Tiesse
Innovation made in Italy®

Network automation

TNA - Tiesse Network Architecture

MoS

Monitoring and analysis module

MoS

Datasheet

WWW.TIESSE.COM

TNA

Tiesse Network Architecture

TNA is a distributed SD-Wan solution that allows complete control over what happens in the network.

TNA (Tiesse Network Architecture) is the software suite consisting of three modules, whose main goal is to enable the realization of a **Zero Touch Provisioning** network architecture, including:

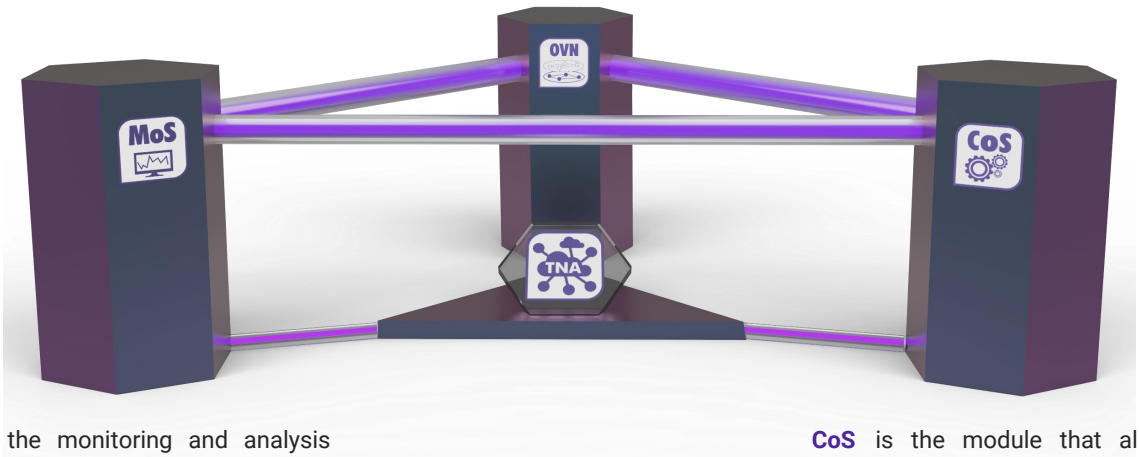
- **monitoring** of equipment and network status
- **displaying** of aggregated data
- **automatic management** of configuration **updates** according to user-set policies, triggers, or data-based information from all devices.

Another feature of the **TNA** suite is the ability to carry out **traffic engineering** functions, in order to transparently select the link that best fits the performance requirements of the applications.

In addition, the TNA suite allows you to connect remote sites by dynamically creating an **overlay network** on the public Internet.

The TNA suite is a modular and flexible solution and consists of the **MoS**, **CoS** and **OVN** modules.

OVN is the module that allows to create and manage an **overlay network** over IP networks subject to NAT, both public and private.



MoS is the monitoring and analysis module that collects data on the behaviour and status of both the network and individual devices. It can monitor the data traffic of more than 200 applications, measure the quality of the links used, detect network congestion, and measure router performance.

MoS also has a specific Network **Anomaly Detection** module.

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

MoS

Monitoring and Analysis Module

The **MoS** module periodically collects on routers, CPEs and IoT peripheral devices produced by Tiesse, data to be monitored by sending them to the central Server/Controller via **TCP or TLS connection**. The reading intervals are configurable for each individual piece of data or globally.

MoS monitors networks, interfaces, recognises the data traffic of more than 200 applications, measures the quality of the links used, detects network congestion, and measures router performance.

The data that can be exported and displayed may vary depending on the type of peripheral device - presence of cellular network connection or voice ports - or depending on the presence of network overlays or other application scenarios.

Specifically, MoS is integrated with **Grafana® software**, which constitutes the analysis environment and allows queries to be performed, information on the status of the link signal on the cellular network, throughput and total amount of traffic, round trip delay, memory and CPU utilisation of individual devices, as well as detailed information on the operating status of the VoIP and overlay network.

Through the installation of simple **plug-ins**, it will also be possible to add new elements to be monitored, such as **NAD (Network anomaly detection)**, which detects anomalies on the network and alerts immediately, allowing timely intervention.

