RIVI NETWORKS

ICX7150 SERIES MANAGED SWITCH

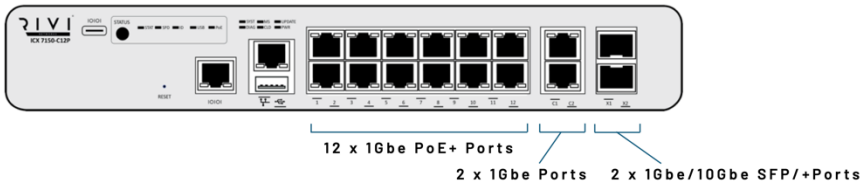
Quick Start Guide

ENGLISH

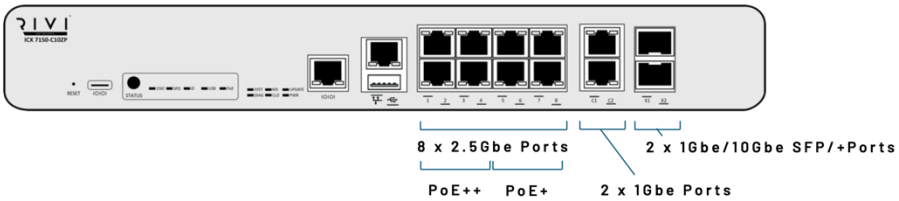
Contents

Product Models and Features

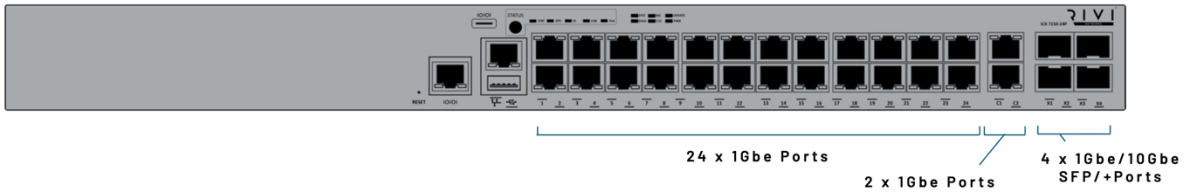
ICX7150-C12P (PoE+, 12 x 1Gbe PoE+, 2 x 1Gbe, 2 x SFP/SFP+



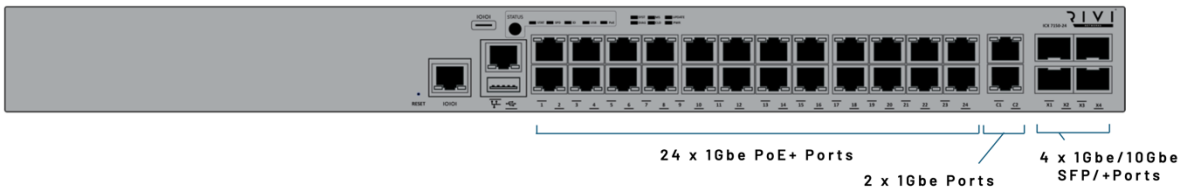
ICX7150-C10ZP (PoE++, 8 x 2.5GbeMultigig, 2 x 10Gbe, 2 x SFP/SFP+)



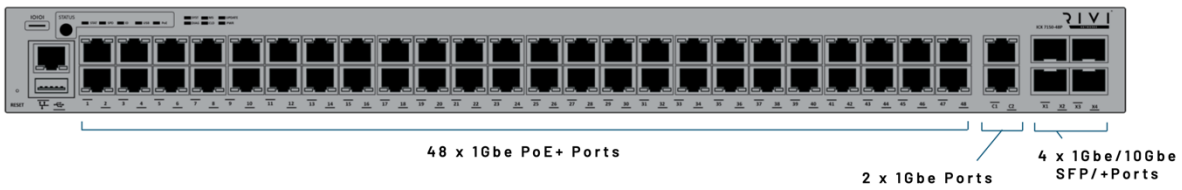
ICX7150-24 (24 x 1Gbe, 2 x 1Gbe, 4 xSFP/SFP+)



