



Router/CPE Testing

Zero-touch automated router/CPE testing for Telecom Operators:

Lab-based CPE verification, provision validation, firmware lifecycle automation

[Challenge](#) | [Solution](#) | [How it works](#) | [Platform capabilities](#) | [5 steps](#) | [Glossary](#)

Can Davutoglu, January 2026





The QiTASC promise

**We ensure your router works flawlessly –
every time, everywhere.**



Challenges

Device complexity

Diverse hardware platforms, firmware, and inconsistent: TR-069, UI, ssh, API, SNMP parameters expand the test matrix and break automation.

Performance variability

Lab testing often misses unpredictable performance caused by real-world network conditions and mesh behavior.

Operational scale

Zero-touch provisioning, inventory control, and fleet-wide upgrades are difficult to validate reliably at scale and across vendors.

Interoperability & security

In end-to-end testing, network integration, continuous security updates, and scalable automation remain difficult.

Solution



Zero-touch automation

Autonomous, zero-touch provisioning allows scalable, repeatable testing across deployment, upgrades, and lifecycle operations.

Constant validation

Intent-based, continuous testing validates reliability, performance, and user experience under deterministic and real-world conditions.

Test abstraction

Protocol and router layers normalize vendor differences for consistent testing across hardware, firmware, and management interfaces.

Actionable insights

Automated diagnostics, negative-path validation, and KPI-driven reporting transform test results into clear, actionable outcomes.