WHAT CAN BE MONITORED - EXAMPLES

- Uptime of peripheral network devices and any time interval reboots
- Bitwise throughput per second and by number of packets per second for all physical, virtual, and tunneling network interfaces
- If the connection is via primary link and those on secondary link
- Signal strength on 2G, 3G and 4G network
- In the case of multi-sim routers if the connection is via primary or secondary SIM
- Number of active connections (TCP/UDP) and number of devices connected to the Wi-Fi network
- Nexthop Round trip time for all interfaces
- Round trip time to an arbitrary destination with a sending protocol of choice between HTTP, ICMP, UDP, and TCP
- CPU usage and equipment memory
- Application-based traffic and network overlay data
- VoIP scenario data (routers with FSX interfaces)
- Data consumption per network interface
- Equipment Reachability and MoS Server/Controller

All metrics and all data can be viewed as well as individually in the form of aggregated data such as the number of devices that transmit or receive on a specific network interface, the router with the higher number of active connections as a percentage, or the devices with metrics below a certain threshold: combinations and analyses are almost unlimited.

GRAPHIC INTERFACE FEATURES

Views — MoS has a wide range of display options to simplify data comprehension.

Multi-channel alerts — Multi-channel notification system, independent from the graphic interface, extensible to other channels in addition to the predefined ones. It limits the "alarm fatigue" phenomenon.

Aggregation — You can group and aggregate the data on a single dashboard.

Open — MoS allows rapid integration and customization thanks to the use of the different plugins available for Graphana technology, which is an open source platform

Extensions — Create hundreds of dashboards and plugins to expand the data management experience

Navigation — Data can be explored thanks to ad-hoc query and dynamic drill-down.

It is possible to compare different periods of data collection time and queries

Collaboration — Thanks to the agile sharing of the data and dashboards offered by Grafana® software, you can create and expand a culture based on network data

Authentication — Authentication mechanisms such as LDAP, Google Auth, Grafana.com and Github are supported

Organization — MoS supports multi-tenancy. Multiple organizations can be managed with their own administrators and users, rules, and dashboards

Preferences — MoS allows administrators to select backgrounds (dark or light theme) of the dashboard, change time zones, and more to suit their specific needs and preferences.

Ad-hoc filters — Ad-hoc filters allow new real-time filter keys/values to be created, and they are automatically applied to all queries using the data source.

MULTI-CHANNEL ALERT SYSTEM

The multi-channel alert system is a **real-time notification system**, independent but still integrated into the graphic interface. It is efficient and able to support complex settings thanks to its own independent database.

Alerts can be sent on different channels: the most used are e-mail, Slack, Pushover and HTTP calls; it is possible to add others, as well as to set events to be notified based on even complex parameters.

The MoS multi-channel alert system also has the **"fatigue alarm" protection** feature. It is not uncommon that in notification systems there may be moments of tilt due to the complexity of the trigger event settings which consequently generate hundreds of alerts, creating the risk of losing important notifications in the amount of those received: multi-channel alert system is able to limit this problem thanks to the "throttling" function.

The system checks how many alerts are sent every hour and if the ones generated by the same trigger event exceed a certain quantity: if so, the sending frequency is revised in order to improve their reception and they are automatically grouped into a single message.

Thanks to the multi-channel alert 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.

ARCHITECTURE

CPE and Tiesse equipment side (access network)

⇒ **Agente MoS** (collectd) installed on Tiesse routers and devices; it is composed of a set of plugins, each of which collects data and information