ICX7150-24P



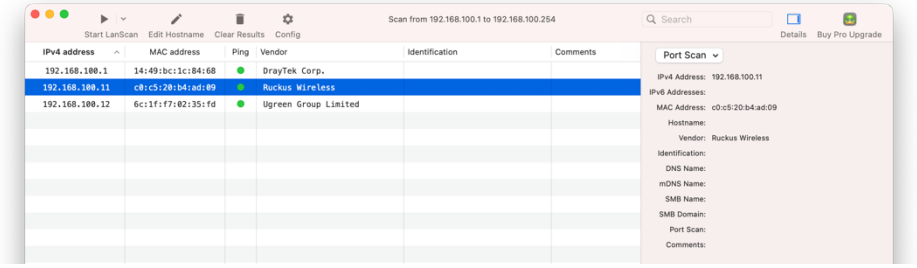
ICX7150-48P



Getting Started – Web Interface

RIVI Switches are shipped with the default IP Configuration as DHCP.

Use an IP Scanner like **Advanced IP Scanner** (Windows) or **LanScan** (macOS) to find the IP Address of the switch.

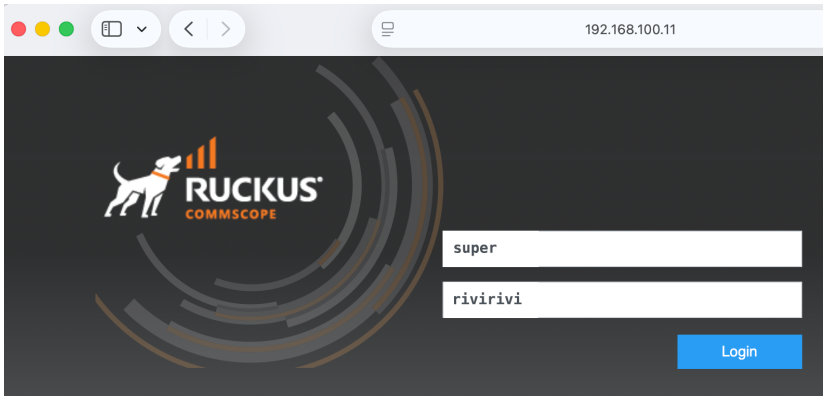


In a browser address bar, type in the IP Address of the switch (in Chrome or Safari you may need to use the prefix **https://**

Eg: **https://192.168.100.11 (enter)**

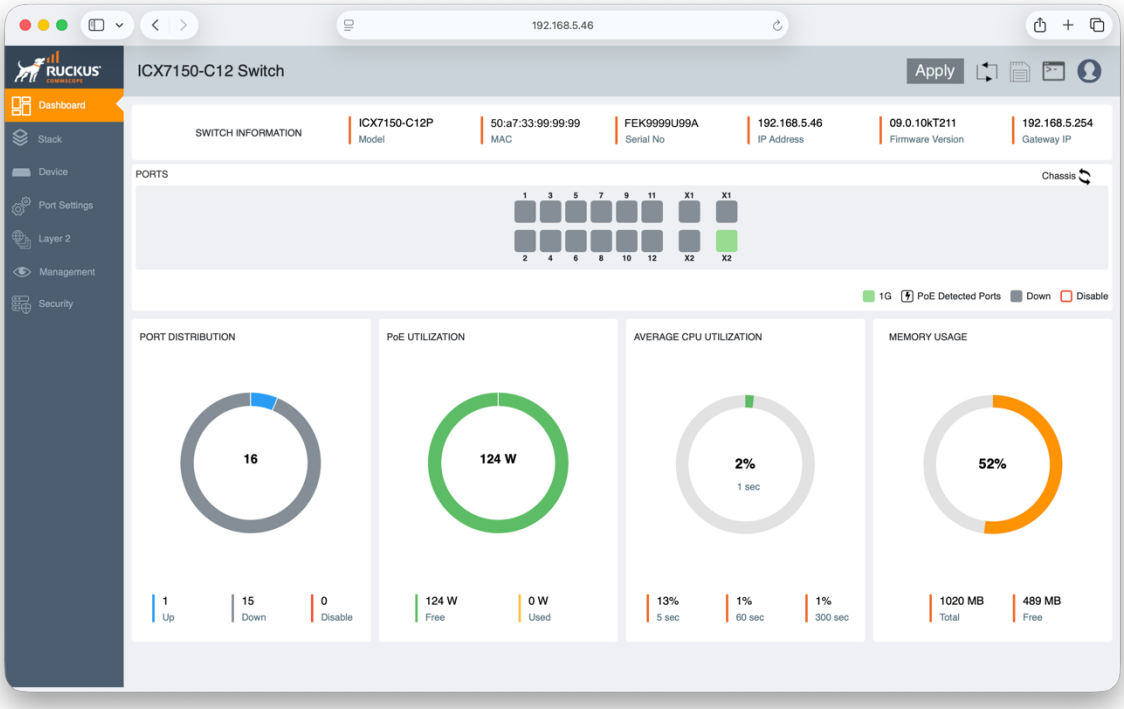
When accessing the switch web interface using HTTPS, a warning appears because the switch uses a default self-signed SSL certificate, which browsers do not automatically trust; this is normal—simply confirm the warning and proceed, or install a trusted certificate to eliminate the message.

