# IP design and exploitation of Geneva city transport network

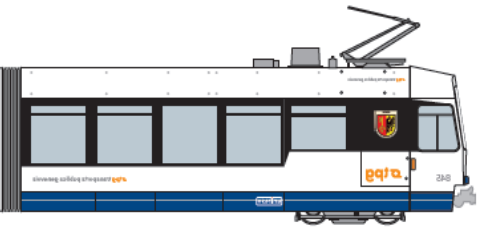
## Unified communication for the TPG fleet

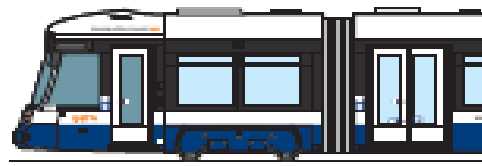
**SIT / Grégoire Huet 14.11.2019**

# About

## Transports Publics Genevois

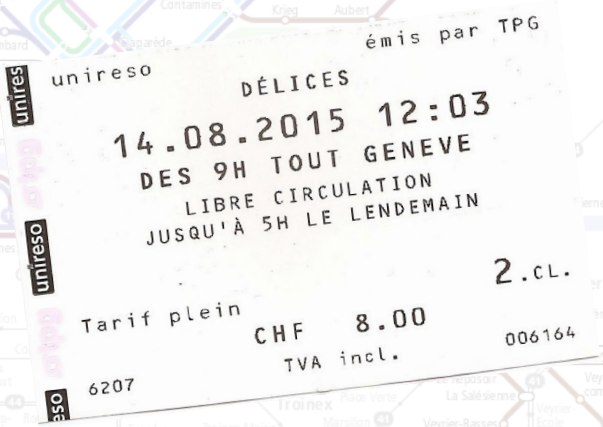
- Created in 1977, from a 1899 company, operations are back to 1833
- ~2000 employees, including ~1350 for exploitation (with drivers)
- ~430 MCHF turnover
- Wholly owned by the *État de Genève*





# Public Transportation Network

- 426 Km of lines (5 x tramway, 6 x trolley, 52 x bus, plus nightly lines)
- 220 millions of rides in 2018 / About 600k rides per day
- 659 vehicles in 2018 = 117 trams, 90 trolleys, 452 autobuses
- Around 30 millions Km per year in total




# The fleet

## A diversity of vehicles



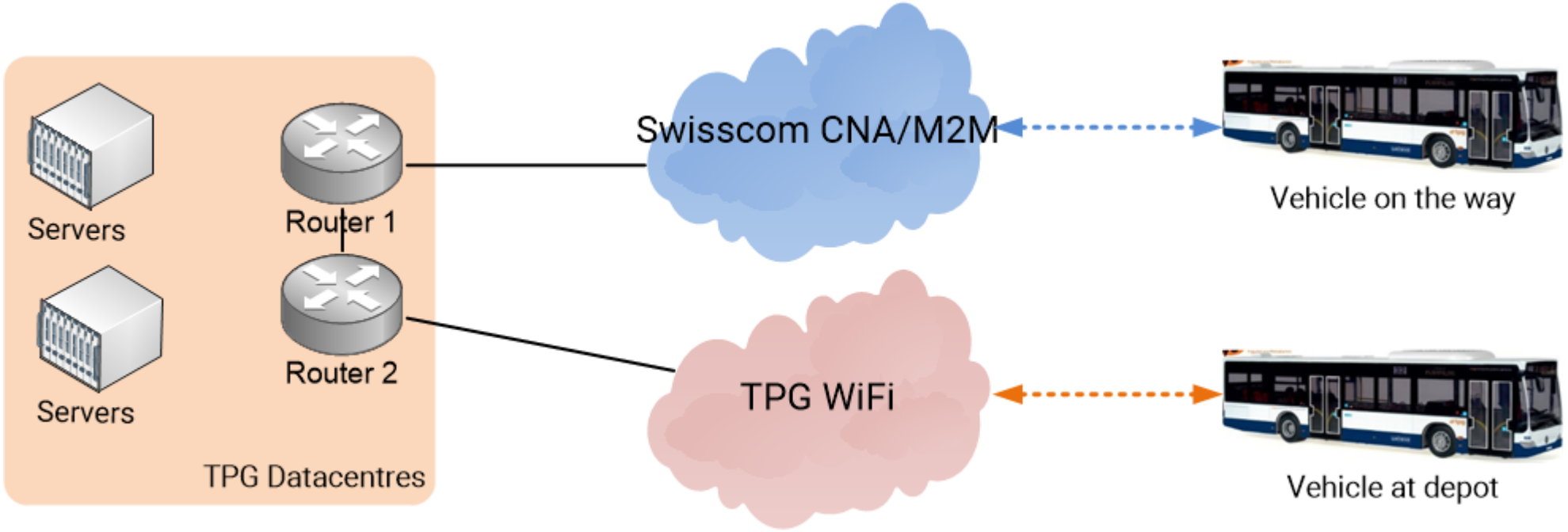

# Vehicles connectivity

## TPG vehicles need connectivity

- Need to supply IP services in the vehicles
  - Ticket machines, inside/outside displays, driving assistance
  - Number of embedded services to grow in the future (video..)
- A fleet of about 700 mobile routers
  - They are Linux PC with a GUI and a suit of network tools
- A mobile “LTE” network
  - The Swisscom Corporate Network Access, with its strength and weaknesses
    - A private virtual network on the 3G/4G infrastructure to connect on-the-road vehicles
- The WiFi enterprise network
  - Under full control
    - Used to join the vehicles at the depots ; without data consumption limits

