

SECURING NETWORKS WITH VLAN TAGGING IN MANAGED SWITCHES

HIGHLIGHTS

- ✓ Many organisations establish VLANs for greater security of their network infrastructure. However, this requires advanced network switches capable of providing granular control that extends even to endpoint devices.
- ✓ Managed switches are the ideal solution for these challenges. They enable network administrators to establish multiple VLANs, effectively segregating company departments while having utmost reachability over each end device.
- ✓ Beyond VLAN tagging, managed switches like the TSW202 and TSW212 offer QoS and scheduling features that allow for prioritised data flow management from multiple endpoints and automate tasks such as periodic port shutdown for even greater network management.

THE CHALLENGE – BEYOND CONNECTIVITY SUPPORT

In any organisation, regardless of size, building a new network infrastructure requires maximising each department's efficiency and security. This is crucial, as no one would prefer to sacrifice their precious data, which hackers seem to like so much that they make each data breach have an average cost of [\\$4.45 million globally](#).

Ensuring your company's data security is also critical, considering the inevitable exchange of sensitive data within each department. For this, you have to ensure that data transfer and access to it are highly controlled and secure, sometimes even from the eyes of other company departments.

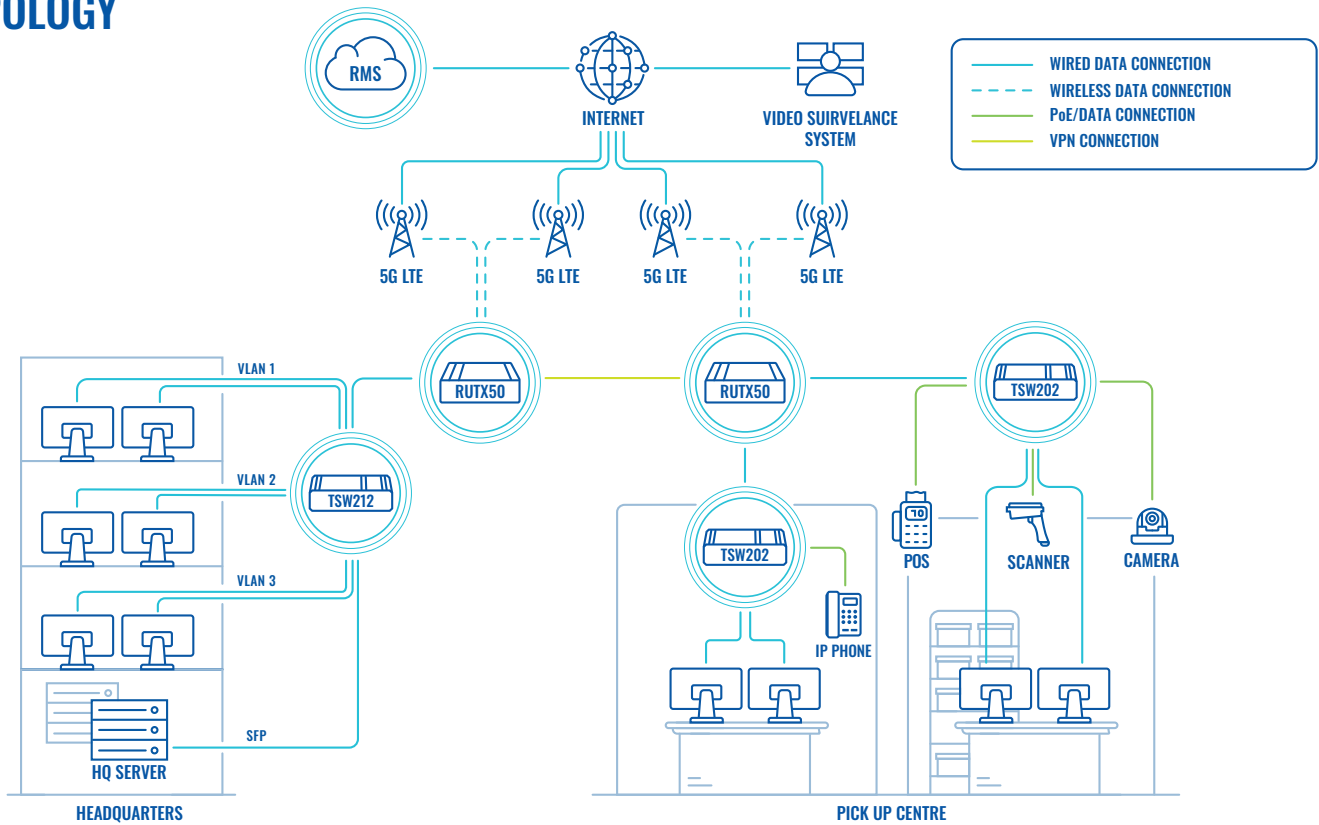
To address these challenges, many choose to establish separate [virtual local area networks](#) (VLANs) for each department, which is relatively cheap and easy to achieve. VLAN in networking effectively isolates departments from one another, preventing them from accessing data that's not meant for them.