Your switch will have usually have been preconfigured. At the username/password prompt, use **super** and **rivirivi:**



IMPORTANT: Switches that are in a factory reset condition have the username **super** and password **sp-admin**. After these credentials have been used the first time you will be prompted to change the password.

The **Switch Dashboard** will now load in the Web GUI:



The **Switch Information** pane provides details of the switch model, MAC Address, Serial Number and Firmware version, along with the IP Address and Gateway IP Address.

The **Ports** pane shows connected devices, port connection speed and PoE (if used).

The **Circular Charts** pane shows port distribution and PoE availability, along with CPU Utilisation and Memory Usage.

Switch Configuration

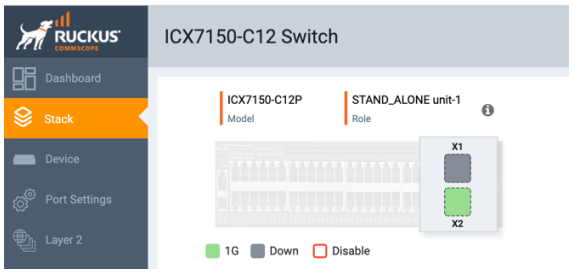
IP Address and Gateway

Since the Web interface requires access to the switch via its IP Address, it is not possible to change the IP Address or Gateway using this interface. Instead, consider using IP/MAC binding in the interface of the router connected to the network.

For Draytek Routers, this is referred to as **Bind IP to MAC** under the **LAN** menu.

The IP Address and Gateway of the switch can also be fixed using the Command Line Interface (CLI) using a serial or SSH connection, or via the RIVI Switch Configuration Utility.

Stack



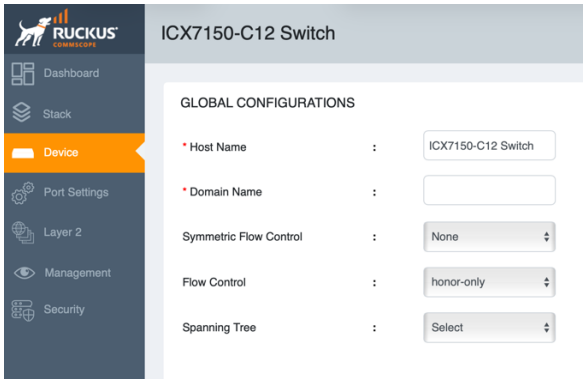
RIVI ICX Switches can be stacked up to 12 units.

This means that, rather than having a separate IP Address and interface for each switch, they can all be accessed from the “Stack Master” IP Address.

For more information see the **RIVI ICX Switch stacking guide**.

The **Stack** menu in the RIVI switch will show the number of units connected in the stack and the port status.