# Duality of communications

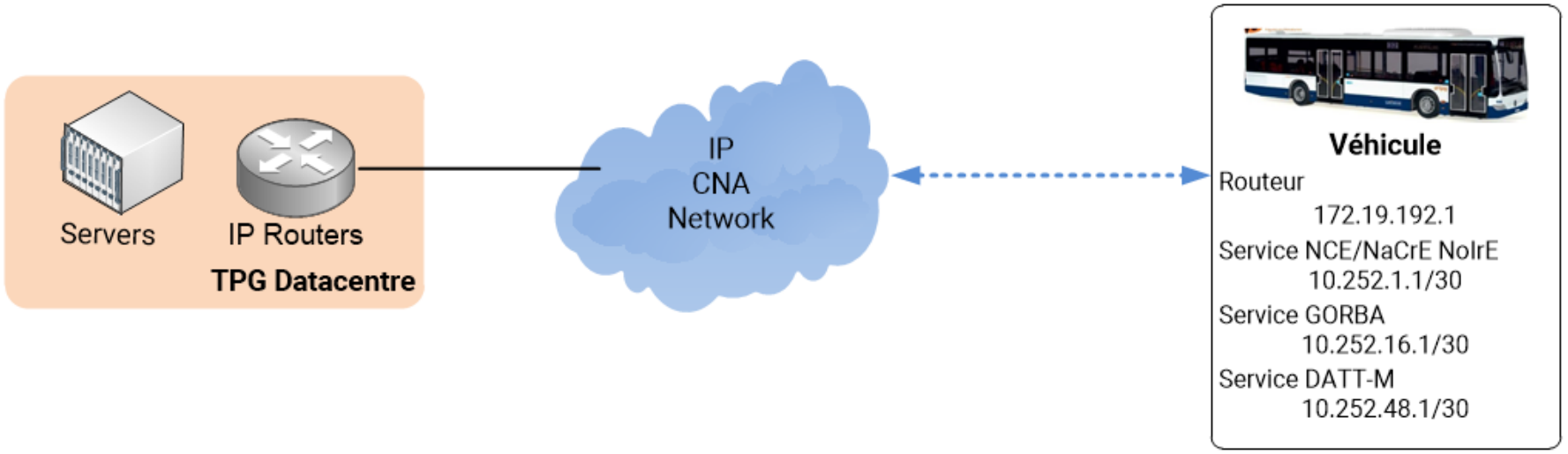
## Need to communicate in every circumstance




- A vehicle's IP address changes depending of its place
  - Need to follow this IP ensure the communication continuity
- No problem when at depot, limitation on the Swisscom CNA
  - Need of surpassing the routing limitation to follow the IP addresses of the embedded services.

# The mobile network constraint

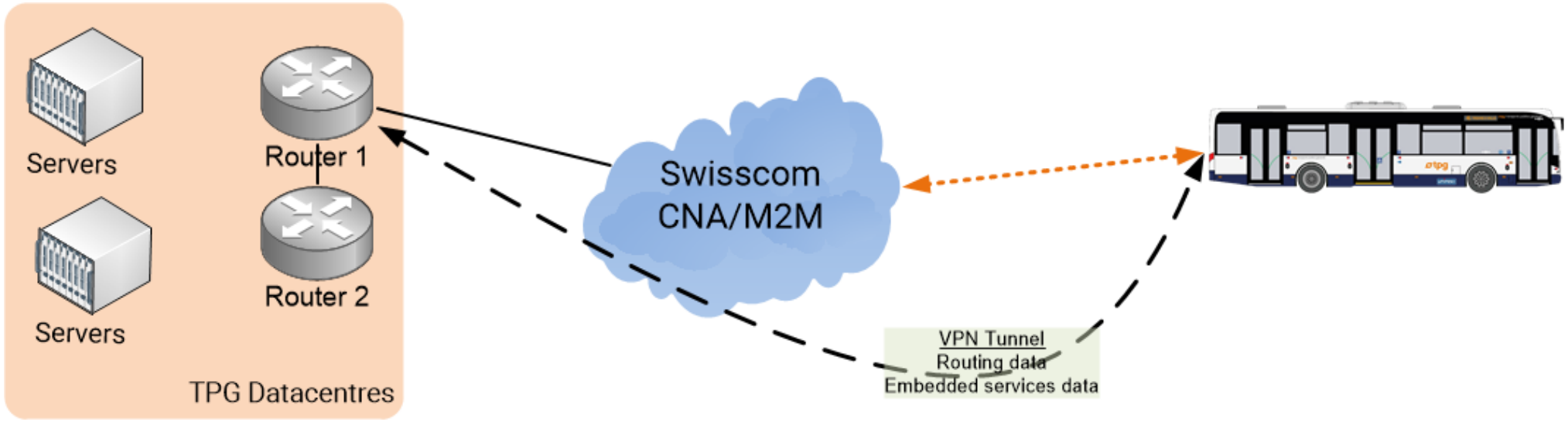
## Restricted routing on the LTE network




