Configure and Monitor Omada Managed Devices

CONTENTS

1.Configure and Monitor Omada Managed Devices

❤ 1. 1 Introduction to the Devices Page

Overview

The Devices page displays all TP-Link devices discovered by the controller and their general information.

For an easy monitoring of the devices, you can customize the column and filter the devices for a better overview of device information. Also, quick operations and Batch Edit are available for configurations.

DEVICE NAME	IP ADDRESS	STATUS	MODEL	VERSION ⬆	UPTIME	ACTION
	192.168.0.1	CONNECTED	ER605 v2.0	2.0.0	23h 16m 25s	⏻
	192.168.0.103	CONNECTED	TL-SG2210MP v1.0	1.0.3	15day(s) 5h 1m 2...	◉ ⏻
	--	PENDING 📶	EAP245 v4.0	--		⊘
	--	MANAGED BY OTHERS 📶	EAP670 v1.0	--		⊘
	192.168.0.101	CONNECTED	EAP235-Wall(US) v1.0	3.1.0	22h 31m 24s	◉ ⏻
	--	MANAGED BY OTHERS 📶	EAP225 v3.0	--		⊘
	192.168.0.100	CONNECTED	EAP265 HD(EU) v1.0	5.0.4	22h 25m 50s	◉ ⏻
	192.168.0.105	CONNECTED 📶	EAP225-Outdoor(EU) v1.0	5.0.7	21h 39m 59s	◉ ⏻

Showing 1-8 of 8 records   ‹ 1 ›   10 /page   Go To page: GO

According the connection status, the devices have the following status: Pending, Isolated, Connected, Managed by Others, Heartbeat Missed, and Disconnected. The icons in the Status column are explained as follows:

PENDING	The device is in Standalone Mode or with factory settings, and has not been adopted by the controller. To adopt the device, click ⊘, and the controller will use the default username and password to adopt it. When adopting, its status will change from Adopting, Provisioning, Configuring, to Connected eventually.
ISOLATED	(For APs in the mesh network) The AP once managed by the controller via a wireless connection now cannot reach the gateway. You can rebuild the mesh network by connecting it to an AP in the Connected status, then the isolated AP will turn into a connected one. For detailed configuration, refer to Mesh.
CONNECTED	The device has been adopted by the controller and you can manage it centrally. A connected device will turn into a pending one after you forget it.
MANAGED BY OTHERS	The device has already been managed by another controller. You can reset the device or provide the username and password to unbind it from another controller and adopt it in the current controller.

HEARTBEAT MISSED	A transition status between Connected and Disconnected.
	Once connected to the controller, the device will send inform packets to the controller in a regular interval to maintain the connection. If the controller does not receive its inform packets in 30 seconds, the device will turn into the Heartbeat Missed status. For a heartbeat-missed device, if the controller receives an inform packet from the device in 5 minutes, its status will become Connected again; otherwise, its status will become Disconnected.
DISCONNECTED	The connected device has lost connection with the controller for more than 5 minutes.
🛜	(For APs in the mesh network) When this icon appears with a status icon, it indicates the EAP with mesh function and no wired connection is detected by the controller. You can connect it to an uplink AP through Mesh.
≡↕	When this icon appears with a status icon, it indicates the device in the Connected, Heartbeat Missed, Isolated, or Disconnected status is migrating. For more information about Migration, refer to 5. 4 Migration.

Configuration

■ **Customize the Column**

To customize the columns, click ⋮ next to Action and check the boxes of information type.

To change the list order, click the column head and ⬍ will appear to indicate the ascending or descending order.

■ **Filter the Devices**

Use the search box and tab bar above the table to filter the devices.

To search the devices, enter the text in the search box or select a tag from the drop-down list. As for the device tag, refer to the general configuration of switches and EAPs.

To filter the devices, a tab bar [All | Gateway/Switches | APs] is above the table to filter the devices by device type. You can also filter the devices by their status by clicking ▼ in the Status colum.

If you select the APs tab, another tab bar [Overview | Mesh | Performance | Config] will be available to change the column quickly.

Overview	Displays the device name, IP address, status, model, firmware version, uptime, channel, and Tx power by default.
Mesh	Displays the information of devices in the mesh network, including the device name, IP address, status, model, uplink device, channel, Tx power, and the number of downlink devices, clients and hops by default.
Performance	Displays the device name, IP address, status, uptime, channel, Tx power, the number of 2.4 GHz and 5 GHz clients, Rx rate, and Tx rate by default.
Config	Displays the device name, status, version, WLAN group, and the radio settings for 2.4 GHz and 5 GHz by default.

■ **Quick Operations**

Click the icons in Header or the Action column to quickly adopt, locate, upgrade, or reboot the device.