Device



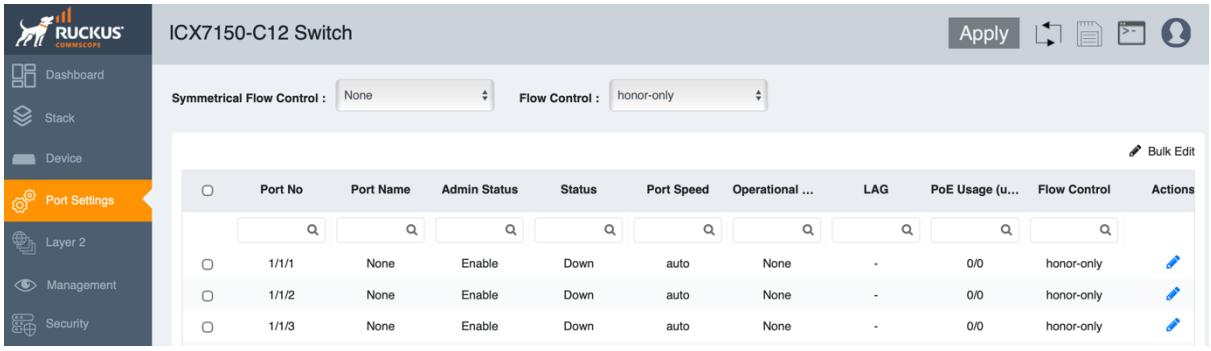
The **Device** menu is for Global Configuration of the switch and used to set the Host Name and (optionally) Domain Name of the switch.

By default this is set to the switch description. It is recommended to change this to a name and location of the switch, e.g.: Living Room Switch 1.

The Symmetric Flow Control and Flow Control options should be left set to **None** and **honor-only** respectively. These should only be changed if advised by a support engineer.

Spanning Tree can be set to either **single** or **path-cost method**. It should only be set when spanning tree is enabled. In modern networks the best setting is **path-cost method**.

Port Settings

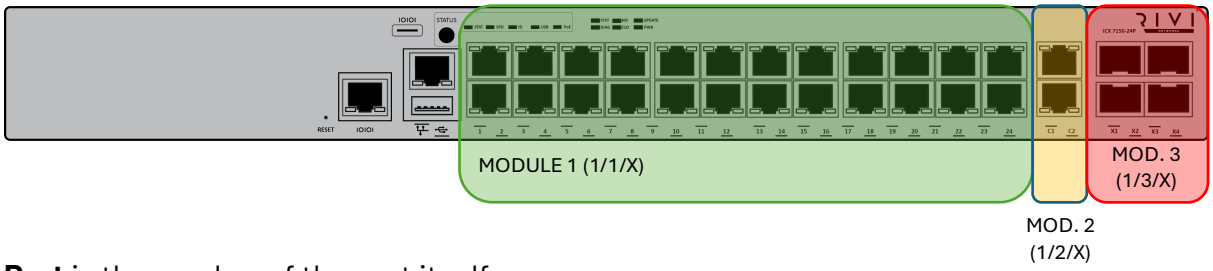


The **Port Settings** menu is used to edit the configuration of ports individually.

Ports are referred to numerically as **Switch/Module/Port Number**:

Switch refers to the number of the switch when it is part of a stack. If the switch is not in a stack the switch number is **1**.

Module refers to the block of ports. Most commonly **Module 1** is the main (usually PoE on PoE switches) module, Module 2 is the secondary (e.g. Copper Uplink) module, and Module 3 is the SFP/+ (usually Fibre) module:



Port is the number of the port itself.

So Port No. **1/1/5** would be port **5** in the main bank of ports in a standalone switch.

Port Name is used to identify the port. Labeling each port simplifies remote network diagnostics by clearly indicating what is connected where.

Admin Status shows whether the port is enabled or not.

Status shows whether something is connected to the port or not.

Port Speed shows how the port is configured. **auto** is the default setting.

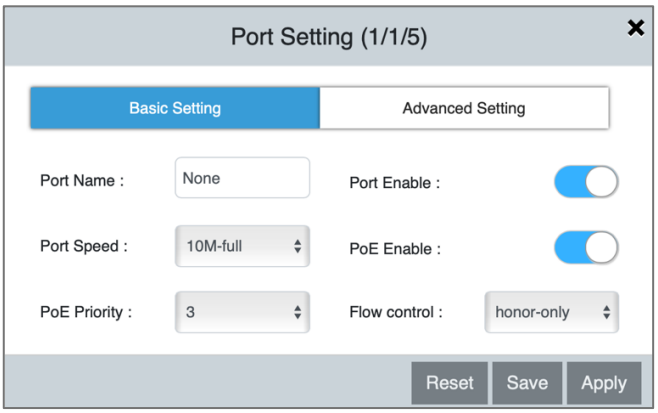
Operational Speed shows the speed that the port is running at. E.g. **1G-full** means that the port is running in 1 Gigabit full-duplex mode.