- There is a routing limitation on the mobile 3G/4G network
- Not like a regular MPLS VPNv4 network
- One endpoint only has one IP
  - Only one route allowed per vehicle ! But a number of services to provide !
  - NBMA limitations

# An overlay network

## A VPN tunnel to each vehicle

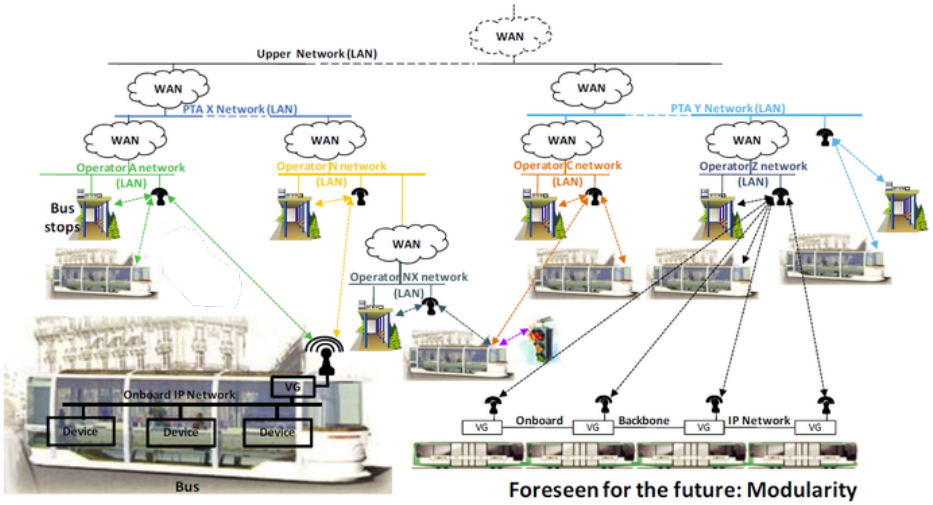


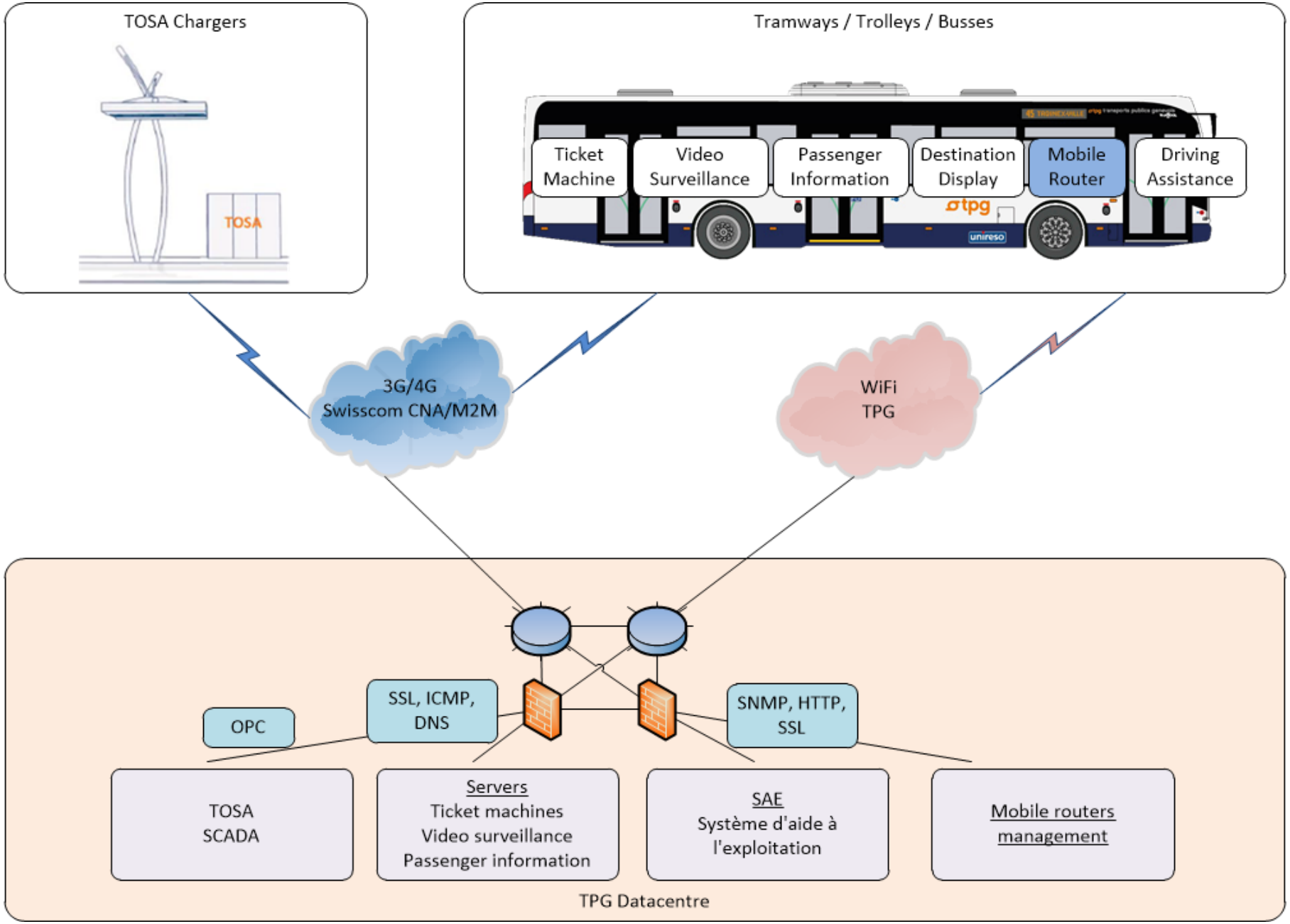

- RFC3344 “Mobile IP” implemented by NetModule
  - To assign a mobile router a constant IP
  - Standard, simple, doing the job... But end-of-life by several vendors !
