Building a Secure Test Environment for an IXP

Marta Burocchi - Network Engineer
RIPE90 - Lisbon

Do you know when you make a small change in the production configuration...

...and everything breaks?

*Please note this is a real life Namex picture
- courtesy of Francesco Ferreri / Namex Archives

The Idea

The idea comes from a very practical need

The Idea

The idea comes from a very practical need

Create a **secure**, **live** pre-production environment that mirrors the **real peering LAN**:

To validate members' configurations

To test our services before deploying them to production

The Evolution of The Idea

Namex needs a test environment

The Evolution of The Idea

Namex needs a test environment

The collaboration with Kathara's Team starts

Kathará

The Evolution of The Idea

Namex needs a test environment

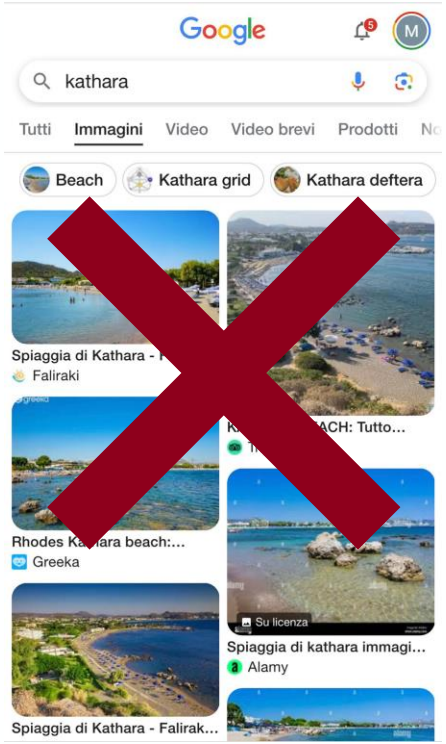
The collaboration with Kathara's Team starts

Kathará

🎀 Namex Digital Twin is born: a faithful replica of the Namex Peering LAN and services 🎀

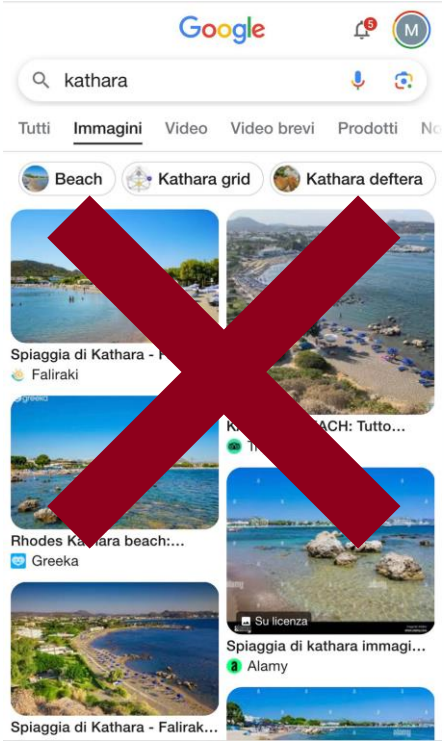
Fun Fact

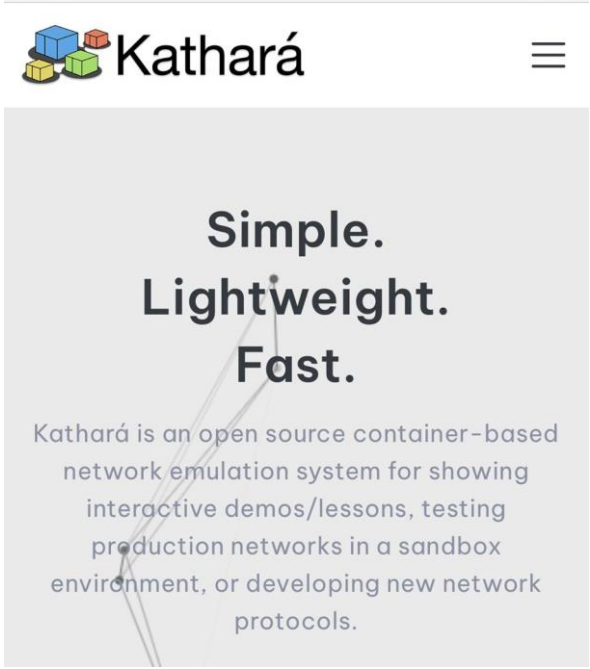
If you google Kathara and you choose “images”…



