrastructure.

Verify Explicitly

Authenticate and authorize every connection request

Least Privilege Access

Grant minimum required network access for each workload



Assume Breach

Design security controls assuming attacker presence

Microsegmentation Strategy

Programmatic enforcement of network boundaries creates isolated security zones with granular policy control, preventing lateral movement during security incidents.

SCADA Isolation

Critical infrastructure traffic completely isolated from corporate networks

Application Segmentation

Database tiers separated from application and presentation layers

User Context

Dynamic policy enforcement based on user identity and device posture

Traffic Prioritization

Policy-based QoS for business-critical applications

Routing Protocol Automation

Multi-Protocol Environments

Enterprise networks often run multiple routing protocols across different domains. Automation ensures consistent policy enforcement regardless of underlying protocol.

- BGP for internet edge and service provider connections
- EIGRP for campus and branch routing
- OSPF for data center fabric routing

Automated protocol optimization adjusts routing metrics, redistribution policies, and path selection based on real-time network telemetry.

Cisco ACI Fabric Integration

Policy Model

Application-centric policy definition with intent-based automation

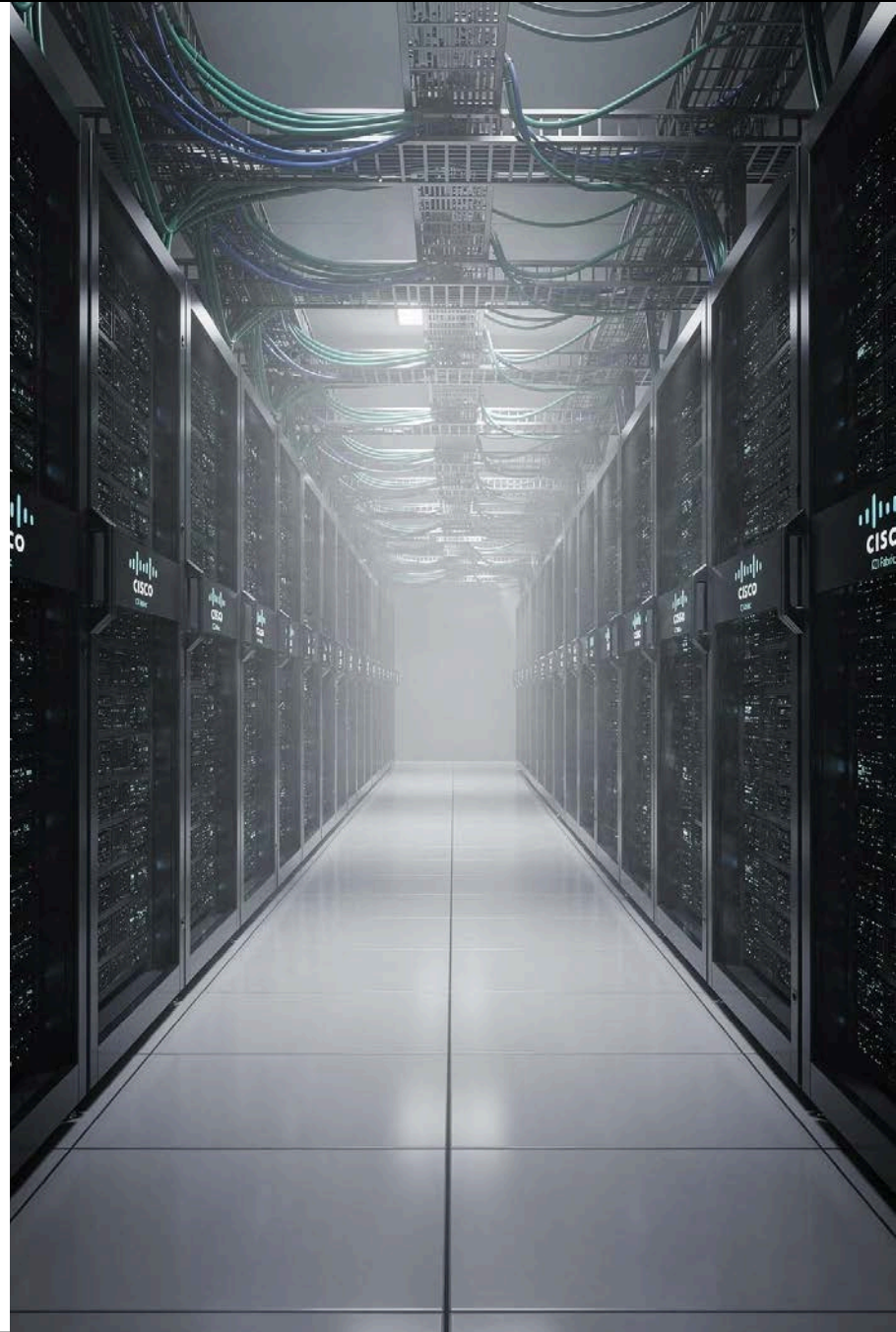
Fabric Architecture

Spine-leaf topology with VXLAN overlay for scalable segmentation

API-Driven

RESTful APIs enable programmatic configuration management

ACI provides declarative policy model for data center networks, integrating seamlessly with SD-WAN for end-to-end automation.



Cloud Integration Architecture

Automated provisioning of secure hybrid cloud connectivity ensures consistent security policy enforcement across on-premises and cloud environments.

AWS Integration

Automated VPN and Direct Connect provisioning with Transit Gateway integration

Azure Connectivity

ExpressRoute and Virtual WAN automation with hub-spoke topologies

Policy Consistency

Unified security policy across cloud and on-premises infrastructure

Monitoring and Observability

Real-Time Telemetry

Centralized collection of network metrics enables proactive incident detection and automated response workflows.

- Interface utilization and error rates
- Application performance metrics
- Security event correlation
- Policy compliance validation

Integration with observability platforms provides end-to-end visibility from application layer to physical infrastructure.

Key Takeaways for Implementation

1

Start with Version Control

Migrate existing network configurations into Git repositories as the foundation for automation

2

Build Validation Framework

Implement pre-deployment testing including syntax checking, policy compliance, and simulation

3

Adopt Gradual Rollout

Use canary deployments and staged rollouts to minimize risk during policy changes

4

Integrate Observability Early

Deploy comprehensive monitoring before automation to establish baseline metrics

5

Automate Rollback Procedures

Ensure automated rollback capabilities for rapid recovery from failed deployments

Thank You!

Questions & Discussion.?

Imran Abdul Majeed Qadri
Pace University, New York
Conf42 DevOps 2025.