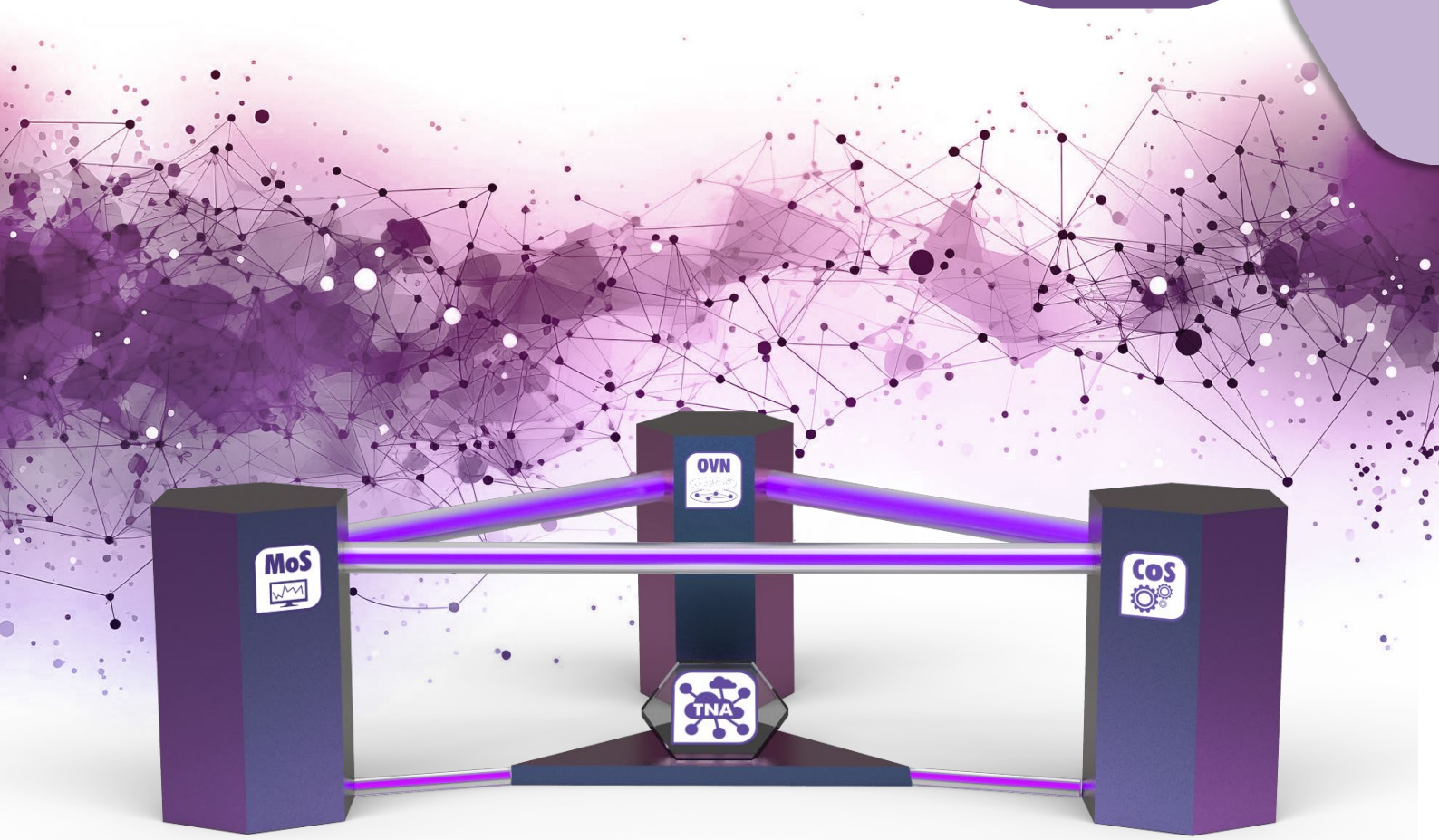
Tiesse
Innovation made in Italy®

Management and automation software



TNA software suite - Tiesse Network Architecture

MoS

Monitoring, analysis and network anomaly detection module

MoS

Datasheet

WWW.TIESSE.COM

TNA

Tiesse Network Architecture

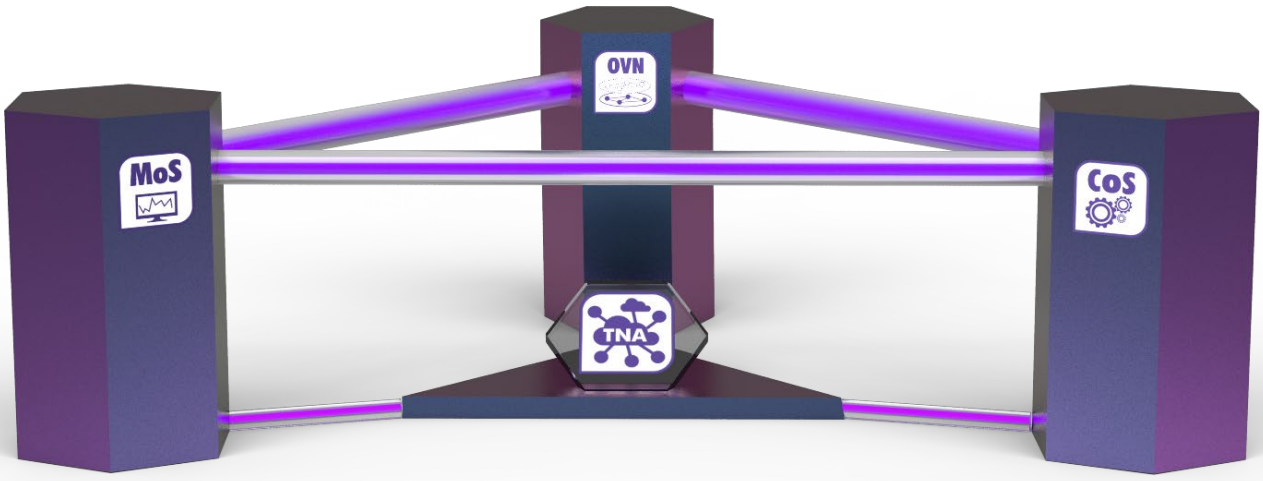
TNA is a distributed SD-WAN solution that gives you complete control over what happens on your network.

TNA (Tiesse Network Architecture) is the platform that gives you complete control over your network. Its main purpose is to enable the creation of a Zero Touch Provisioning network architecture and the monitoring of that network.
It allows you to:

- monitor devices and network status
- view aggregated data
- automatically manage configuration updates according to user-defined policies, triggers or information based on data from all devices.

Another feature of the TNA suite is the ability to perform traffic engineering functions in order to transparently select the link that best suits the performance requirements of the applications.
In addition, the TNA suite allows remote sites to be connected by dynamically creating an overlay network on the public Internet.
The TNA suite is a modular and flexible solution consisting of the following modules **MoS**, **CoS** and **OVN**.

OVN is the module that allows you to create and manage an overlay network on both public and private IP networks subject to NAT, used in the context of an SD-WAN solution.



MoS is the monitoring and analysis module that collects data relating to the behaviour and status of both the network and individual devices. It is capable of monitoring the data traffic of **over 400 applications**, measuring the quality of the links used, detecting any network congestion, and measuring router performance.
MoS also has a specific **Network Anomaly Detection** module.

CoS is the module that allows you to centrally inventory, configure, maintain and update networks of remote routers and IoT devices, both on public and private IP networks.