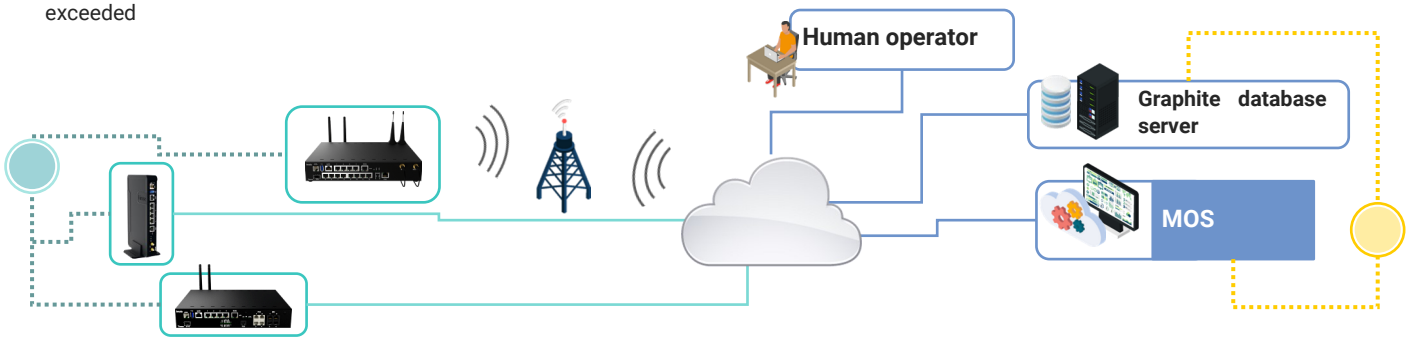
⇒ The **Responder Time Reporter (RTR)** service measures network running performance and traversal times (round trip delay) to an IP address, a specific TCP/UDP port, or a specific URL, while configuring triggers and actions when certain thresholds are exceeded

Server / Controller

⇒ **Load Balancer** and relay nodes, to manage up to 10 million metrics per minute

⇒ **Database** time-series and backend series

⇒ **Front end**, which displays data and allows to use them (system based on Grafana® software GUI)



DASHBOARD

The dashboard is flexible and can be customized to the user's specific needs directly by the administrators themselves or it can be first adapted by Tiesse.

However, the product comes with a default dashboard that includes the following areas.

Router Panel

Monitoring and views of key resources **for each individual device** (Router, CPE, IoT).

- Router reachability
- Connectivity towards a target/internet network (primary, backup, other)
- Reboot count
- Uptime
- RTT - Round Trip Time
  - last mile
  - towards an internet target
- Router load based on current and queued activities on the system
- CPU and memory usage
- Number of active connections
- Throughput - inbound/ outbound, per interface
- Traffic - inbound/outbound, per interface
- Traffic classification by application type for the specific device
- Number of connected devices to the Wi-Fi network/ s
- GPON optical connection:
  - Uptime
  - Optical power inbount/ outboung
  - Transceiver temperature
- Radio cellular connection
  - Signal power for each connection type (4G/3G/2G e SINR, RSRP, RSSI, RSCP, EC/ IO)
  - Current SIM
- xDSL connection:
  - Uptime
  - Connection status
  - Signal attenuation
  - SNR (signal-to-noise ratio)
  - CRC errors (Cyclic Redundancy Check)

All Routers

Aggregate Monitor and View.

- Total number of routers, including all which can be reached and which cannot, depending on the uptime
- Number of routers transmitting on a specifice interface
- Total number of the routers with an active mobile connection
- Number of active routers grouped by connection type (primary, backup, other)
- First 5 active routers by number of connection
- Number of router connected on 4G, 3G and 2G networks
- Classification by time of the last connected routers and those no longer reachable
- Classification of devices by response time (highest and lowest RTT) to a given destination
- Reachable and unreachable devices, as a function of uptime, in a specified time

OVN

Overlay Network data monitoring and views.

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

VoIP

Monitor and view data for **Voice over IP** (VoIP) scenarios.

- Date and time of last response call, unanswered, busy, failed, congested
- Total Response Call Duration
- Total call total and total divided by answers, unanswered, busy, failed, congested, and total
- Line usage based on active and concurrent calls
- Connection status for each VoIP server (not registered, registered, rejected)
- For each registered VoIP server, the total number of calls from it is shown, divided by type (answers, unanswered, congested, busy and failed), date and time
- For each individual FSX port (pots) on the router, the following are:
  - the operational status
  - bytes and packets number for calls in progress
  - last response, unanswered, failed, busy and congested calls, total number of calls
  - last outgoing answered call, unanswered, failed, busy and congested, total number of calls
- Tension and current values

Intelligent routing - Advanced Traffic Engineering

Thanks to its modules (CoS, MoS, OVN) and their features, the TNA suite allows you to perform "Intelligent routing", i.e, the intelligent routing of data according to the state of the network and of the devices that compose it.

