KEYSIGHT

Dynamic cyber range solution

Architectural challenges and solutions

Bogdan Stefan, DevSecOps Software Architect
Razvan Chitu aka CRC, DevOps Engineer

KEYSIGHT

Virtualized performance

Challenges

#1 High multi-tenancy count

Actual requirement: having a large number of tenants (>100) each emulating a real network and host environment, running at the same time (x5 – x7 VMs/tenant)

1. Isolate each tenant infrastructure while preserving outside access
2. Smart management of cluster resources (keep each tenant infrastructure consistent and grouped)
3. Storage subsystem bottlenecks

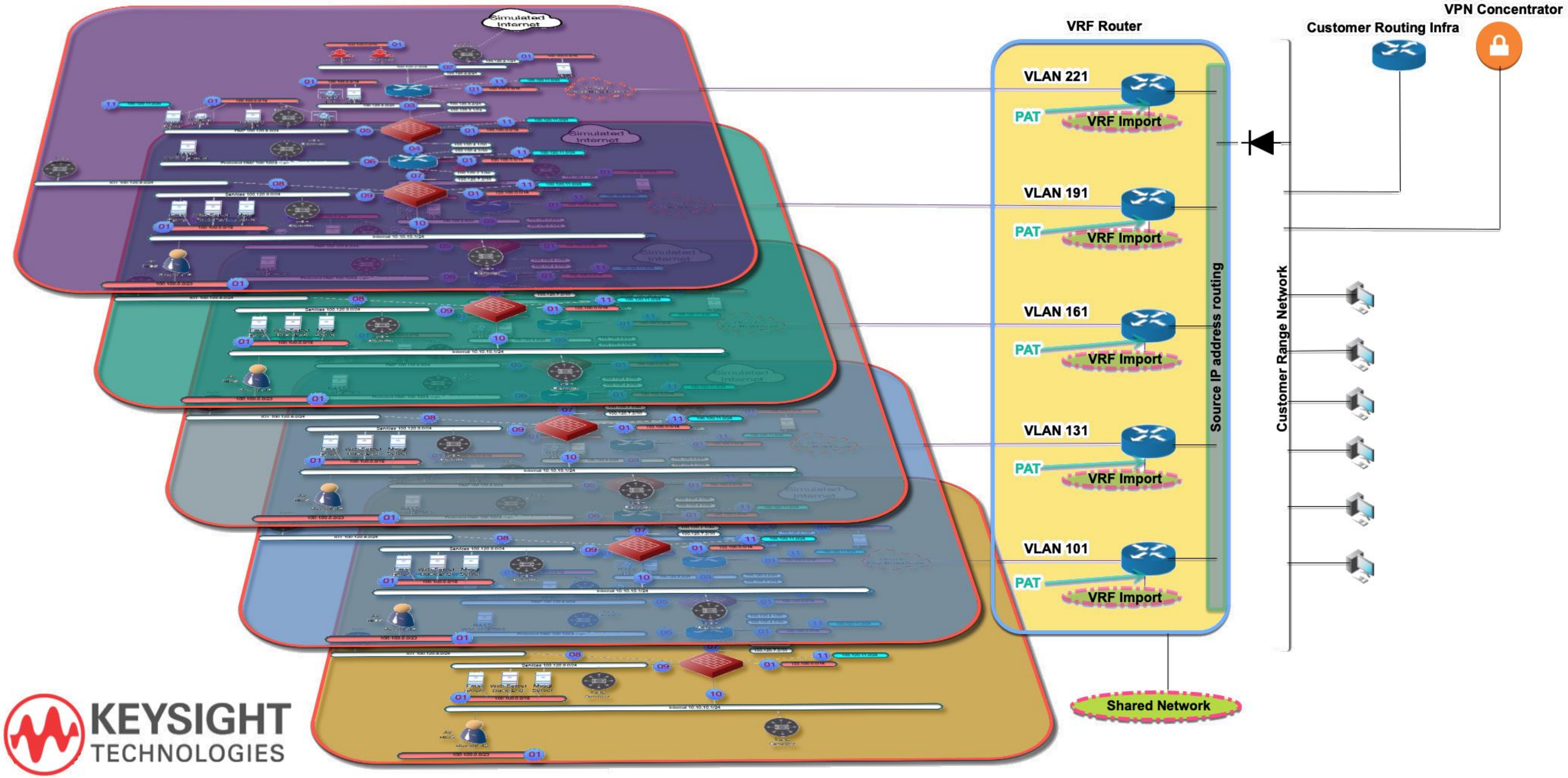
Solutions

#1 I. Tenant isolation

Isolate each tenant infrastructure while preserving outside access

- Using a high performance VRF instance
- REST API integration between the cyber range and VRF service
- Automatic firewall rules on login
- In-place upgrades
- VLAN separation between tenant subnets on the hypervisor side
- Trunk ports between cluster nodes