MoS

Network monitoring and analysis module

The router has an additional agent that periodically sends router operating data to the MOS I module via a TLS session.
The frequency of transmission is a configurable parameter expressed in seconds.
The data that can be exported and viewed may vary depending on the type of device and service. For example, the following information is sent:

- *Uptime* of peripheral network devices and any reboots per time interval
- *Throughput* expressed in bits per second and number of packets per second for all physical, virtual and tunnel network interfaces.
- In the case of a multi-home system, which link is used for the connection (primary or secondary)
- Signal strength on 2G, 3G and 4G networks, if present
- xDSL line alignment data, if present
- Number of active connections (TCP/UDP)
- Number of devices connected to the Wi-Fi network, if present
- Nexthop Round trip time for all interfaces
- Round trip time to an arbitrary destination and with a choice of sending protocol between HTTP, ICMP, UDP, TCP, BFD and TWAMP
- Device CPU and memory usage
- Application-based traffic data
- Data consumption per network interface
- Etc.

COME FUNZIONA

MoS is specifically integrated with Grafana® software, which provides the analysis environment and allows you to run queries and view information using flexible, customisable dashboards.

All metrics and data can be viewed individually or in aggregate form, such as the number of devices transmitting or receiving on a specific network interface, the router with the highest number of active connections as a percentage, or devices with metrics below a certain threshold: the combinations and analyses are virtually unlimited.

Plugins are available that allow interfacing with the most popular data analysis systems.

Furthermore, integration with Open Source monitoring tools is possible.

A **NAD (Network Anomaly Detection)** module is also available, integrated with MOS, which allows you to train an LSTM model, such as Keras/Tensor Flow, to predict unusual network conditions, such as congestion or connection degradation, and prevent impacts on service quality.

ALL-IN-ONE

- ✓ **Visualization** - Wide range of display options to simplify data comprehension.
- ✓ **Multi-channel notification system** - Independent of the graphical interface and extensible. Limits the phenomenon of 'alarm fatigue'.
- ✓ **Aggregation** - Data can be gathered and aggregated within a single dashboard.
- ✓ **Open** - Allows rapid integration and customisation thanks to the use of various plugins available for Grafana® software, an open-source platform.
- ✓ **Extensions** - Creation of hundreds of dashboards and plugins to enhance the data management experience.
- ✓ **Navigation** - Data exploration thanks to ad-hoc queries and dynamic drill-downs. Comparison of different data collection periods and queries.
- ✓ **Collaboration** - Through the agile sharing of data and dashboards from Grafana® software, a data-driven culture is created and expanded across the network.
- ✓ **Autenticazione** - Supportati vari meccanismi di autenticazione quali LDAP, Google Auth, Grafana.com, Github.
- ✓ **Organizzazione** - Possono essere gestite molteplici organizzazioni ognuna con i propri amministratori ed utenti, regole e dashboards. E' supportata la funzione multi-tenancy.
- ✓ **Preferenze** - Per gli amministratori, è possibile selezionare sfondi (tema scuro o chiaro) delle dashboard, modificare i fusi orari e altre impostazioni secondo le specifiche esigenze e preferenze.
- ✓ **Filtri ad hoc** - Creazione di centinaia di dashboard e plugins per ampliare l'esperienza di gestione dati.

MULTI-CHANNEL NOTIFICATION SYSTEM

The multi-channel notification system is **a real-time notification** system that is independent but still integrated into the graphical interface. It is efficient and capable of supporting complex settings and configurations thanks to its own independent database.

Notifications can be sent via various channels: the most commonly used are email, Slack, Pushover and HTTP calls; it is possible to add others, as well as set events to be notified based on even complex parameters.

The MoS multi-channel notification system also has an **"alarm fatigue" protection** function. It is not uncommon for notification systems to experience moments of tilt due to the complexity of trigger event settings, resulting in hundreds of alerts being generated, with the risk of missing important notifications among the large number received: the multi-channel notification system is able to limit this problem thanks to the '**throttling**' function.

The system monitors both the number of alerts sent per hour and whether those generated by the same trigger event exceed a certain amount: in this case, the frequency of sending is revised in order to improve reception, and the notifications themselves are automatically grouped into a single message.