LAG indicates whether the port is part of a **Link Aggregation Group**.

PoE Usage shows the PoE setting for the port and what is being drawn by the attached device.

Flow Control is set to **honor-only** and should only be changed if advised to by a support engineer.

The ✎ **Pencil** icon in the **Actions** column is used to edit ports individually. The ✎ **Bulk Edit** icon can be used to edit multiple ports selected from the selection box column:



Port Setting Edit Box

The **Port Speed** setting is used to override the port's auto-negotiation feature, forcing a specific speed and duplex mode. This should only be changed on the advice of a support engineer. Manual overrides are typically required only for compatibility with legacy network devices or to resolve negotiation issues.

The **PoE Priority** setting determines which ports receive power first if the switch's total PoE capacity is exceeded. Lower numbers (e.g., **1**) have higher priority and retain power before higher numbers.

Use the **Port Enable** and **PoE Enable** switches to turn each port or its power on or off. Disabling and then re-enabling a port will force DHCP-enabled devices to reconnect and request a new IP address. This is useful for troubleshooting devices that fail to connect or do not obtain an IP address.

Use the **Apply** button to immediately apply the settings, or **save** to save them for when the switch next restarts.

Note: For changes to take effect immediately and persist after a reboot, first click Apply, then use the 🖹 Save icon at the top right of the Web UI to write the changes to the startup configuration.

Layer 2

LAG

The **LAG** page is used to create Link Aggregation Groups, where multiple ports can be assigned to a LAG, enabling high bandwidth links between switches.

Note: A **LAG (Link Aggregation Group)** increases total bandwidth, but each device or data stream is limited to the capacity of a single member port. For example, in a LAG of four gigabit ports, total bandwidth is 4 Gbps, but any single stream is limited to 1 Gbps.

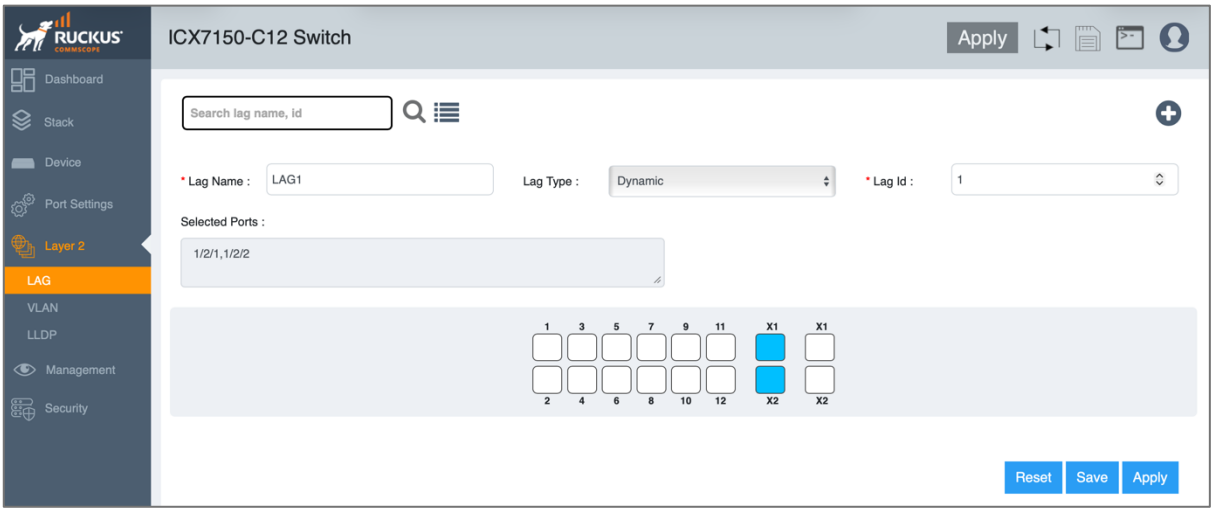
RIVI switches offer three types of Link Aggregation Groups (LAGs) to bundle multiple physical ports into a single logical link, increasing bandwidth and providing redundancy.