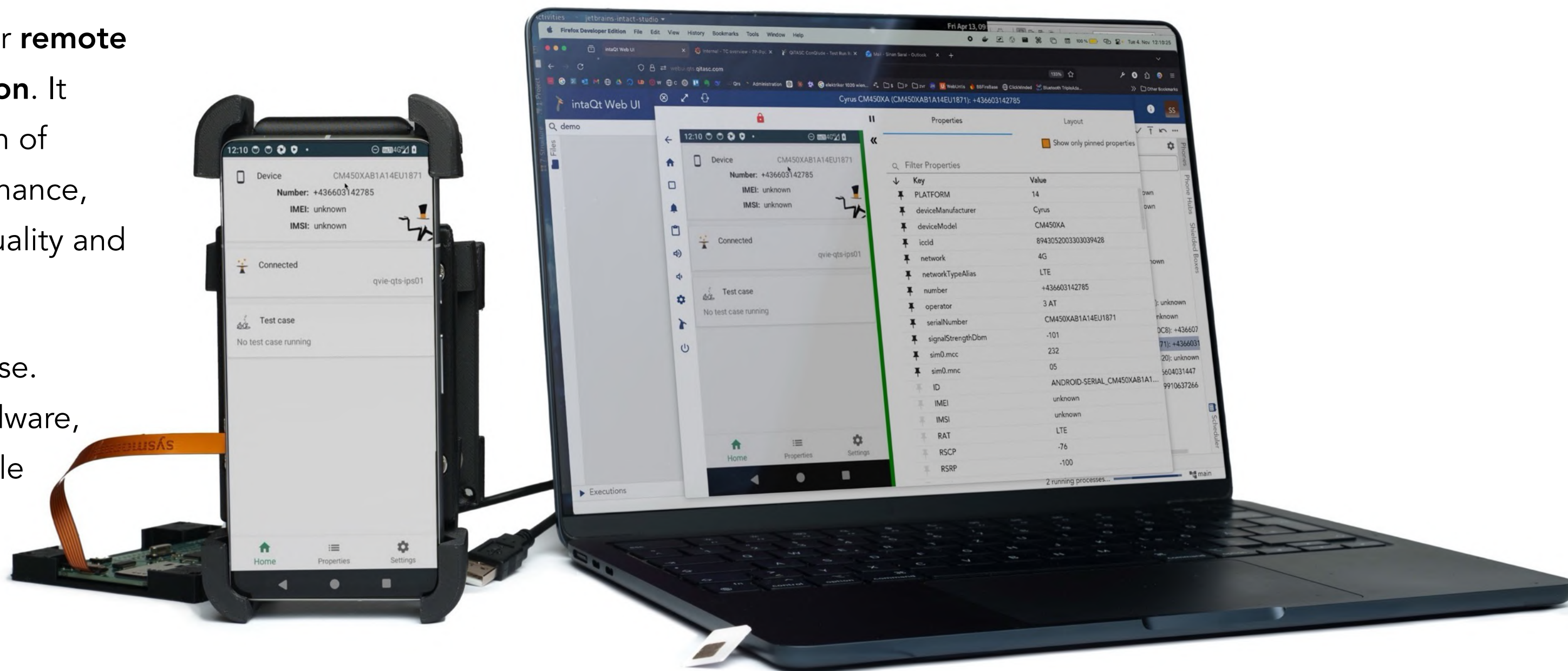
Solution

We test routers automatically

We are **QiTASC**, a successful IT-company located in Austria. We offer a tool that ensures operational reliability for routers across diverse brands and telecom environments.

We offer the technology for **remote end-to-end test automation**. It ensures seamless validation of router connectivity, performance, user experience, service quality and operation experience.

The framework is easy to use. It consists of software, hardware, AI and a remotely accessible lab solutions.





**Get more than
test execution:
3 reasons why
your router/ CPE
type acceptance
and regressions
will be
successful.**

1

You get a zero-touch, enterprise-ready automation platform that unifies authoring, scheduling, execution, reporting, regression hardening, RBAC, end-to-end traceability, and KPI dashboards.

2

True end-to-end testing is done with real devices and backend/NE integration, using vendor-agnostic connectors (TR-069, SSH, SNMP, Web-UI), open-source extensibility, and automated evidence correlation.

3

Scalable, telco-grade operations with proven acceptance expertise, reusable assets across environments and suppliers, as well as parallel execution for complex multi-service testing.

Main use cases



#	User Story	Key Benefit	Main Challenge
1	Multi-Access Technology (FTTx/DSL/4G/5G)	Eliminate manual reconfiguration across connection types	Are you spending days on physical setup changes for each access type?
2	Multi-Protocol Provisioning (UI/SSH/TR-069/SNMP/PDU)	Verify all provisioning methods work together	How confident are you TR-069 doesn't break SSH access?