  - Builds a simple VPN between the datacentre and each mobile router
    - All the VPN form an “overlay” network on top of Swisscom GSM private network
    - The routing limitation of the LTE network are exceeded

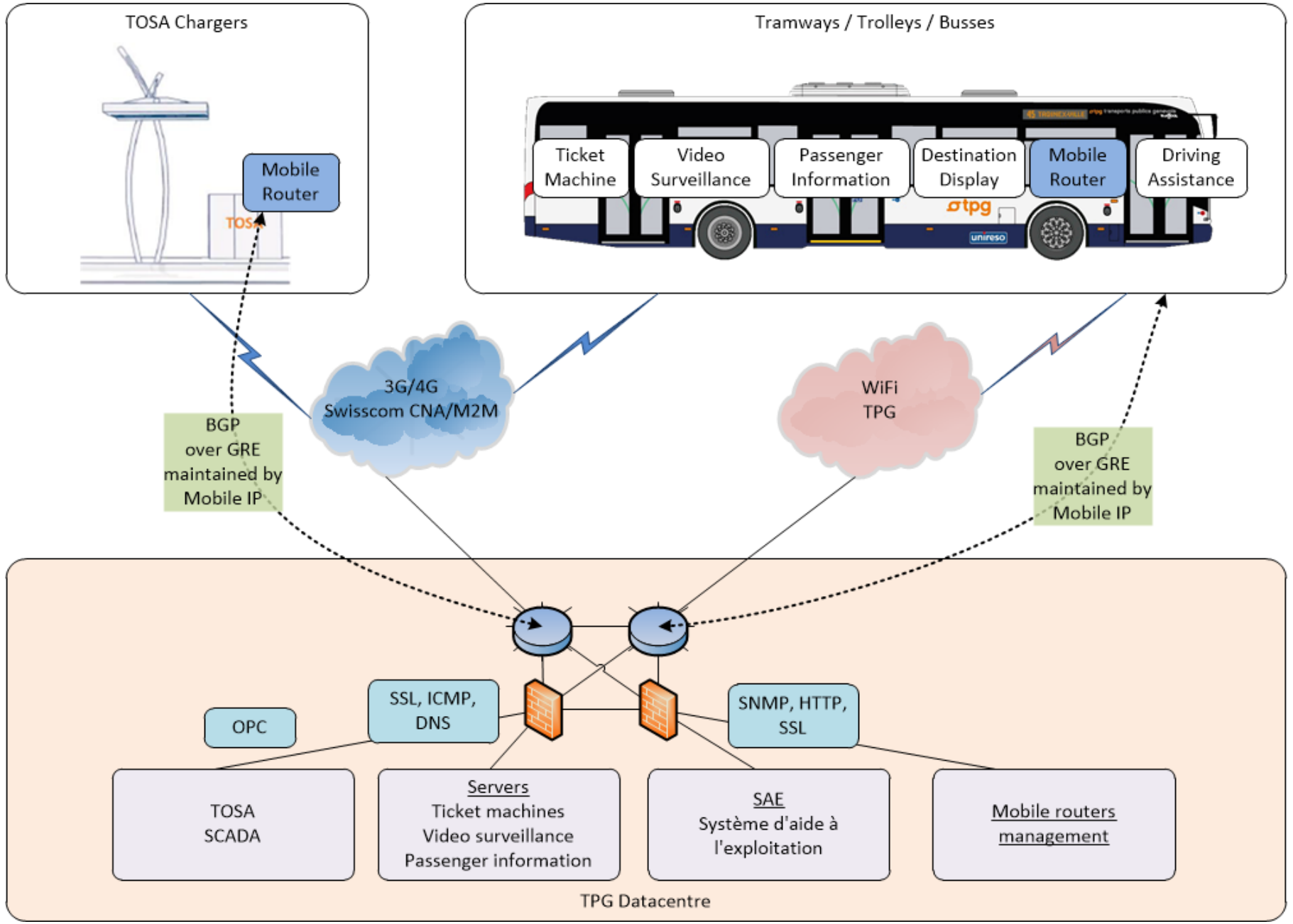
# A need to conform to standards

- ITxPT
  - Standardization effort in public transports IT
    - Standard hardware and architecture
    - Prevent vendor lock-in
  - Cabling, connectors
  - Secure IP connectivity
- IETF standards
  - Internet Engineering Task Force
  - Use of protocols described in RFCs