The features most involved are:

- Policy Based Routing
- L7 classifier
- Responder Time Reporter (RTR)
- Overlay Network Management (OVN module)

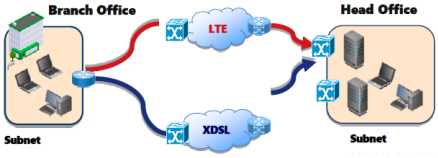
Thanks to the joint use of these and other features, the devices are able to dynamically change the used configurations and routes.

In this way you get the use of a complete distributed SDN solution, ready to react to changes in network and link states, managing them in an advanced and intelligent way.

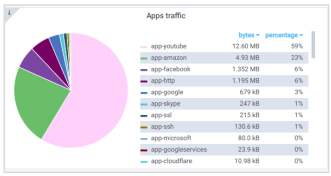
Example - HTTP traffic intelligent routing

In this scenario, the xDSL connection is used to connect the main office with the branch ones.

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



L7 CLASSIFIER



MoS has **L7 classifier module**, used for the classification of the applications and protocols mostly used thanks to an accurate and detailed traffic inspection (DPI).

For each application, the total of data and recognized packages are reported. All data can also be used to implement any user-defined policies.

In addition, the L7 classifier allows for advanced QoS policies within the **TNA** suite..

SCALABILITY

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

The use of resources by MoS is optimized to make it highly scalable; the sizing of these resources is a function of the routers to be monitored, as well as the number of metrics per router, data storage time, and the granularity with which data is monitored over time: the system hosting the Server/Controller will then need to be properly configured with these values in mind. A single instance of Dual Processor Server equipped with 8GB RAM can support up to 500,000 metric per minute.

MoS therefore offers high scalability, availability, and effici ency.

The architecture is also based on micro-services and can be run on **Kubernetes** for reliability and scalability.

RTR - Responder Time Reporter

MoS is completed by the **Responder Time Reporter (RTR) module**, which provides the ability to measure both network performance and crossing times.

RTR sends periodically probe packets towards a specific recipient (probe type are HTTP request, ICMP Echo, UDP Echo, TCP syn, TWAMP - RFC 5357), collecting for earch measurement:

- **Round Trip Time**
- **Packet loss**
- **Errors number**

You can set thresholds on packet loss and Round Trip Time, which allows you to enable specific events when the detected values are outside the set threshold, thus enabling the implementation of advanced traffic engineering. For example, the user can perform an automatic connection change by sertting an event: when the detected values are not included in the defined threshold, the connection is moved transparently and automatically.

ANOMALY DETECTION

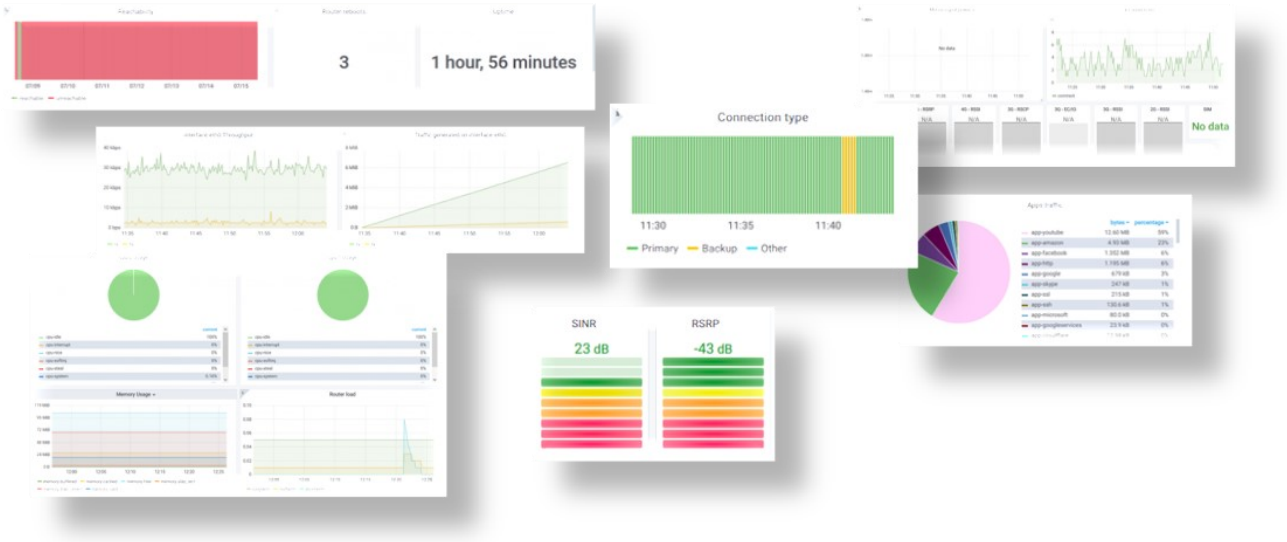
MoS is able to recognize the presence of anomalies thanks to a specific data analysis component; it catches network and traffic anomalies both to routers and to central systems.