3	End-to-End Device Scenario (TV/VoIP/mobile/PC)	Real household traffic patterns, not synthetic loads	Can you monitor 10+ devices simultaneously during manual tests?
4	Advanced WiFi Testing (2.4/5/6 GHz, roaming, steering)	Reproducible WiFi scenarios, eliminate "walk around" testing	Does band steering actually work or just annoy users?
5	Firmware Lifecycle (flash/rollback/migration)	Test scary upgrade paths (version skipping, downgrades)	What happens upgrading from v1.2 directly to v3.5?
6	Service Quality Metrics (VoIP MOS/IPTV/QoE KPIs)	Business-relevant metrics, not abstract packet loss %	Can you prove 2% packet loss ruins VoIP calls?
7	Power Interruption (remote PDU control)	Test power loss during critical operations	Tested power failure at 3.7 seconds into boot?
8	Firmware Failure Recovery (interruption + auto-recovery)	Prevent bricked routers in field deployments	What if 47% of firmware flashes before corruption?
9	Zero-Touch Reprovisioning (factory reset + RAL)	Verify "turn it off and on" actually fixes issues	Do factory resets create working configs or support calls?
10	WAN Impairment Profiles (latency/jitter/packet-loss)	Simulate real ISP network conditions	Your perfect lab ≠ customer reality - tested for that?
11	Backend Correlation (colleQtor integration)	Instant root cause with auto-collected diagnostics	Days to reproduce bugs vs. hours with automated diagnostics?
12	Device Compatibility Matrix (brands/OS/protocols)	Systematic IoT device interoperability testing	Tested with that 2019 Samsung TV? Or waiting for complaints?