INFORMATION TECHNOLOGY for PUBLIC TRANSPORT

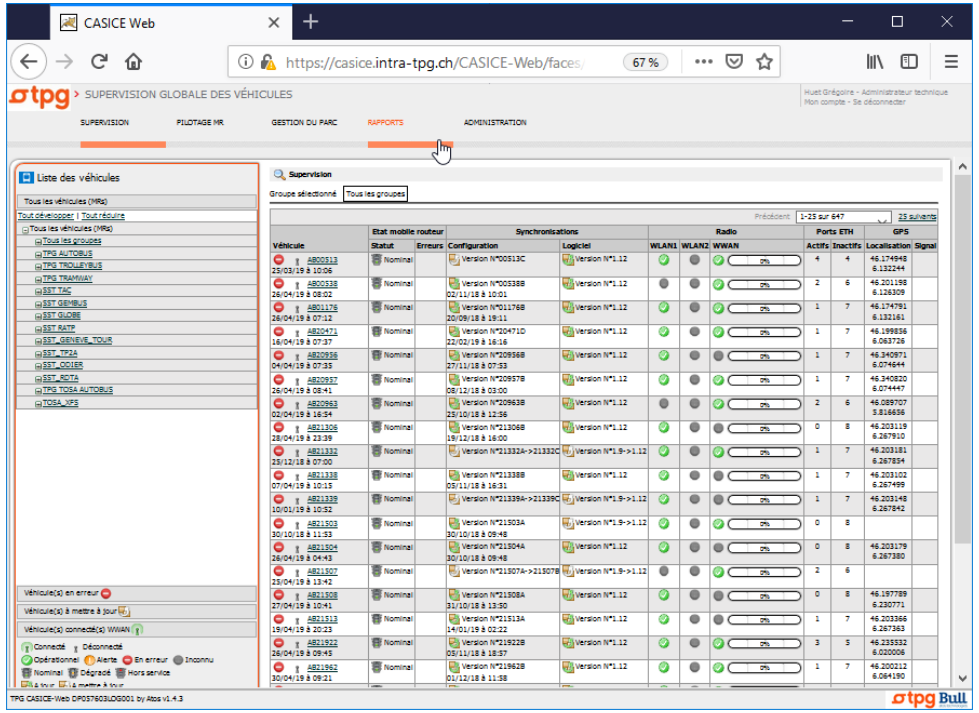


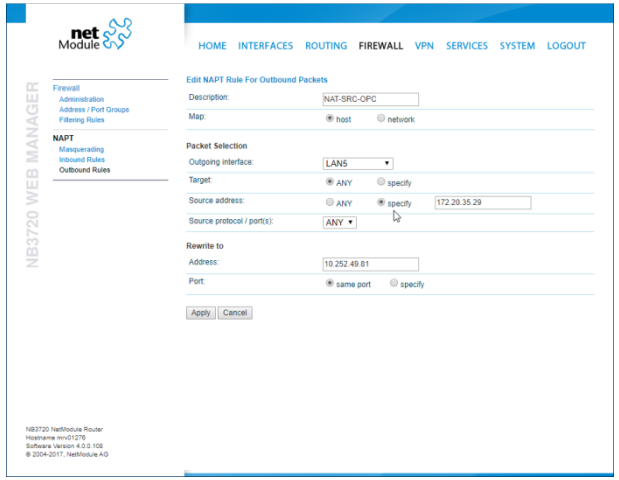

TOSA Chargers
TOSA
Tramways / Trolleys / Busses
Ticket Machine
Video Surveillance
Passenger Information
Destination Display
Mobile Router
Driving Assistance
3G/4G
Swisscom CNA/M2M
WiFi
TPG
OPC
SSL, ICMP, DNS
SNMP, HTTP, SSL
TOSA
SCADA
Servers
Ticket machines
Video surveillance
Passenger information
SAE
Système d'aide à l'exploitation
Mobile routers management
TPG Datacentre


TOSA Chargers
Mobile Router
Tramways / Trolleys / Busses
Ticket Machine
Video Surveillance
Passenger Information
Destination Display
Mobile Router
Driving Assistance
3G/4G
Swisscom CNA/M2M
WiFi
TPG
BGP over GRE maintained by Mobile IP
BGP over GRE maintained by Mobile IP
OPC
SSL, ICMP, DNS
SNMP, HTTP, SSL
TOSA SCADA
Servers
Ticket machines
Video surveillance
Passenger information
SAE
Système d'aide à l'exploitation
Mobile routers management
TPG Datacentre