Thanks to the multi-channel notification system, the operator will no longer be dependent on the monitor and graphs for information on events and conditions of interest, but will receive notifications on the channels set up.

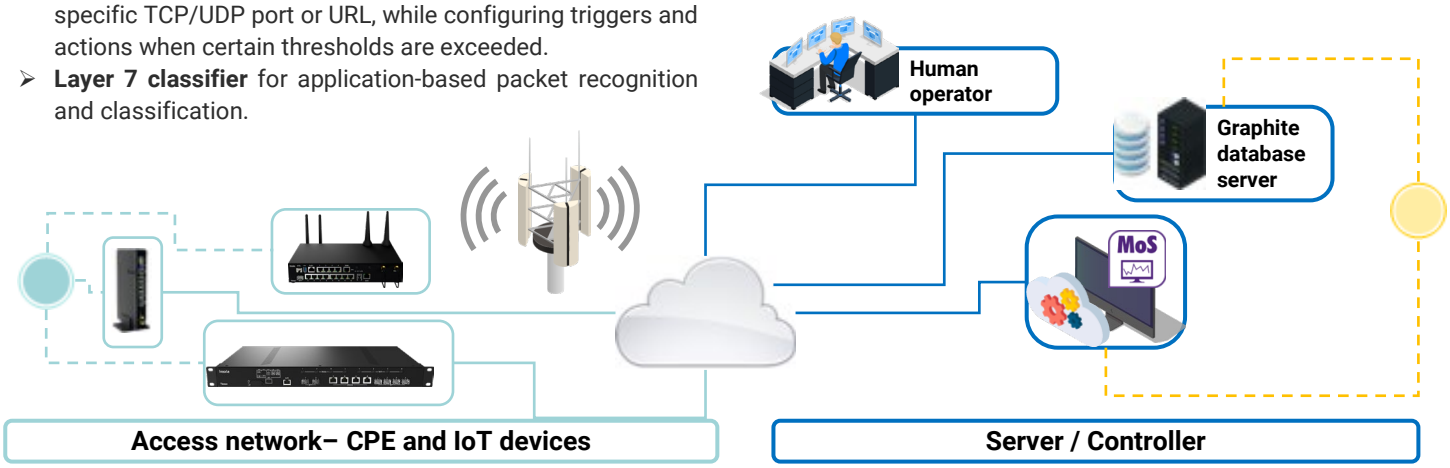
ARCHITECTURE

CPE and Tiesse equipment side (access network)

- ➢ **MoS agent (collectd)** installed on Tiesse routers and devices, consisting of a set of plugins, each of which collects data and information.
- ➢ **RTR service** (Responder Time Reporter) present to measure performance and round trip delay to an IP address, a specific TCP/UDP port or URL, while configuring triggers and actions when certain thresholds are exceeded.
- ➢ **Layer 7 classifier** for application-based packet recognition and classification.

Server / Controller

- ➢ **Load Balancer** and relay nodes to handle up to 10 million metrics per minute.
- ➢ The **database** time-series and the backend server.
- ➢ **Front end** which displays data and allows it to be used (system based on the Grafana® software GUI).



DASHBOARD

The dashboard is flexible and can be customised and personalised according to specific requirements directly by the administrators themselves or can be set up in advance by Tiesse. The product is supplied with a predefined dashboard that includes the following areas.