Test case combinations

Basic Dimensions

- 3 Router types
- 10 Basic configs (QoS and Routing)
- 6 Access types
- 4 Device types
- 3 Device brands per type
- 3 Firmware versions
- 4 Configuration methods
- 2 Load variants

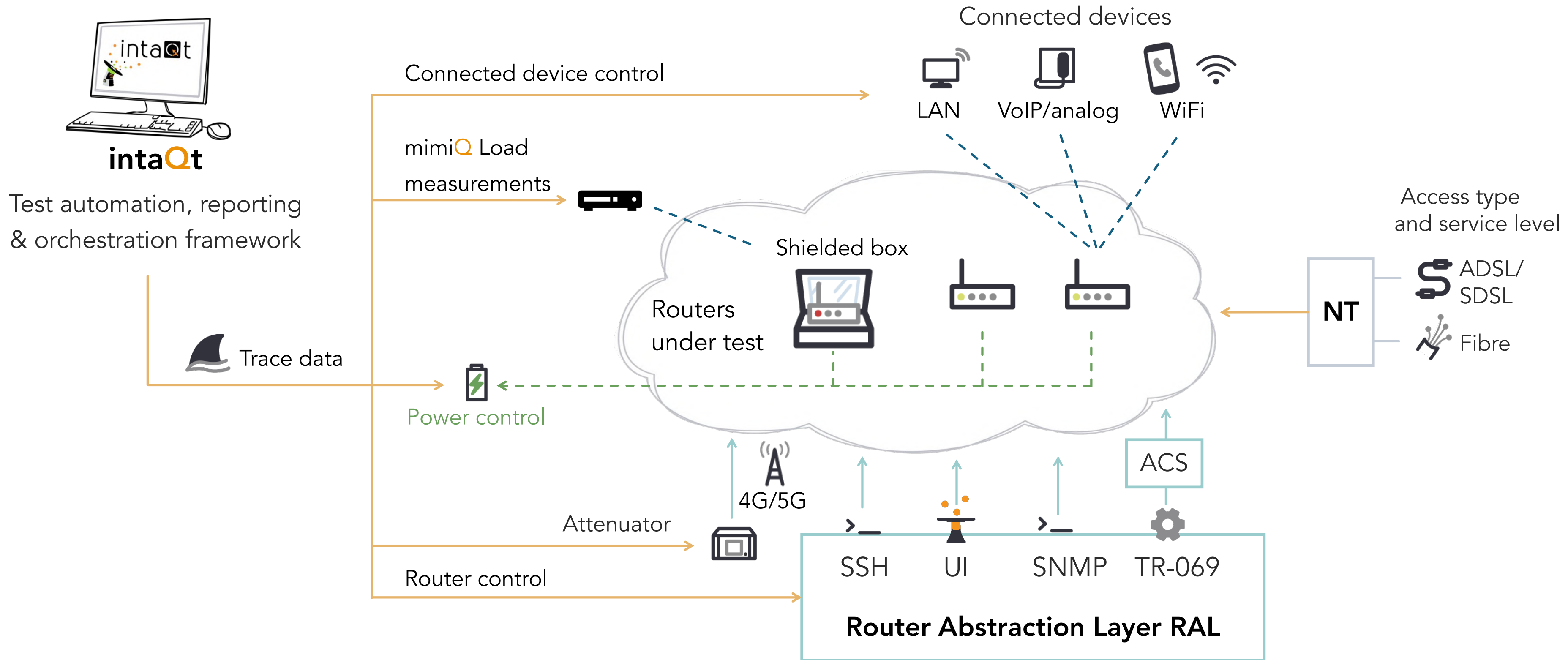
Additional dimensions

- 8 WiFi configurations
- 5 WAN impairment profiles
- 4 Firmware lifecycle scenarios
- 5 Power/Resilience variants
- 3 Service quality levels
- 4 Security/Firewall configs
- 3 VLAN variants
- 3 IPv4/IPv6 options
- 3 Provisioning status
- 2 Time-critical scenarios