# The legacy

- On the datacentre side
  - Supervision and configurations management tool
  - Termination on Cisco ASA
    - No support for GRE




- Fleet
  - Manageable Mobile Routers
    - SNMP, Web, propriétary shell commands
  - Heterogeneous
    - VHC, TOSA, xFS, F2G

# Implementation : the headend

## Datacentre side

- Setup of two dual-routers clusters
  - In place of a pair of firewalls
  - One cluster (2 routers) for LTE
  - One cluster for WiFi
  - Solution subject to evolution
    - Mobile IP protocol to replace
      - OpenVPN
    - Mobile IPv6
      - Depending of the mobile router manufacturer support
- Configurations generation
  - The whole fleet has been pre-configured on the datacentre side
    - The tunnels are waiting for the vehicles to connect

# Implementation : on the vehicles

## Migration of the mobile routers

- A number of parameters to change on every vehicle
  - To be done while in production (exploitation)
  - NTP, MIP, BGP, NAT, IP computation, DNS, OSPF
- Adapting the whole fleet by hand is impossible / given time
- Dev of a script to adapt the mobile routers configurations
  - Python, shell, Apache
- Setup of an automation tool to manage the fleet
  - Ansible : mainly because of “no agent” needed
  - Simple “playbooks” (no Python on mobile routers)
  - Capacity to target the vehicles per groups

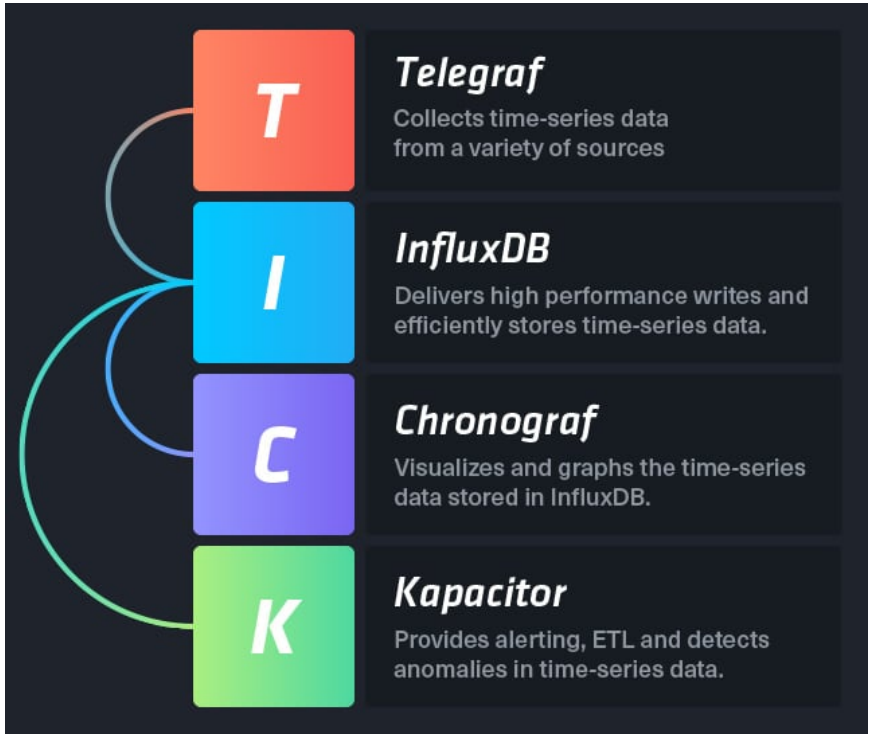
# Monitoring

## Identifying problems, keeping an history

- TOSA charging stations are very sensitive
  - In particular the *Terminal Feeding Stations*
  - Monitoring & alerting Icinga (Common tool for Infrastructure, VM,...)