Router panel

Monitoring and visualisation of key resources **for each individual device** (router, CPE, IoT)

- Router reachability
- Connectivity to a target network/internet (primary/backup or other)
- Reboot count
- Uptime
- RTT - Round Trip Time
  - last mile
  - towards internet targets
- Router load based on current and queued activities on the system
- CPU and memory usage
- Number of active connections
- Inbound/outbound throughput, per interface
- Traffic generated/received per interface
- Traffic classification by application type for specific router
- Number of devices connected to active Wi-Fi network(s)
- GPON optical connections
  - Uptime
  - Input and output optical power
  - Transceiver temperature
- Radio cellular connection
  - Signal strength for each type of connection (4G/3G/2G e SINR, RSRP, RSSI, RSCP, EC/IO)
  - SIM card in use
- xDSL connection
  - Uptime
  - Connection status
  - Signal attenuation
  - Signal-to-noise ratio (SNR)
  - Redundancy errors (CRC)

All router panel

Monitoring and **aggregate** visualisations

- Total number of connected routers, reachable and unreachable, based on uptime
- Number of routers transmitting on a specific interface
- Total number of routers with active mobile connection
- Number of active routers grouped by connection type (primary, backup, other)
- Top 5 active routers by number of connections
- Number of routers connected to 4G, 3G and 2G networks
- Ranking by time of the last routers connected and those no longer reachable
- Ranking of devices by response time (highest and lowest RTT) to a given destination
- Reachable and unreachable devices, based on uptime, within a specified time range

OVN

Monitoring and visualisation of **data relating to the Overlay Network**

- Number of nodes (edges) with which the router has an open peer-to-peer channel
- Bytes and number of packets of the overlay network control protocol
- Total bytes and packets transmitted/received by the router in the overlay network
- Total data transmitted/received via supernode (unicast, multicast and broadcast)
- Bytes and packets transmitted/received via peer-to-peer
- For each router with which peer-to-peer data exchange has taken place, the following are reported:
  - number of bytes/packets passed both in reception and transmission
  - amount of data exchanged with the router via supernode
  - data exchanged via supernode divided by type (unicast, multicast and broadcast)

VoIP

Monitoring and visualisation of relevant **data in Voice over IP (VoIP) scenarios**

- Date and time of the last answered, unanswered, busy, failed, or congested call
- Total duration of answered calls
- Grand total of calls and total divided by answered, unanswered, busy, failed, congested, and total
- Line usage based on active and simultaneous calls
- Connection status for each VoIP server (not registered, registered, rejected)
- For each registered VoIP server, the total number of calls originating from it is shown, divided by type (answered, unanswered, busy, failed, and congested), date, and time
- For each individual FSX port (POTS) on the router, the following information is provided:
  - operating status
  - number of bytes and packets for calls in progress
  - last incoming call answered, unanswered, failed, busy and congested, total number of calls
  - last outgoing call answered, unanswered, failed, busy and congested, total number of calls
- Voltage and electric current values

Intelligent routing - Advanced Traffic Engineering

Thanks to its modules (**CoS**, **MoS**, **OVN**) and their functionalities, the **TNA** suite allows for 'Intelligent routing', i.e. the intelligent routing of data based on the status of the network and the devices that comprise it. The most relevant functionalities are:Policy Based Routing

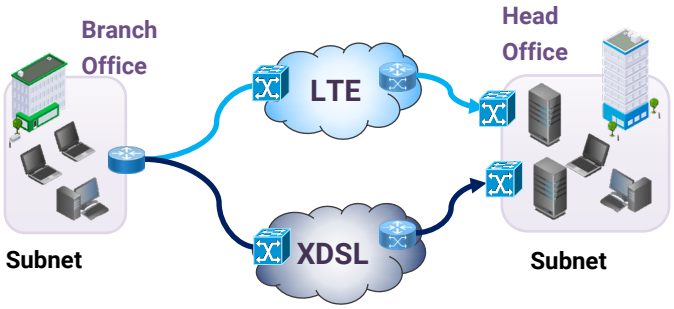
- L7 classifier
- Responder Time Reporter (RTR)
- Overlay Network management (**OVN** module)

By using these and other features together, devices can dynamically modify the configurations and routings used. This provides a complete distributed SDN solution that is ready to respond to changes in network and connection statuses, managing them in an advanced and intelligent manner.