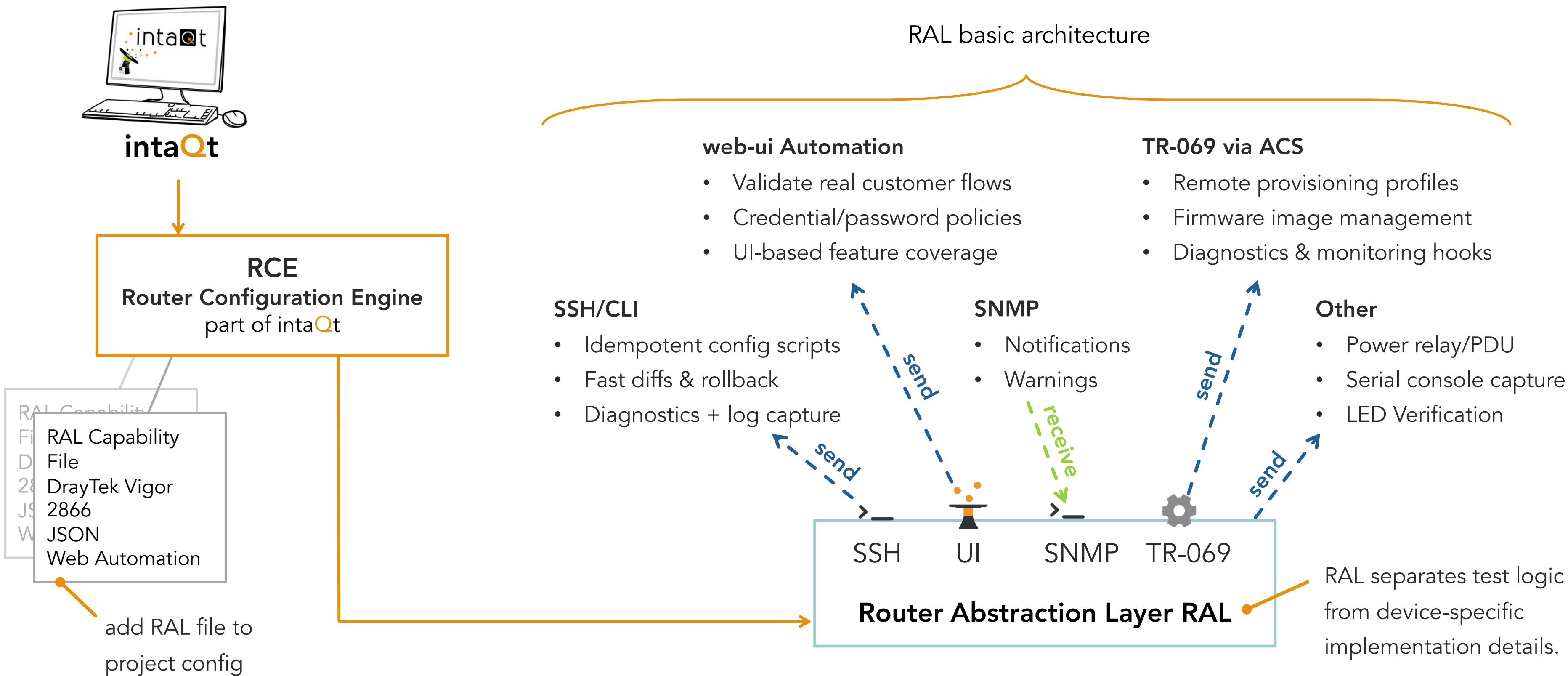
Lab architecture for router testing





How it works

Minimize effort to extend router pool > RAL integration





Test case: Router firmware update & verification with load test

```
1  Given a router as Router-A
2      * with profile FritzBox1
3  And verify if router set-up is singleRouter
4  And verify Router-A is up and running
5  And store software version on Router-A as SWV_before
6      * via ssh
7  And deferred reset Router-A
8  And initiate firmware update for Router-A within 120 seconds
9      * via TR-069
10 And store software version on Router-A as SWV_after
11     * via web-UI
12 And store measurement for Router-A in Measurement_result
13     * profile Basic_load
14     * duration 1 minute
15 Verify SWV_after > SWV_before
16 And verify Measurement_result within boundaries
```