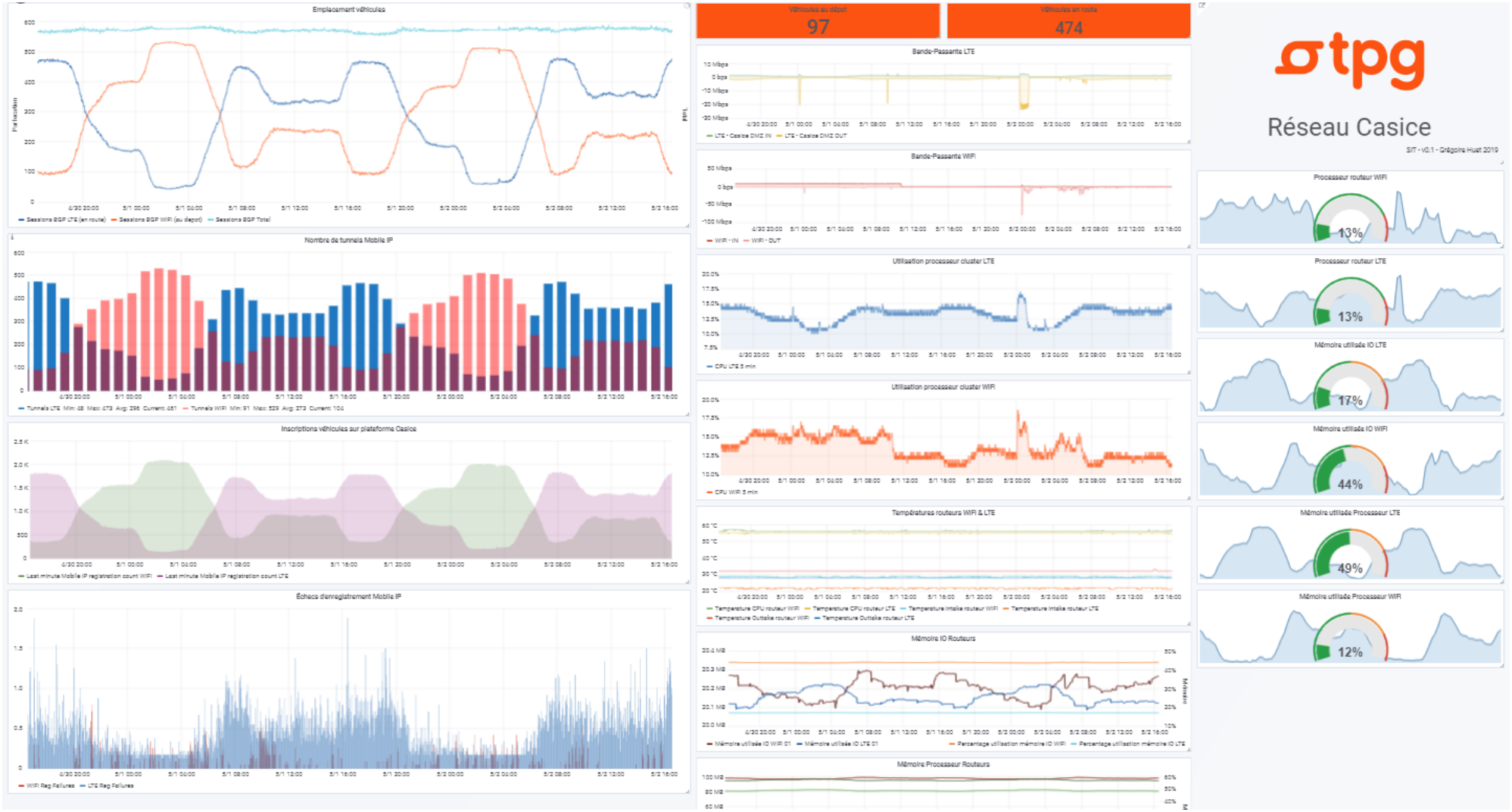
- Visualisation tool based on dashboards
  - Concise and useful information
  - Easily customisable

```
[[inputs.snmp.table]]
  name = "bgpPeers"
  inherit_tags = [ "hostname" ]

[[inputs.snmp.table.field]]
  name = "bgpPeerState"
  oid = "BGP4-MIB::bgpPeerState"

[[inputs.snmp.table.field]]
  name = "bgpPeerRemoteAddr"
  oid = "BGP4-MIB::bgpPeerRemoteAddr"
  is_tag = true
```