Fun Fact

If you google Kathara and you choose “images”…





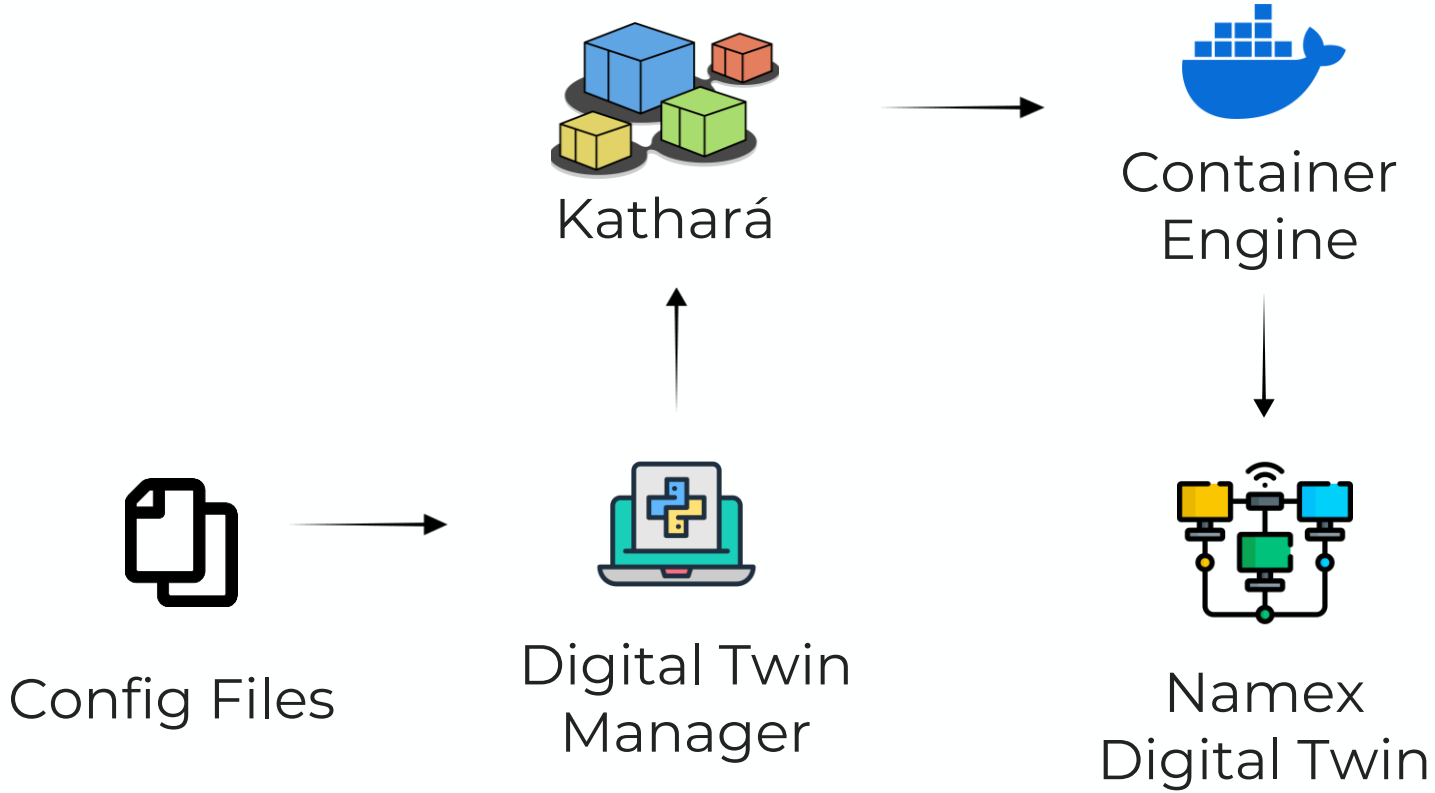
Namex Digital Twin

What? A faithful replica of the Namex Peering LAN with the same members, Route Servers, IP addressing and even MAC addresses

How? Members and Route Servers from the Peering LAN are emulated as dedicated Kathará devices

Where? On a pre-production environment (quarantine VLAN)

The Architecture



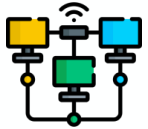
Digital Twin is a Snapshot of the Real LAN

The virtual environment is **synchronized** with the production network, using real-time data

List of all the peers on the Peering LAN

Dumps of the actual Route Servers' RIBs (v4/v6)