The system uses the APIs of **Machine-Learning Keras/Tensorflow** 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.

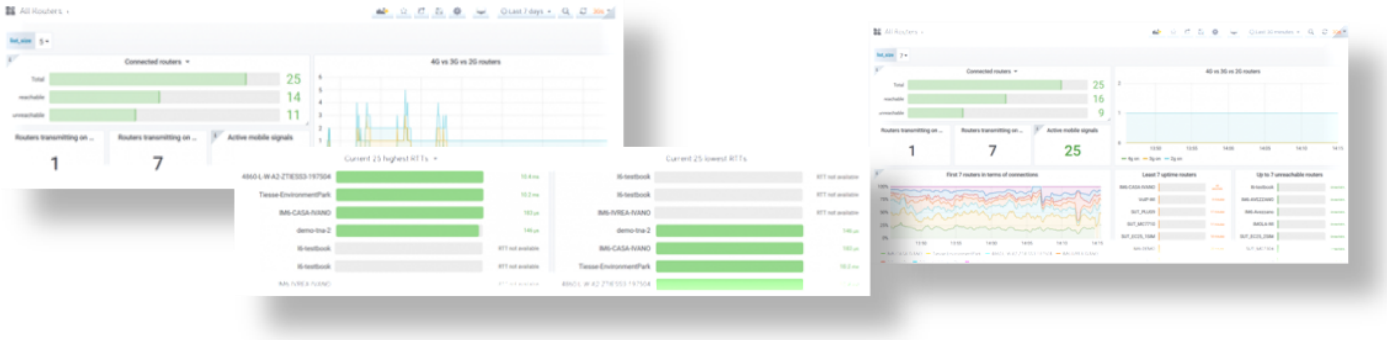
When one of these values is exceeded, the network administrator is immediately alerted by appropriate alarms.

