Evolving CERN’s Network Configuration Management System

Stefan Nicolae Stancu¹ (stefan.stancu@cern.ch), Arkadiy Shevrikuko¹, David Gutierrez Rueda¹  
² CERN, Geneva, Switzerland

CERN networks’ overview

The CERN IT Communication Systems group provides wired and wireless communication services across the laboratory. In particular, the group designs, installs and manages a large set of IP networks, comprising approximately 400 routers and 4,000 switches from multiple vendors and different generations, with heterogeneous configurations.

Current network configuration solution

To ensure a consistent reproducible configuration across all these devices, a Perl based in-house software package, cfmgr, has been developed and augmented over the past 20 years.

Based on a central network database (which stores the network model information for all connected devices at CERN), cfmgr is able to derive and enforce the desired configuration on all our network devices.

Network automation ecosystem

The demand for increased agility in network provisioning has led to an active network configuration ecosystem with contributions from both network vendors and the open-source community.

A network automation stack comprises multiple layers:
• Orchestration: trigger the action of reconfiguring network devices;
• Model: device independent network configuration data;
• Driver and device interface: translate the model to the appropriate device specific format and enforce it on the device.

Various orchestration tools can handle network automation:
• Ansible: derive initial configuration
• SaltStack: enforce desired configuration and extract parameters from devices
• StackStorm: event driven IFTTT (if-this-then-that) platform

The generation of the network configuration is specific to each environment.
• At CERN we rely on LANDB for deriving the network configuration.

Configuration models are typically vendor specific.
• Part of the configuration space is covered by OpenConfig or IETF models

Evolved network configuration system

Our evolved network configuration management platform will consist of modular components that can be changed independently and will exploit open-source libraries for:
• the generation of an abstract network device configuration;
• the translation of the abstract model to a device specific configuration, and
• enforcing the configuration on the network devices.

The decoupling of the configuration generation from the configuration enforcement is key for being able to gradually evolve the cfmgr network configuration system whilst keeping it functional and backwards compatible.