Digital Twin Manager
Manages the lifecycle of the Digital Twin

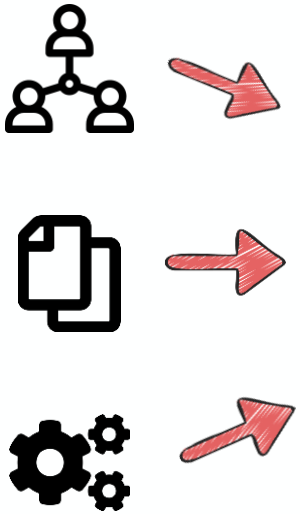


Namex Digital Twin

Real Route Servers' configuration files

Digital Twin is a Snapshot of the Real LAN

The output is a **faithful replica** of the peering LAN



Digital Twin Manager
Manages the lifecycle of the Digital Twin

Namex Digital Twin

One Kathará device for each peer

One Kathará device for each Route Server

The virtual peering LAN

Digital Twin: Use Cases

- New members can connect their router to the quarantine VLAN and **safely test and tune** their BGP setup **without affecting** the production network

- New members can use the Digital Twin to **test their configurations** according to the Route Servers' policies in a **safe sandbox**

- NOC can **validate** Route Servers' configurations changes or new services **before deploying** them to the production environment

Extending the Digital Twin

The Digital Twin can be **extended** to support **more features** and **use cases**:

1. Quarantine Dashboard
2. RPKI Validation
3. ASPA Testing
4. Traffic Generation
5. ROSE-T (MANRS Compliance)

Extending the Digital Twin

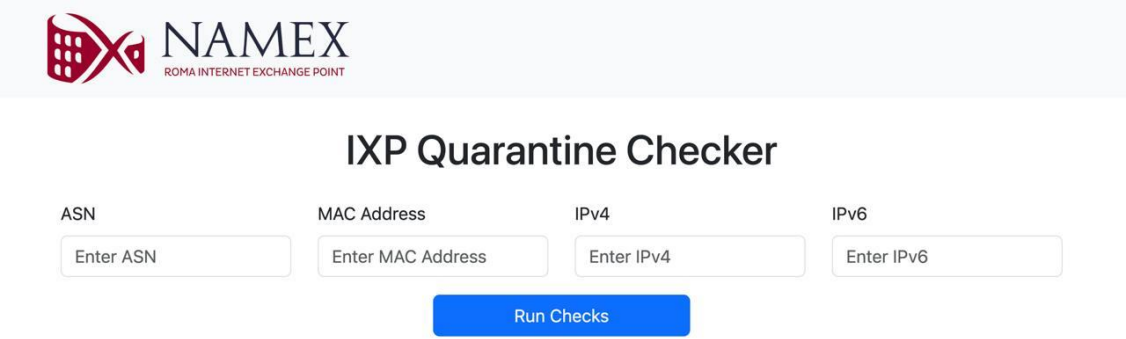
The Digital Twin can be **extended** to support **more features** and **use cases**:

1. **Quarantine Dashboard**
2. RPKI Validation
3. ASPA Testing
4. Traffic Generation
5. ROSE-T (MANRS Compliance)