Example - Intelligent routing of HTTP traffic

In this scenario, an xDSL connection is used to connect the head office with the branch offices.

By setting up an event related to HTTP traffic, it is possible to automatically divert web traffic to a mobile radio connection when the values detected do not fall within the threshold values set by the user.



L7

MoS features the **L7 classifier module**, which classifies the most commonly used applications and protocols through accurate and detailed inspection of generated traffic (DPI).

The total amount of data and packets recognised is reported for each individual application. All data can be used to implement any user-defined policies.

The L7 classifier also allows you to set advanced quality of service (QoS) policies within the TNA suite.

SCALABILTY

The Server/Controller component of the MoS module is based on **GOLANG**, the language created by Google for cloud computing infrastructures.

The use of resources by MoS is optimised to make it highly scalable; however, the sizing of these resources depends on the routers to be monitored, as well as the number of metrics per router, the data storage time and the granularity with which the data is monitored over time: the system hosting the Server/Controller must therefore be appropriately configured with these values in mind. A single instance of a dual-processor server equipped with 8GB of RAM can support up to 500,000 metrics/minute.

MoS therefore offers high **scalability**, **availability** and **efficiency**. The architecture is also based on micro-services and can be run on **Kubernetes** for maximum reliability and scalability.

RTR - Responder Time Reporter

MoS is complemented by the **RTR (Responder Time Reporter)** module, which offers the ability to measure network performance and transit times.

RTR periodically sends probe packets (HTTP request, ICMP Echo, UDP Echo, TCP syn, TWAMP - RFC 5357 probe packets) to a specific recipient, collecting the following data for each measurement:

- Round Trip Time
- packet loss
- number of errors

It is also possible to set threshold values for packet loss and Round Trip Time, which allow specific events to be triggered when the values detected do not fall within the set threshold, thereby enabling the implementation of advanced traffic engineering. For example, the user can perform an automatic connection change by setting an event: when the detected values are not within the defined threshold, the connection is moved transparently and automatically.

ANOMALY DETECTION

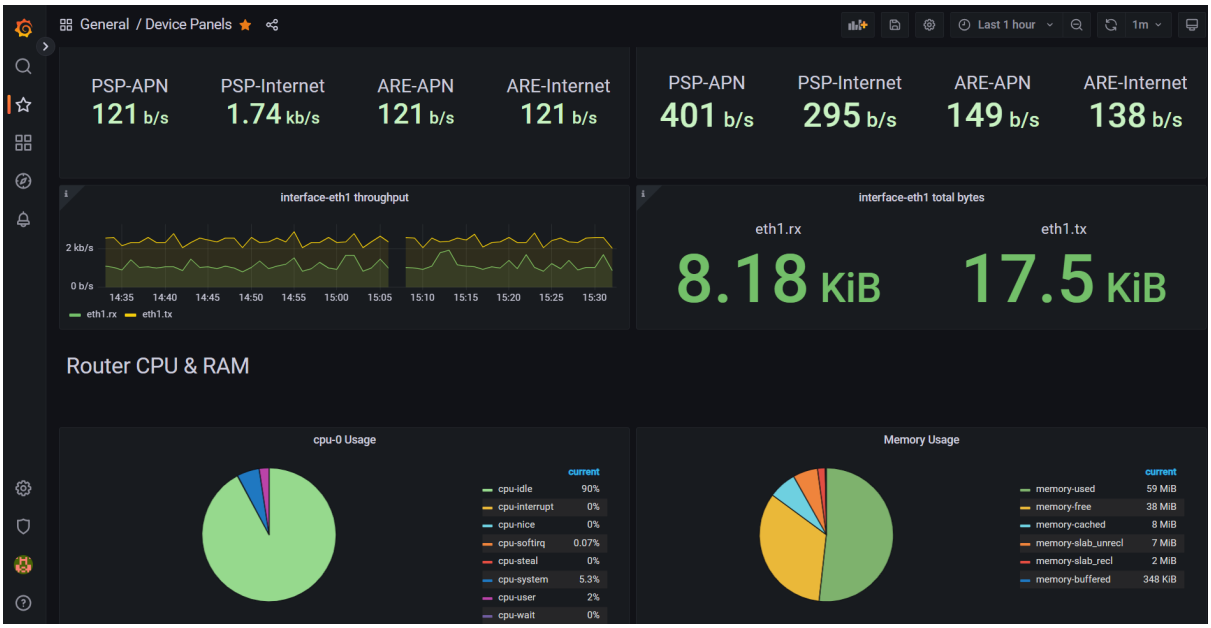
MoS is able to detect anomalies thanks to a specific data analysis component; it recognises network and traffic anomalies both towards routers and central systems.