High level overview



Solutions

#1 II. Smart resource management

Smart management of cluster resources

- Proprietary code for tenant deployment inside a unique hardware resource (cluster node)
- Custom algorithm to account for RAM and vCPU provisioning (including vCPU oversubscription)

KEYSIGHT

Solutions

#1 III. Shared and custom storage

Storage subsystem bottlenecks

- Choosing shared storage
- Linked cloning vs full cloning
- ZFSoNFS vs ZFSoiSCSI vs CephFS
- Custom distributed storage solution

KEYSIGHT

Concurrency and timing

Challenges

#2 Highly dynamic setup changes

Actual requirement: cloning, starting, stopping and destroying hundreds of VMs in dozens of networks simultaneously

1. Hypervisor access concurrency issues
2. Storage subsystem locks
3. Disaster mitigation and recovery

Solutions

#2 I. Task prioritization

Hypervisor and storage concurrency

- Infrastructure task prioritization for optimum resource usage (e.g. higher priority for teardown as opposed to setup)
- Self-adjusting idle timer based on user concurrency for better task scheduling
- NFS task scheduling to prevent locks

Solutions

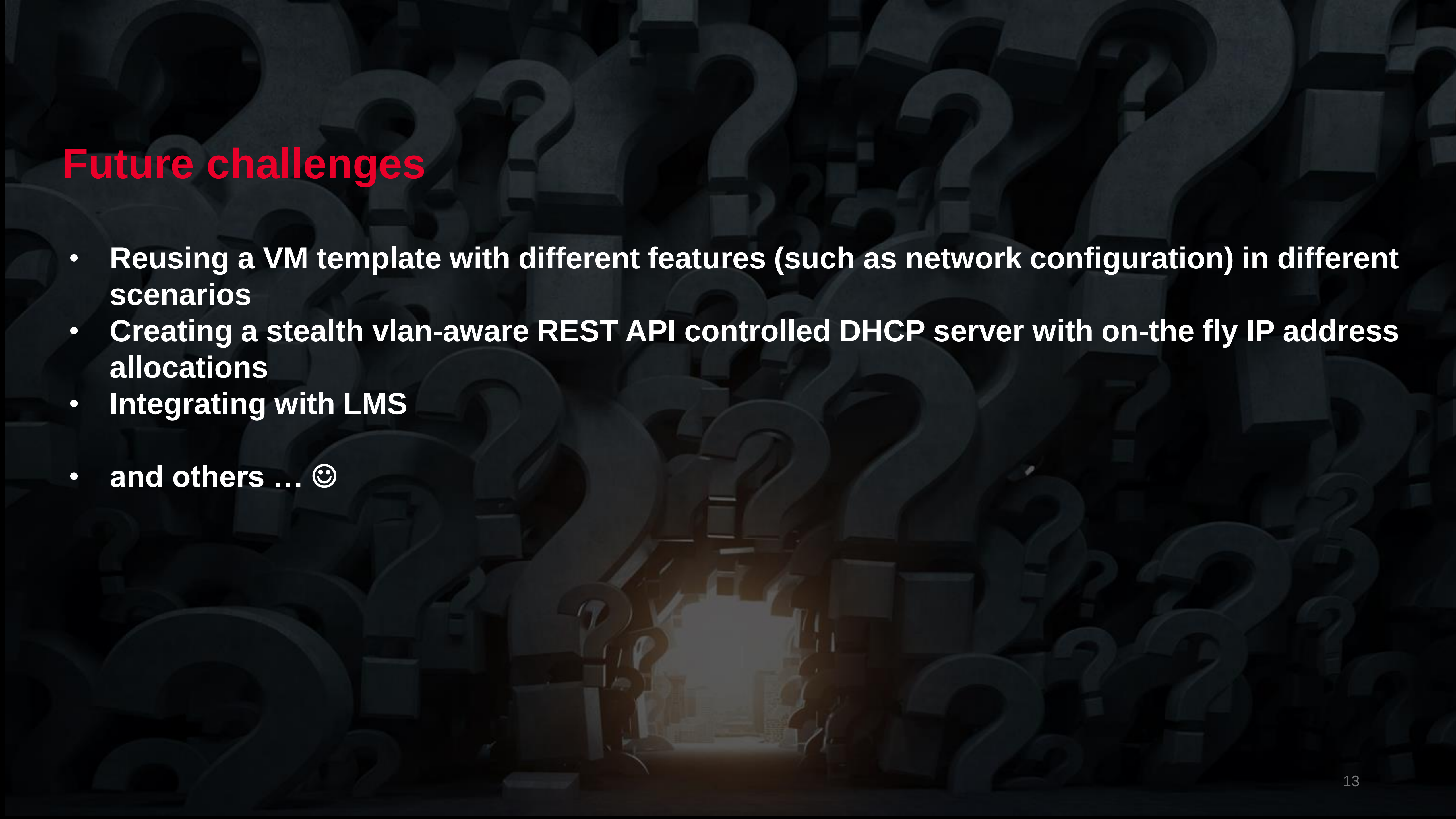
#2 II. Disaster scenarios

Disaster mitigation and recovery

- Depending on the underlying storage subsystem, a tenant environment might be recoverable or completely lost
- For shared storage, manual recovery by the range administrators is possible
- Cluster resources monitored at all times from within the cyber range solution