# Monitoring

## Dashboard – Datacentre side

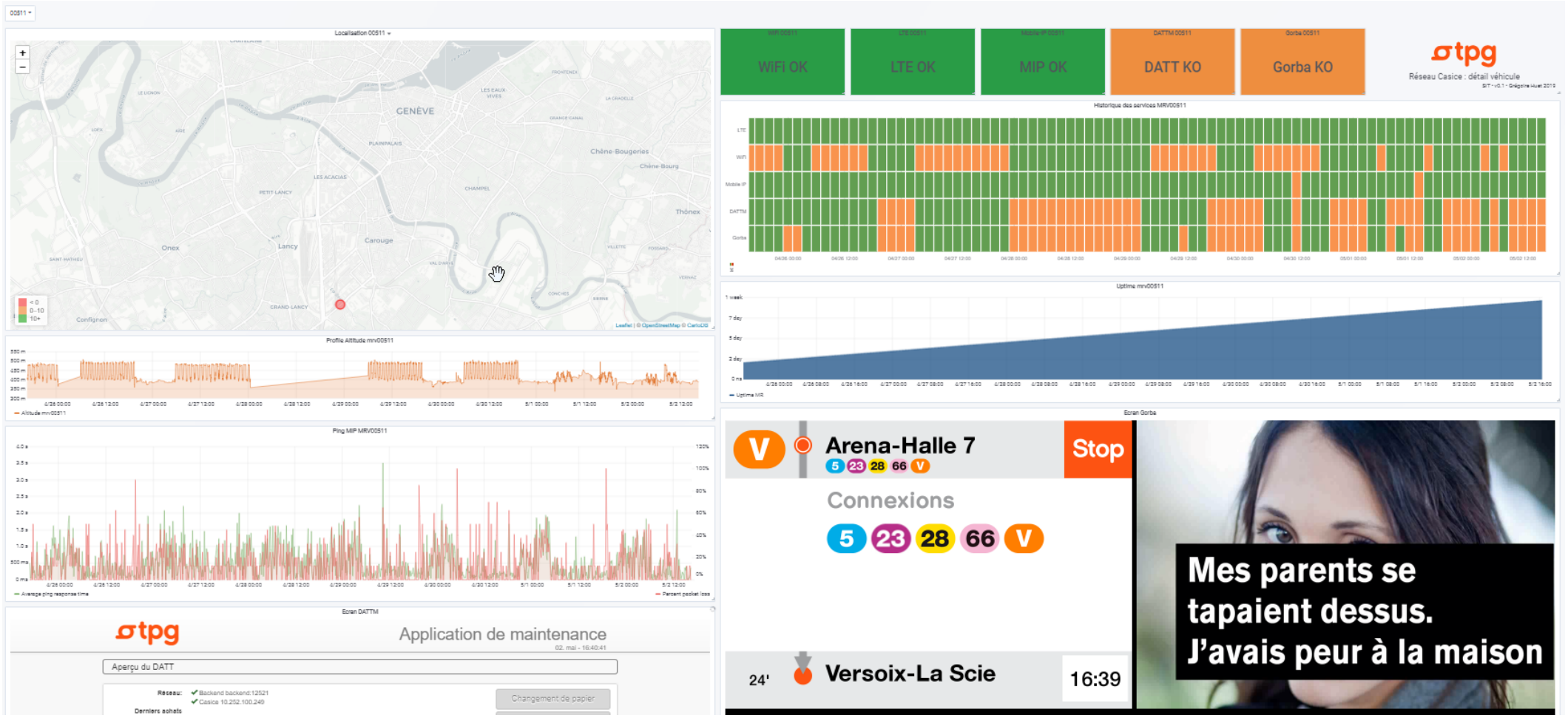


# Monitoring

## Dashboard– Per vehicles series

# Monitoring

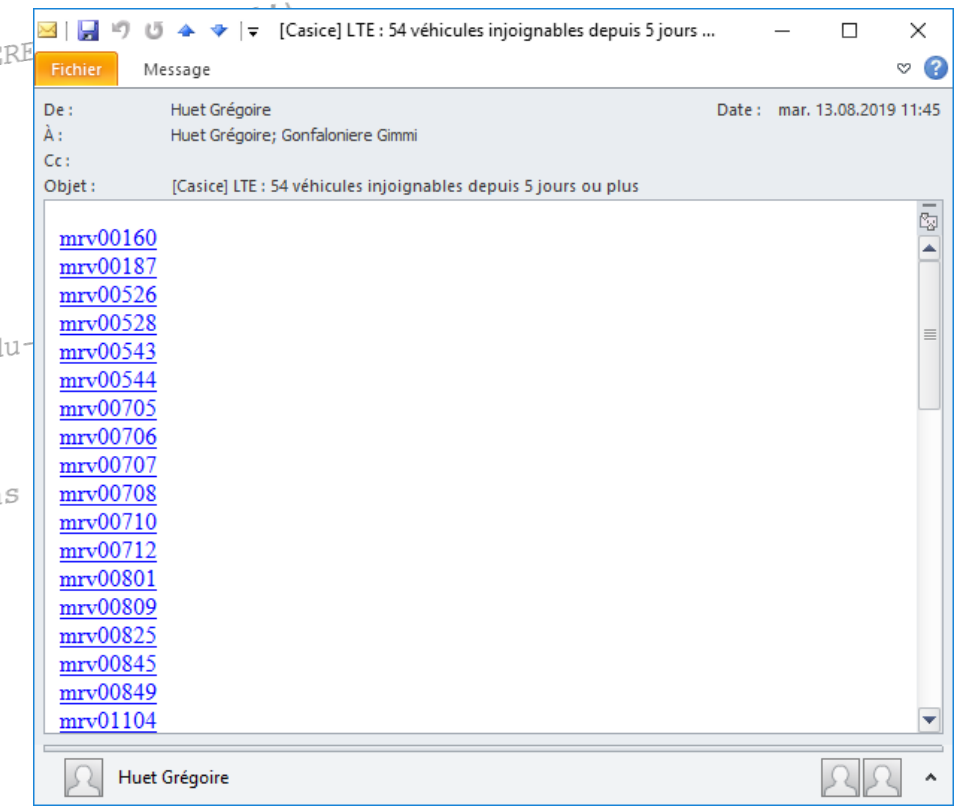
## Dashboard– Per vehicle



# Reporting

## To answer difficult questions

- « I want a daily report by email of all vehicles which did not connect to 3G/4G for 5 days or more.»
  - ***Kapacitor*** monitors time series in batch or “real-time”
  - Provides a monitoring programing language
  - Anomaly detection / Machine learning
  - Dynamic monitoring : no treshholds, possibility the refer to the preceding values in order to alert
  - Integration to multiples alerting systems



# Thank you