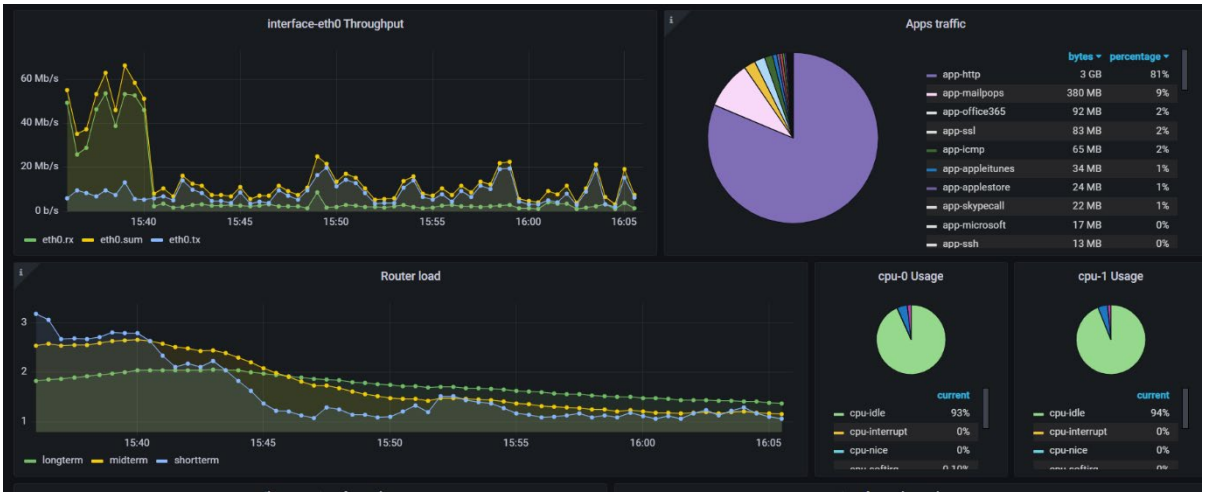
The system uses Keras/Tensorflow **Machine Learning APIs** to autonomously build anomaly thresholds (without human intervention, there is no need to configure or set anything). These thresholds are then updated according to an incremental learning model.

When one of these values is exceeded, the network administrator is immediately notified via appropriate alarms.

DASHBOARD EXAMPLES

Router panel





DASHBORD EXAMPLES

All routers

OVN

VoIP

xDSL

Tiesse

Innovation made in Italy®

Tiesse is a totally Italian company with more than 25 years of experience in the design, development and production of network equipment and IoT devices, suitable for use in mission-critical and industrial scenarios. Tiesse's most successful series, Imola, Lipari and Levanto, are innovative, competitive and certified, and are present in the networks of the major telecommunications operators, in the energy sector, large-scale distribution and vertical sectors, both in the Italian and foreign markets.

Further information on Tiesse solutions can be found on the company website www.tiesse.com.

Info: info@tiesse.com

Marketing & Commerciale: marketing@tiesse.com

www.tiesse.com

Disclaimer

The informations in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Tiesse may change the informations at any time without notice.

Ver. ENG 220925

erion

1000 Trees in Italy