DASHBOARD EXAMPLES

Router



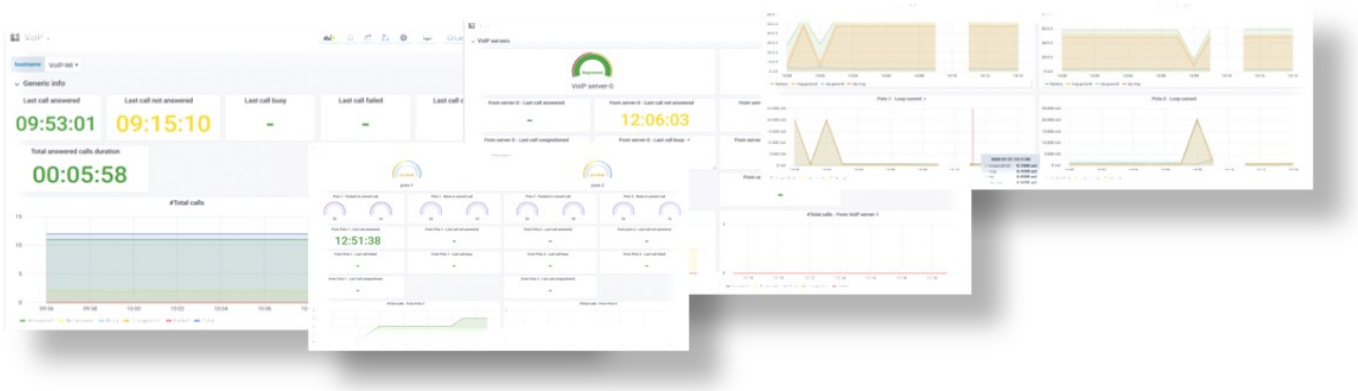
All Routers



OVN

DASHBOARD EXAMPLES

VoIP

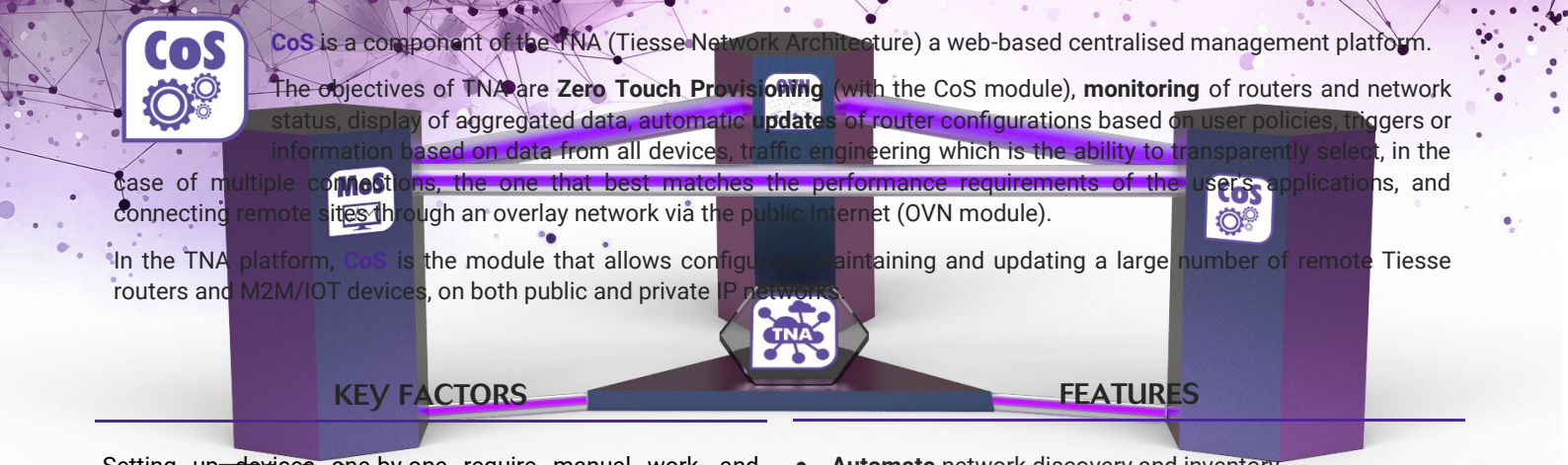


xDSL

Tiesse
Innovation made in Italy®

CoS Network automation

Centralised management module



CoS is a component of the TNA (Tiesse Network Architecture) a web-based centralised management platform.

The objectives of TNA are **Zero Touch Provisioning** (with the CoS module), **monitoring** of routers and network status, display of aggregated data, automatic **updates** of router configurations based on user policies, triggers or information based on data from all devices, traffic engineering which is the ability to transparently select, in the case of multiple connections, the one that best matches the performance requirements of the user's applications, and connecting remote sites through an overlay network via the public Internet (OVN module).

In the TNA platform, **CoS** is the module that allows configuring, maintaining and updating a large number of remote Tiesse routers and M2M/IOT devices, on both public and private IP networks.

KEY FACTORS

Setting up devices one-by-one require manual work and implies the possibility of human errors, which increases the deployment time.

CoS by Tiesse

- **reduces the effort**
- **limits the errors**
- **cuts the costs**

configurations at once as well as to upload firmware to different Tiesse routers and appliances, copy configurations, planning updates with just one click.

Moreover, it enables:

- Fast configuration deployment and reduced setup time
- Greater deployment efficiency
- Reduction of risks due to the overall administration of the network
- Easy integration of new remote site
- Long life installations, supporting easy configuration migration

FEATURES

- **Automate** network discovery and inventory
- **Display information** about configurations and firmware versions
- **Update firmware and configurations** manually by an operator or **planned** by setting time slots
- Create and deploy network **devices configuration templates**
- **Classify** the devices and create multiple groups
- Setup networks and new network in few simple steps
- **Set commands** for specific services activation or deactivation, for specific carriers or types of connection
- Support **self-provisioning configurations**
- Display and download **reports** for each scheduled update
- Define **user accounts with different privilege** levels from read only mode up to administrator. Each level of user has specific restriction, like setting updates, creating and modifying templates, managing additional services and exceptions, modifying and creating user accounts and manage global settings.