Static LAG: This is a basic configuration that requires manual setup on both ends of the link. It does not use a protocol to verify the connection, so it can be less reliable if misconfigured or if a one-way failure occurs. It is primarily used for compatibility with devices that do not support LACP.

Dynamic LAG (LACP): This is the recommended method. It uses the Link Aggregation Control Protocol (LACP) to automatically negotiate, create, and maintain the LAG between compatible devices. If a link within the group fails, LACP dynamically removes it from the LAG, ensuring traffic is rerouted over the remaining active links with no service interruption.

Keep-alive LAG: This type is designed for situations where one device is not LACP-compatible. It offers more reliability than a static LAG by monitoring link status, but it is not as dynamic as an LACP-based LAG.

Setting up a LAG Group



RIVI switches support up to 128 LAG groups, each with up to 16 member ports. Create multiple LAG groups only if you need to separate traffic by VLAN or require multiple switch-to-switch connections.

Use the ⊕ icon to create a new LAG group.

In the Lag Name: box use a suitable name (e.g. LAG1)

Set the Lag Type (Dynamic Recommended) and LAG ID (e.g. 1)

Click Apply and then Save the Running Config using the **Save** icon at the top right of the Web UI.

Repeat the process for the other connected switch.

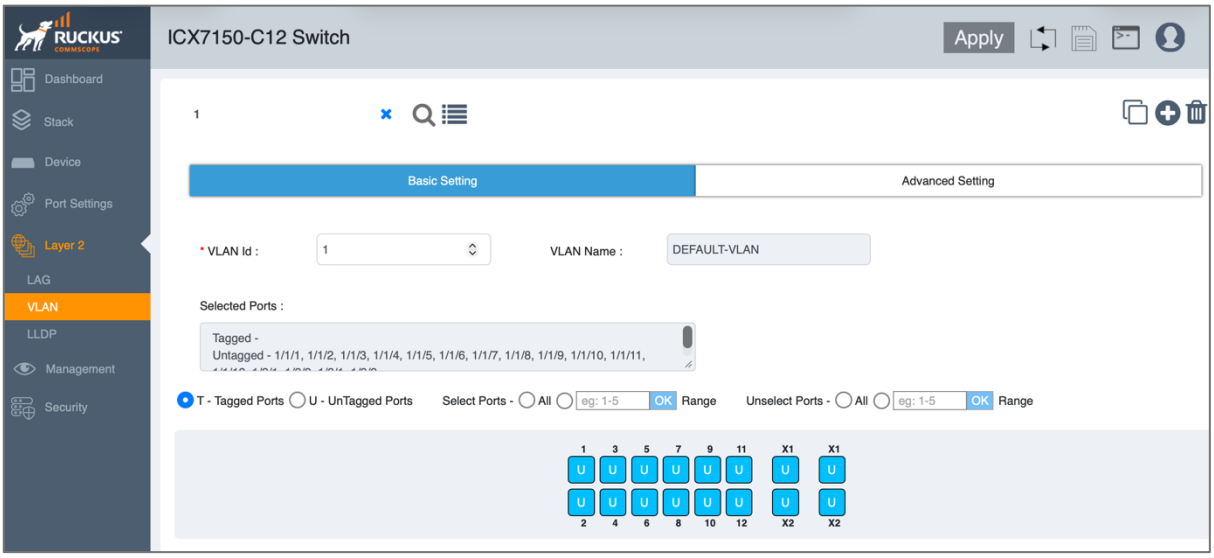
VLAN

The **VLAN** page is used to create and edit VLANs.

By default, all ports on a RIVI switch are members of VLAN1. If a port is set as untagged in another VLAN, it is removed from VLAN1 untagged membership automatically.

You should **not attempt to edit or delete** VLAN1.