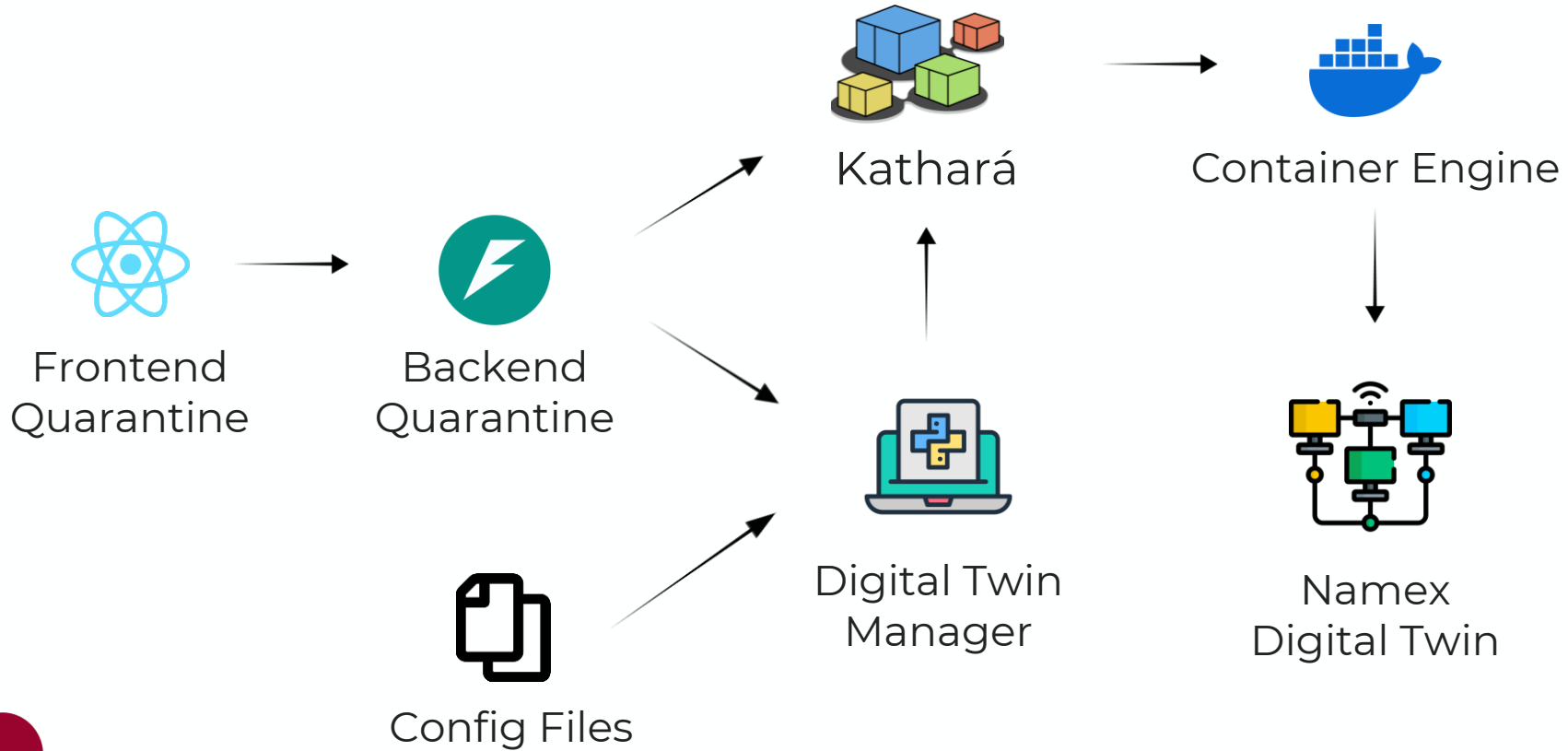
Quarantine Dashboard

New members can **test** their configuration **compliance** to our technical rules

Immediate feedback helps members fixing issues before going into the production network



Quarantine Dashboard Architecture



Checks Performed

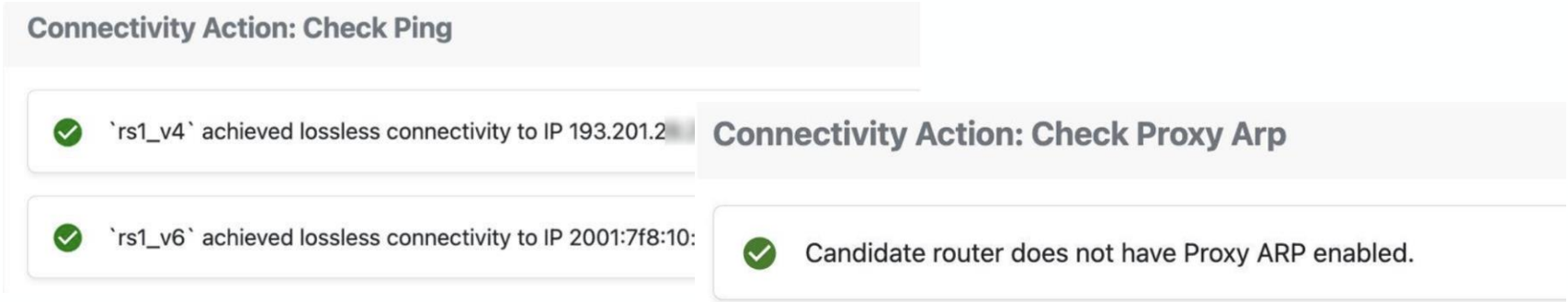
- Connectivity Tests (ping/ping6, MTU, proxy ARP)
- BGP Checks (established sessions, prefix limit check, default route advertisement, private prefix advertisement, next hop validation, AS path consistency, announcement consistency)
- Unauthorized Traffic Detection (neighbour discovery protocols, internal routing protocols, or router advertisements)
- Security Tests (open ports for DNS, NTP, SNMP)

These checks confirm that configurations are correct **when they are performed**

Note that router configurations may change and unwanted traffic needs continuous monitoring