Integration points

- CI pipelines (triggered via intaQt CLI)
- Test case in Gherkin syntax via Cucumber integration in intaQt
- Device selection via profile
- Read version via ssh
- ACS integration
- Test case run and control via intaQt
- Verification via UI
- Traffic load via mimiQ
- Reporting via conQlude -> Jira
- Grafana Dashboards: Success/failure rates, trend KPIs by firmware, model, type, etc.
- Automatic reset via deferred steps

Platform capabilities

A framework that simplifies work

Automation & control

framework: Technician-friendly Gherkin/ Cucumber scripting with ACS and CI integration; test execution, control, traffic, SSH verification, reporting, and profile-based device selection

WAN/access impairment:

Latency, jitter, loss, NAT/IP changes, mobile reattach, DSL retrain/link flaps. 24-72h stability, memory leaks, roaming, band steering, parallel routers

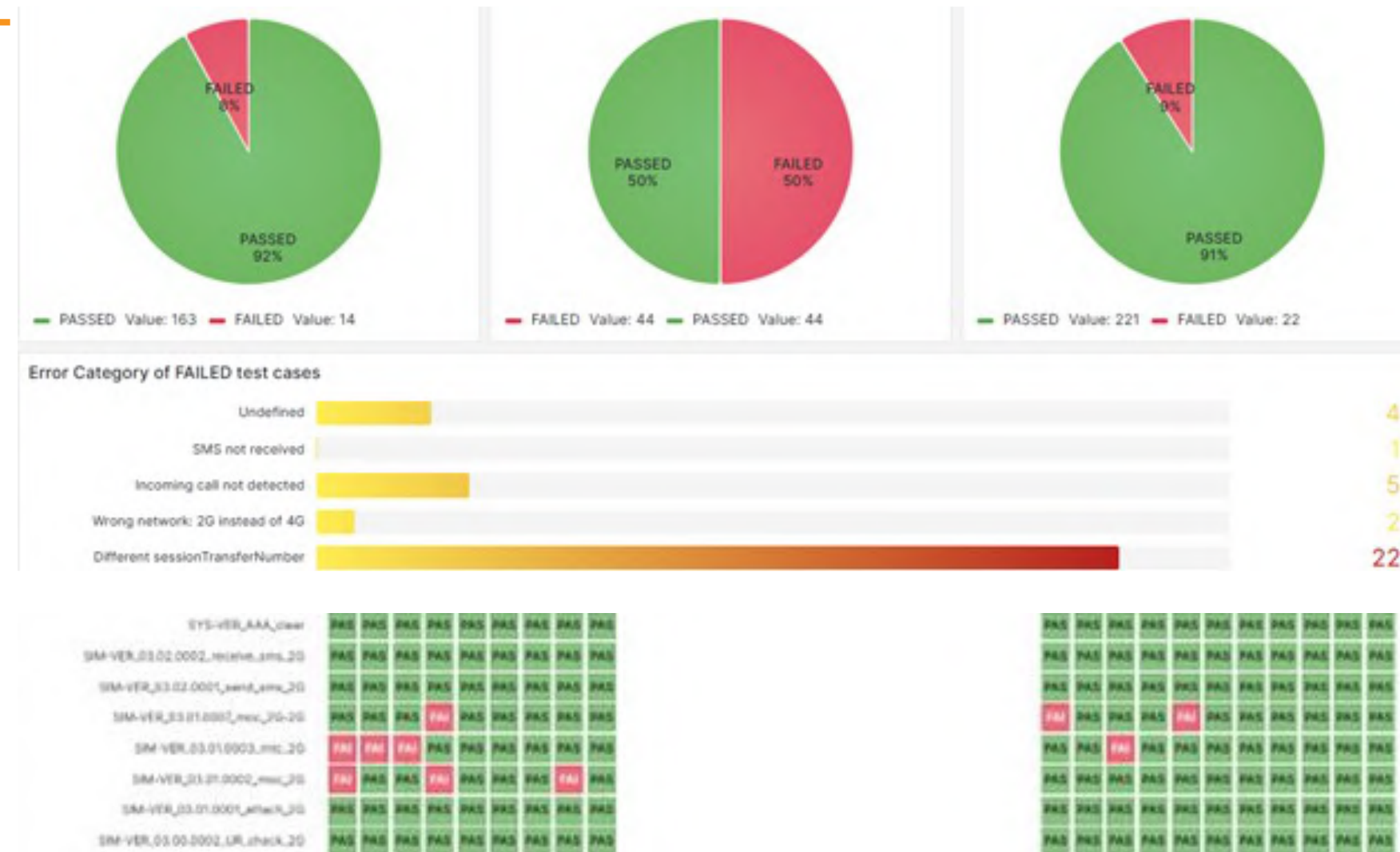
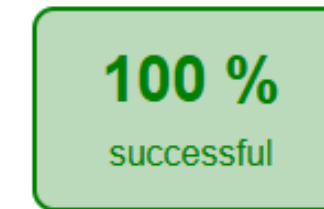
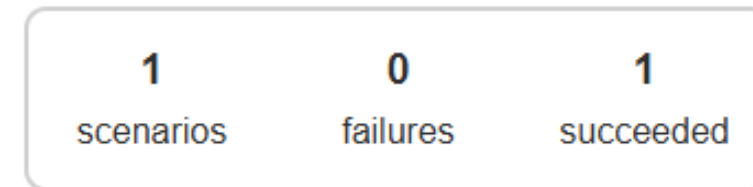
Traffic & QoS: Competing flows, bufferbloat, queues/ DSCP, QoS profiles, shaping/ prioritization. MOS and service KPIs (VoIP/IPTV) under load