It can also provide an added layer of security from outside threats: if one department suffers a data breach, others belonging to different VLANs remain unaffected.

However, an additional challenge emerges for larger companies that sell goods and have many pick-up centres across multiple cities or countries, as transferring data to headquarters from these locations introduces another level of security concerns.

Given the importance of managing data from multiple endpoints, it's clear that components like network switches are vital for establishing a complex network infrastructure. They should facilitate centralised data flow management and ensure that only authorised personnel, like system administrators, can access it safely.

TOPOLOGY



THE SOLUTION – MANAGED SWITCHES FOR MAXIMISED CONTROL

For such challenges, managed switches such as Teltonika Networks’ TSW202 and TSW212 are ideal. They provide robust network connectivity across office departments and offer granular control over the entire network infrastructure, extending it even up to endpoint devices.

When connected to our RUTX50 5G router via Ethernet cable, the TSW212 8-port managed switch expands connectivity to the headquarters’ server through SFP ports. It also connects multiple computers in different departments via Gigabit Ethernet ports for high-throughput data transmission for all endpoints.

The potential for more advanced configurations can be unlocked with excellent connectivity covered. The TSW212 managed switch supports VLAN tagging configurations, allowing each department to operate on separate VLANs.

This feature enables effective traffic management, as if departments are operating on separate networks while maintaining isolation from one another. This can then be centralised, managed, and monitored by the network’s administrators, who can oversee the entire network infrastructure and data transmission across all departments.

Also, the TSW212 managed switch supports quality of service (QoS), which you can use to prioritise specific types of traffic. For instance, sales department data can be prioritised over accounting data, ensuring that when network infrastructure experiences data congestion, data from sales will be the first to reach corresponding endpoints.

So, with features like QoS and VLAN tagging, you can ensure a secure network and seamless data transmission for the best efficiency.

The same network prioritisation can be applied with the TSW202 managed switch in remote pick-up centres, giving POS terminals higher priority over data-intensive camera feeds to ensure the highest accuracy over stock data, at all times.

And since the TSW202 is a **PoE+** switch, it can be plugged into POS systems, cameras, scanners, and IP phones to supply the end devices with network connectivity and power.

Managed switches additionally excel in this scenario for features like scheduling, which you can use to automatically turn on or off end devices, enable prioritisation for specific hours only. Additionally, given their compatibility with RMS, you can leverage [RMS](#) management and its multiconfiguration tool to execute these procedures remotely for all devices in a single session.

Since both headquarters and pick-up centres need to uphold communication with one another for commands and data transmission to know the stocks, payment information, etc., they must do so remotely yet securely. For this reason, a VPN-enabled connection is necessary. A VPN will enable the administrators to reach headquarters and pick-up centre data securely.

Managed switches like the TSW202 and TSW212 are particularly valuable in complex network infrastructures because they support multiple protocols. They're compatible with STP and RSTP protocols, which prevent network loops and broadcast storms and facilitate quick recovery from network topology changes, crucial for maintaining network uptime.