TNA - Tiesse Network Architecture

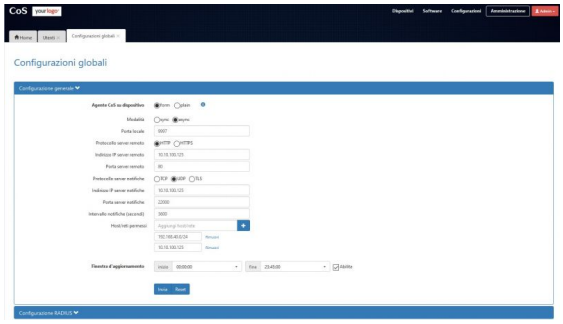
MoS
Monitoring and analysis module

HOW IT WORKS

CoS's server process (cosd) communicates with the **CoS** part installed on Tiesse routers (named **CoMS agent**).

Each device periodically sends a notification to the server process containing the information on current firmware and configuration. After receiving them, the server process compares the current versions installed on the routers to the desired ones and so determines if the devices need to be updated (configuration, firmware or both).

The process manage the updating process by contacting each single router on a specific web page. When this phase starts, the router contacts the CoS web server to ask which versions should be updated and applied. Server process continues to monitor the notifications to check the success or the failure of the update and then provides a report for each scheduled one.



The update on a single router can be performed by an operator or in the set time slot previously authorized via web gui.

CoS server achieves routers data via XML files in the Router Directory (SAR).

CoS is available both in Italian and English.

It is customizable with specific customer information and it allows, via API, the export of data to be used in the customer's monitoring platforms.

It is customizable with specific customer informations and it allows, via API, the export of data to be used in the customer's monitoring platforms.

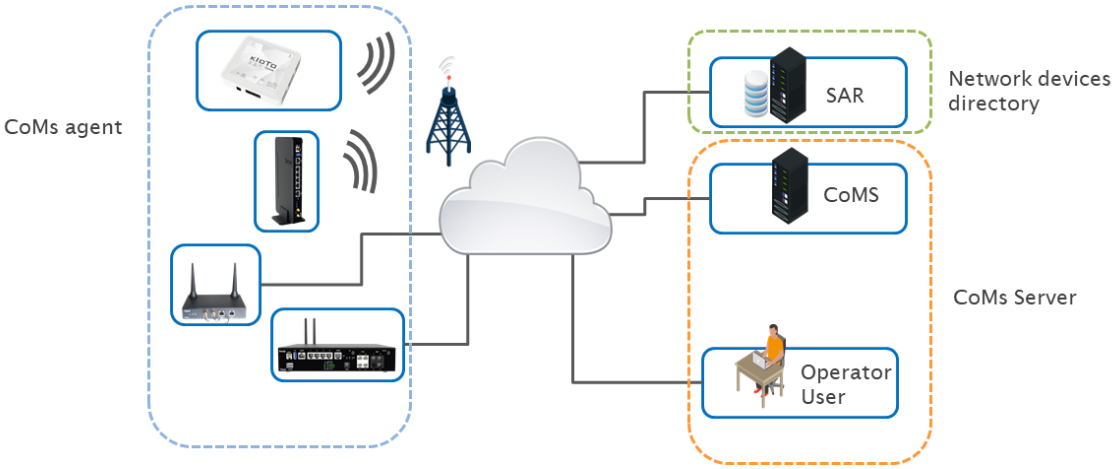
SCENARIOS

CoS consists of three elements:

⇒ **Tiesse routers and M2M/IoT network appliances** equipped with CoS agent

⇒ **CoS server** which manages both control and update processes. The application represents the CoS system core and is in charge of listening to the messages/notifications sent from the network devices. A web interface allows interactions between operators and users.

⇒ **The Router Directory (SAR)** in which the data related to the administrative status of each devices and the configuration parameters are stored in XML file format.



WEB GUI

The web interface is accessible with the proper level of authentication (via Radius server). The interface is organized by tabs grouped by functionalities as well as subdivided in specific sections.