Configuration & firmware:

Routing (static/dynamic), VLANs, NAT/firewall, secure Wi-Fi; flash/upgrade/ downgrade, config migration, rollback, recovery

Devices, power control:

Reboot sequencing, PDU/ relay power cycling, LED checks, remote control, functional validation



↖ **Measurement & evidence:** Throughput, latency, jitter, RSSI/ link stats; logs, traces, PCAPs, config diffs, screenshots, false-positive analysis, Grafana KPIs/ trends

Platform Capabilities



Remote control: Control test devices and lab equipment from anywhere.



Monitoring: Real-time test run tracking and false positive analysis



Network element integration: API integration to NE like HLR, AAA, CCS, PCRF, MME, EPG,...



Roaming integration: Real roaming site connections



Multi-tenancy: Isolated environments and devices per project.



Reports & KPIs: Automated reporting and evidence collection.



Test automation: Complete test automation framework.



Simulation: Virtual test environments.



Authoring environment: User roles and authoring profiles.



Result visualization: Interactive charts and trend analysis.



Trace collection: Trace collection (pcap), log, full evidence & audit trails.



Version control: Test case and project versioning and rollback via git.



Security: Enterprise security standards applied to all tools.



AI analysis: Intelligent defect resolution and root cause analysis.



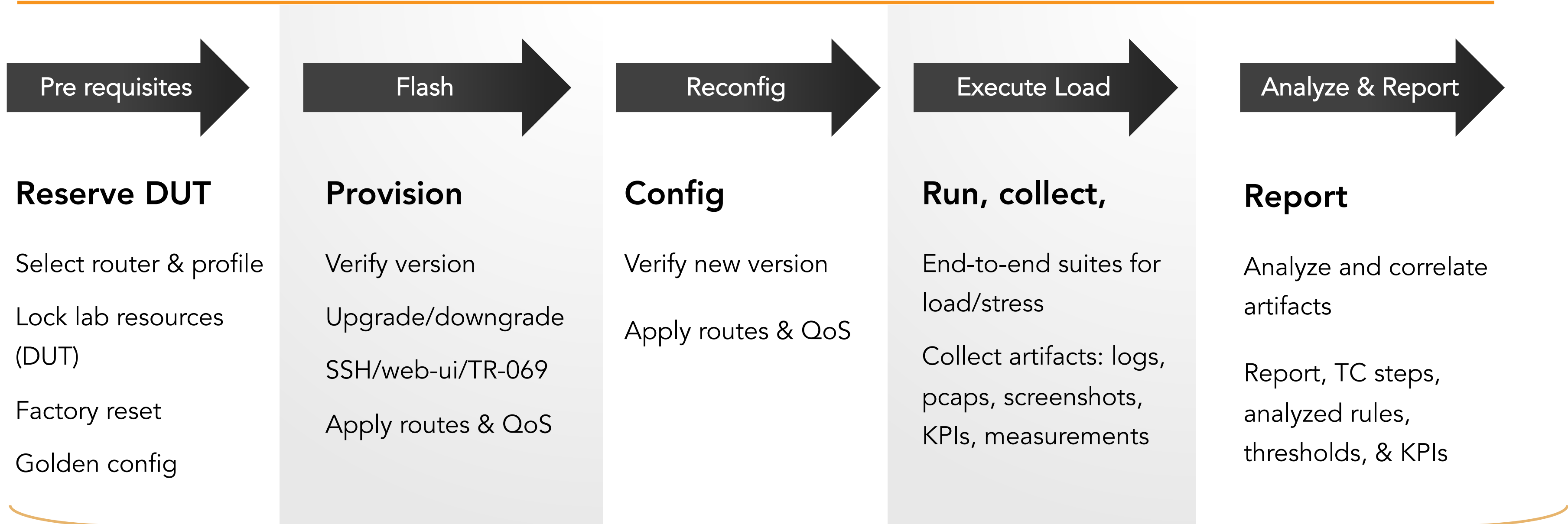
CI/CD integration: Seamless DevOps pipeline integration.



Scalability: Scale from 10 to 10,000+ tests, and 2 to 500 devices.



End-to-end workflow without manual interaction



Outputs per run

Pass/fail result, thresholds (KPIs, service checks), Artifact bundle, KPIs/dashboard statistics.
Reproducible snapshot: router profile, lab topology, Correlation pointers to backend trace: timestamps, IDs.



What now?



Demo

Live at your office or via a video-call. Understand technical details.



Proof of concept

A small project demonstrates our capabilities for your business case.





Get in touch!

Can Davutoglu

Founder & CEO

Mail can.davutoglu@qitasc.com

Web www.qitasc.com

Glossary (A-Z)



4G/5G: Fourth-/fifth-generation mobile access

ACS: Auto Configuration Server

ADSL: Asymmetric Digital Subscriber Line

CI: Continuous Integration

CLI: Command-Line

CPE: Customer Premises

DSCP: Differentiated Services Code

DSL: Digital Subscriber

E2E: End-to-end

FTTx: Fiber-to-the-x (fiber access variants)

GHz: Gigahertz (Wi-Fi bands: 2.4/5/6 GHz)

IP: Internet Protocol

IPTV: IP Television (service validation, KPIs)

KPI: Key Performance Indicator

LAN: Local Area Network

MOS: Mean Opinion Score (voice QoE metric)

NAT: Network Address Translation

PCAP/pcap(s): Packet capture file(s)

PDU: Power Distribution

QoE: Quality of Experience

QoS: Quality of Service

RAL: Router Access Layer

RBAC: Role Based Access Control

RCA: Root Cause Analysis

RCE: Router Configuration Engine

RSSI: Received Signal Strength Indicator

SDSL: Symmetric Digital Subscriber Line

SSID: Service Set Identifier (Wi-Fi network name)

SSH: Secure Shell

TCP: Transmission Control Protocol

TR-069: Broadband Forum CPE WAN management protocol

TWAMP: Two-Way Active Measurement Protocol

VLAN: Virtual LAN

VoIP: Voice over IP

WAN: Wide Area Network

Web-UI: Web-based user interface

Wi-Fi: Wireless LAN

p95: 95th percentile