Creating a VLAN in the switch



1. Use the ⊕ icon to start the process of creating a new VLAN.

2. In the VLAN Id: box use a suitable VLAN number (e.g. 10)
   Note that the VLAN Id number will also be the tagged value if you tag a VLAN

3. Enter a name for the VLAN in the VLAN Name: box (e.g. Dante)

4. Click the U – UnTagged Ports button and select the ports that should be allocated as untagged.
   Note that only one VLAN may be untagged per port.

5. Click the T – Tagged Ports button and select the ports that should be allocated as tagged.
   Note that a port may contain multiple VLAN tags.

6. Click the Apply and then Save the Running Config using the 💾 Save icon at the top right of the Web UI.

Repeat the process for the required VLANs.

Editing or Deleting VLANs

1. Use the icon to display a list of configured VLANs.
2. From the drop-down list, choose the VLAN to edit or delete.
3. To delete the VLAN click the icon.
4. To change port membership, use the T - Tagged ports and U – Untagged ports buttons and select or deselect the ports required.
5. Click Apply and then Save the Running Config using the **Save** icon at the top right of the Web UI.

LLDP

The LLDP page is used to create to enable and display Link Local Discovery Protocol information.

LLDP is enabled by default on RIVI ICX 7150 switches, allowing the device to automatically share and receive network information with directly connected devices.

When an LLDP-capable device is connected, an icon appears above or below the port; hover over the icon to view details about the detected device.

Management

Infra

The **Infra** page is used to manage the switch. From here it is possible to upgrade firmware in the two storage partitions of the switch, backup and restore configurations, and save logs for support engineers.

Firmware Upgrade: Use this section to upgrade the firmware. This is only advised if recommended by a network support engineer.

Configuration Update: Use this section to back up the running configuration for your records or support, or to restore a configuration from an archive or a file provided by a network engineer.

Configuration files use the .txt format, so they can be easily viewed and edited in any common text editor.

Configuration Archive: It is possible to save and manage multiple configurations using this function.

Syslog

The **Syslog** page contains a continual running log of activities on the switch. It is useful for diagnosis of network issues.

Note: Syslog events are time-stamped, so it is essential to configure the switch with the correct time zone and ensure accurate time - either manually or by connecting to an NTP server.

DNS Server

The **DNS Server** page lists the DNS servers the switch uses to resolve Internet domains, such as when contacting an NTP server for time synchronization. Do not change these settings unless directed by a network support engineer.

Smart Zone

If the RIVI ICX switch is managed by a SmartZone network, the Smart Zone page must be configured with the Active IP addresses of the SmartZone controllers.

There is no need to change any parameters on this page unless directed to do so by a network support engineer.

Polling Interval

The Polling Interval page sets how often the switch polls and reports various network parameters. Do not change these settings unless instructed by a network support engineer.

Security

AAA Servers

The **AAA Servers** page is used to manage users of the switch.

The **Local Users** tab is used to edit and add users to the switch.

The **AAA Servers** tab lets you configure external servers (like RADIUS or TACACS+) to authenticate users, control access, and log network activity on the switch.

The **AAA Settings** tab is used to configure how the switch prioritizes and uses different authentication, authorization, and accounting methods.

This includes:

- Setting the order of preference (priority) for external servers (RADIUS, TACACS+) and local authentication.
- Selecting which methods are used for login authentication, command authorization, and accounting.
- Assigning privilege levels for different types of access or commands.

ACL

The **ACL** page is used to manage Access Control Lists (IPv4 and IPv6).

An **ACL** is a set of rules used to allow or deny specific network traffic based on criteria like source/destination IP address, MAC address, or protocol type.

Creating an ACL

1. **Use** the ⊕ to display the Add Access List dialog box.

2. **In the** Name/ID: Enter a unique ACL name or number.

3. Select **Standard** from the list to create a standard IPv4 ACL.

4. For **Rules**, select ⊕ to add ACL rules with the following parameters:

5. **Seq**: Assign a sequence number to the ACL rule.
6. **Action**: Select **permit** or **deny** from the list to filter the traffic according to the rules.
7. **Network**: Enter the source IP address.

8. Select **Apply** to create the standard IPv4 ACL.

Create additional ACLs to permit or block traffic, as required.