Checks Performed: Connectivity Tests

- **ping/ping6**: Tests basic connectivity using ICMP ping, ensuring that the peer can reach other devices on the network using IPv4/IPv6
- **Proxy ARP**: Verifies that Proxy ARP is disabled on the interface to avoid unwanted routing of packets, ensuring that each peer handles only the traffic intended for them
- **MTU**: Checks the MTU settings to make sure that packet sizes are correctly handled



Checks Performed: BGP Checks

- **Established Sessions**: verify the BGP session between the peer and the Route Server is properly established
- **Prefix Limit Check**: Ensure that the number of prefixes advertised by the peer does not exceed the allowed limit
- **Default Route Advertisement**: Check if the peer is announcing a default route (0.0.0.0/0 for IPv4 or ::/0 for IPv6)
- **Private Prefix Advertisement**: Verify that the peer is not announcing private prefixes that should not be routed through the IXP
- **Next Hop Validation**: Ensure that the next hop of advertised prefixes corresponds to the peer's router IP, as assigned by the IXP
- **AS Path Consistency**: Confirm that the AS-PATH of the prefixes they advertise starts with the ASN of the peer

Checks Performed: Unauthorized Traffic Detection and Security Tests

- **Unauthorized Traffic Detection**: Monitor traffic for 1 minute to detect any unauthorized traffic types such as neighbour discovery protocols, internal routing protocols, or unsolicited router advertisements
- **Security Tests**: are conducted to detect open ports for DNS, NTP, and SNMP

Digital Twin Scalability

Currently emulating:

- ~220 members
- 4 Route Servers (2 for IPv4, 2 for IPv6)
- Hardware specs:
  - Memory: 32GiB
  - Processors: 4 cores

⚙ **Designed to scale** with Namex's growth

For large IXPs, the full network can be deployed using the **distributed emulation feature** supported by Kathará

Conclusions

The Digital Twin provides a **secure and isolated** testing ground to support the development of new services

The **Quarantine Dashboard** provides a sandbox to validate members' compliance with technical rules and services in the onboarding phase

The Dashboard is just **one of many applications** we can imagine:

- RPKI Validation, ASPA Testing, Traffic Generation, ROSE-T, etc.

You can read more about our experience on RIPE Labs

How To Build your Digital Twin?

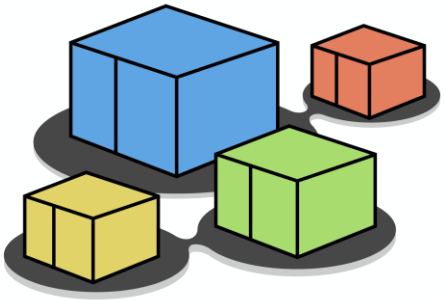
The Kathará IXP Digital Twin is **open source**

You can contact the developers team at contact@kathara.org

VSIX UNIVERSITÀ DEGLI STUDI DI PADOVA is building its Digital Twin too!

...who's next?

Repository



Kathará

What is Kathará?

A container-based network emulator

- Based on Docker containers
- Can run on Kubernetes to scale up the emulation in a cluster

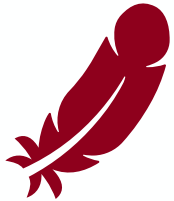
Open-source project born at Roma Tre University

- Over 100K downloads
- 500+ stars

Widely adopted for academic teaching and research

- Used in more than 35 different courses, 25 universities and 14 countries
- Several publications and research framework based on Kathará

Why Kathará?

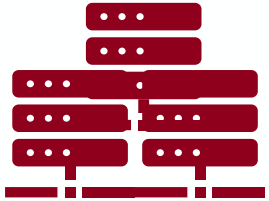


Lightweight

- Minimal resource usage
- Fast startup

Python APIs

- Simple programming interface
- Easy to extend



Scalable

- Docker on single host
- K8s on a cluster

Contacts

Lorenzo Ariemma

lorenzo@kathara.org

Tommaso Caiazzi

tommaso@kathara.org

Mariano Scazzariello

mariano@kathara.org

github.com/KatharaFramework/Kathara

linkedin.com/company/kathara

contact@kathara.org

Website

Kathará Development Association

No-profit organization for maintaining the Kathará Framework ecosystem:

High quality tools for researcher and network developers

- Many publications based on Kathará
- Collaborations with industry for fostering innovation

High quality computer networks education materials

- Many universities choose Kathará

Open-source projects for the networking community

- IXP Digital Twin
- ROSE-T (MANRS Compliance)

More to come!

Support Kathará

Believe in open networking and innovation?

Got ideas or want to collaborate with us?

We'd love to hear from you: contact@kathara.org

Q&A

NAMEX
ROMA INTERNET EXCHANGE POINT