THIS IS FINE.
I'M OKAY WITH THE EVENTS THAT ARE UNFOLDING CURRENTLY.
THAT'S OKAY, THINGS ARE GOING TO BE OKAY.

Future challenges



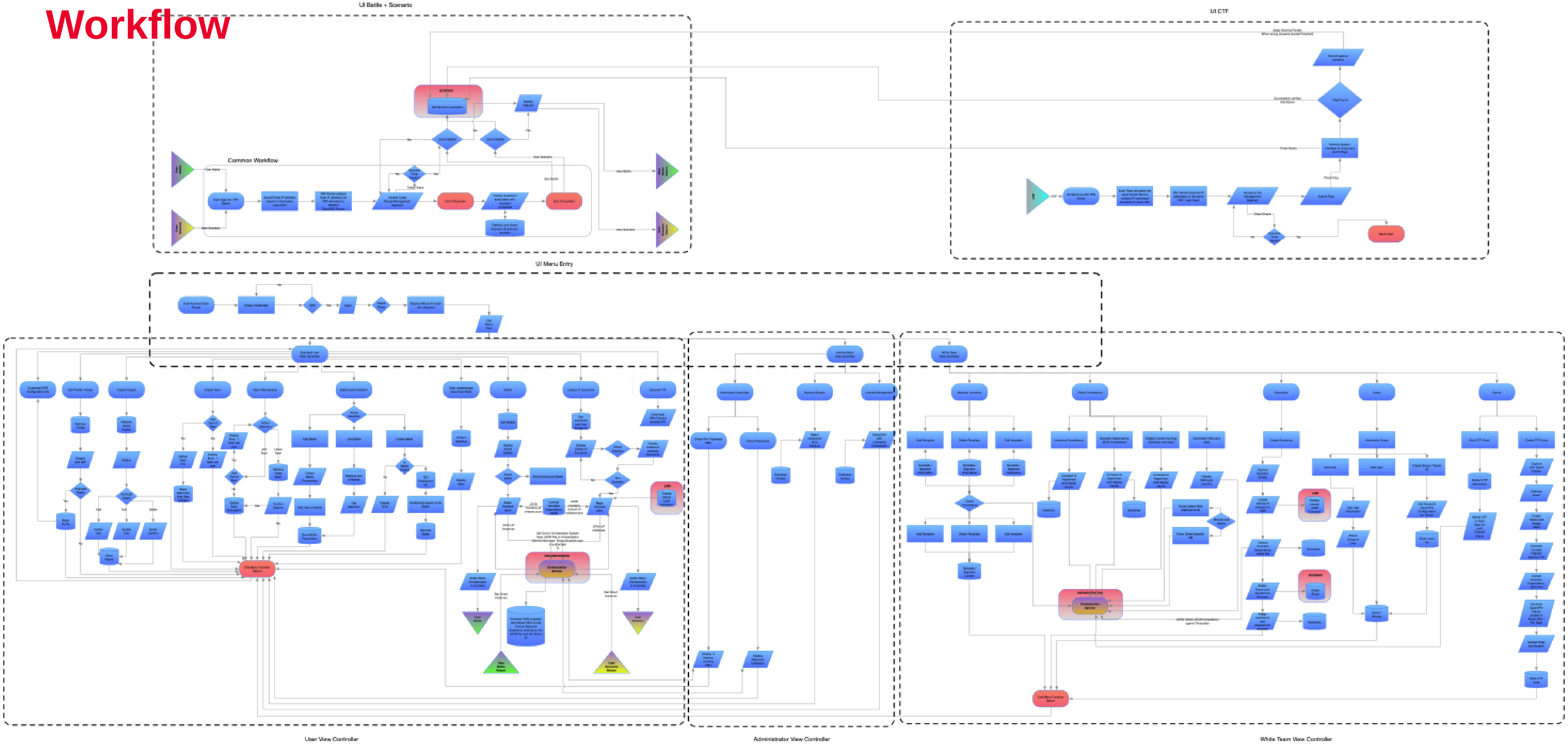
Future challenges

- Reusing a VM template with different features (such as network configuration) in different scenarios
- Creating a stealth vlan-aware REST API controlled DHCP server with on-the fly IP address allocations
- Integrating with LMS

- and others … ☺

Q&A

Workflow



KEYSIGHT