Main Group Functionalities	Sections
iOS	Firmware
Devices	Groups
	Routers
Admin	Global Settings
	Users

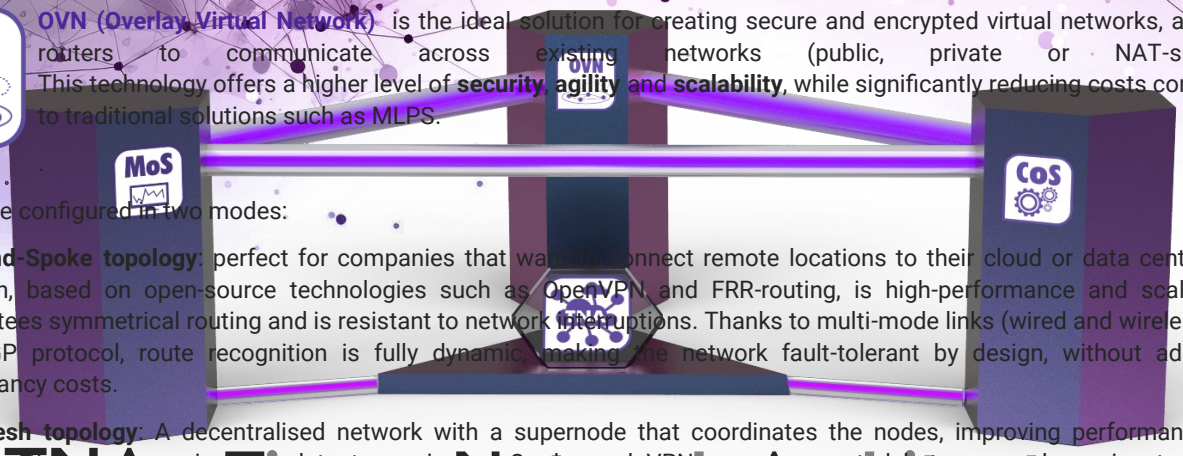
Main Group Functionalities	Sections
Configurations	Services
	Carriers
	Line Types
	Router models
	Router functions
	Templates
	Add-on services

Tiesse
Innovation made in Italy®

OVN Network automation

Overlay Networks Management Module

OVN (Overlay Virtual Network) is the ideal solution for creating secure and encrypted virtual networks, allowing routers to communicate across existing networks (public, private or NAT-subject). This technology offers a higher level of **security**, **agility** and **scalability**, while significantly reducing costs compared to traditional solutions such as MLPS.



OVN can be configured in two modes:

1. **Hub-and-Spoke topology**: perfect for companies that want to connect remote locations to their cloud or data centre. Our solution, based on open-source technologies such as OpenVPN and FRR-routing, is high-performance and scalable; it guarantees symmetrical routing and is resistant to network interruptions. Thanks to multi-mode links (wired and wireless) and the BGP protocol, route recognition is fully dynamic, making the network fault-tolerant by design, without additional redundancy costs.
2. **Full-Mesh topology**: A decentralised network with a supernode that coordinates the nodes, improving performance and reducing the steps required for data transmission. On-demand VPNs can be created between nodes using tunnelling protocols such as GRE, VXLAN and IPSEC.

TNA - Tiesse Network Architecture

KEY FACTORS

The OVN module was designed to achieve

- **Security**
- **Agility**
- **Scalability**
- **Competitive**

And also

MoS
Monitoring and analysis module

High Cost reduction

Unlike more popular solutions, such as MPLS and IPSec, which also require a very expensive hardware part, Tiesse's solution is much cheaper and lowers utilisation/ management/maintenance costs, because it uses user-space tunnelling technologies and relies on 'general-purpose' hardware (such as virtual machines or physical servers on x86 platforms), exploiting parallelism for OVN tunnel management.

Advanced Monitoring

Integrated with **TNA** and **Grafana®**, the OVN module allows monitoring of nodes, data traffic and tunnel status, providing a complete and detailed view of the network

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: mail@tiesse.com

Marketing & Sales: marketing@tiesse.com

www.tiesse.com

Via Asti 4
10015 Ivrea (TO)

Tel +39.0125230544
Fax +39.0125631923

Viale L. Gaurico 9/11
00143 Roma EUR

Tel +39.0654832203
Fax +39.0654834000

Via Livorno 60
10144 Torino (TO)

Via C. Corradini 80
67051 Avezzano (AQ)

Ver. ENG 030225

erion

1000 Trees in Italy