Start Rolling Upgrade	Click to upgrade the managed devices in batches.
⬆	Click to check if there is new firmware for the managed devices.
⊘	(For pending devices) Click to adopt the device.
◉	(For connected switches and APs) Click this icon and the LEDs of the device will flash to indicate the device's location. The LEDs will keep flashing for 10 minutes, or you can click the ▣ icon to stop the flashing.
⏻	(For connected devices) Click to reboot the device.
⬆	Click to upgrade the device's firmware version. This icon appears when the device has a new firmware version.

■ **Batch Edit (for Switches and EAPs)**

After selecting the Gateway/Switches or APs tab, you can adopt or configure the switches or EAPs in batches. Batch Config is available only for the devices in Connected/Disconnected/Heartbeat

Missed/Isolated status, while Batch Adopt is available for the devices in the Pending/Managed By Others status.

Click Batch Action. select Batch Adopt, click the checkboxes of devices, and click Done. If the selected devices are all in the Pending status, the controller will adopt then with the default username and password. If not, enter the username and password manually to adopt the devices.

Click Batch Action, select Batch Config, click the checkboxes of devices, and click Done. Then the Properties window appears. There are two tabs in the window: Devices and Config.

In Devices, you can click ✕ to remove the device from the current batch configuration.

In Config, all settings are Keep Existing by default. For detailed configurations, refer to the configuration of switches and EAPs.

⟩	Click to minimize the Properties window to an icon. To reopen the minimized Properties window, click ▯.
▢	Click to maximize the Properties window. You can also use the icon on pages other than the Devices page.
✕	Click to close the Properties window of the chosen device(s). Note that the unsaved configuration will be lost.
⋯ 2	The number on the lower-right shows the number of devices in the batch configuration.

◆ 1. 2 Configure and Monitor the Gateway

In the Properties window, you can configure the gateway managed by the controller and monitor the performance and statistics. By default, all configurations are synchronized with the current site.

To open the Properties window, click the entry of a router. A monitor panel and several tabs are listed in the Properties window. Most features to be configured are gathered in the Config tab, such as IP, SNMP, and Hardware Offload, while other tabs are mainly used to monitor the devices.

ⓘ Note:

- You can adopt only one router in one site.

- The available functions in the window vary due to the model and status of the device.

1. 2. 1   Configure the Gateway

In the Properties window, you can view and configure the ports in Ports, and configure the gateway features in Config.

■ **Ports**

In Ports, you can view the status and edit settings of the ports.

To configure a port, click ☑ in the table.

Link Speed	Select the speed mode for the port.
	Auto: The port negotiates the speed and duplex automatically.
	Manual: Specify the speed and duplex from the drop-down list manually.
Mirroring	Mirroring is used to analyze network traffic and troubleshoot network problems.
	Enable this option to set the edited port as the mirroring port, then specify one or multiple mirrored ports. The gateway will sends a copy of traffics passing through the mirrored ports to the mirroring port.
Mirror Mode	Specify the directions of the traffic to be mirrored.
	Ingress and Egress: Both the incoming and outgoing packets through the mirrored port will be copied to the mirroring port.
	Ingress: The packets received by the mirrored port will be copied to the mirroring port.
	Egress: The packets sent by the mirrored port will be copied to the mirroring port.

In the Properties window, click Config and then click the sections to configure the features applied to the router, including general settings, SNMP, and advanced functions.

■ **General**

In General, you can specify the device name and LED settings of the router.

Name	Specify a name of the device.
LED	Select the way that device's LEDs work.
	Use Site Settings: The device's LED will work following the settings of the site. To view and modify the site settings, refer to 4. 2. 2 Services.
	On/Off: The device's LED will keep on/off.
Longitude / Latitude / Address	Configure the parameters according to where the site is located. These fields are optional.

■ **Services**

In Services, you can configure SNMP to write down the location and contact detail. You can also click Manage to jump to Settings > Services > SNMP, and for detailed configuration of SNMP service, refer to 4. 10. 4 SNMP.

■ **Advanced**

In Advanced, you can configure Hardware Offload, LLDP (Link Layer Discovery Protocol) and Echo Server to make better use of network resources.

Hardware Offload	Hardware Offload can improve performance and reduce CPU utilization by using the hardware to offload packet processing. Note that this feature cannot take effect if QoS, Bandwidth Control, or Session Limit is enabled. To configure Bandwidth Control and Session Limit for the router, refer to 4. 6 Transmission.
LLDP	LLDP can help discover devices.
Echo Server	Echo Server is used to test the connectivity and monitor the latency of the network automatically or manually. If you click Custom, enter the IP address or hostname of your custom server.

■ **Manage Device**

In Manage Device, you can upgrade the device's firmware version manually, move it to another site, synchronize the configurations with the controller, and forget the router.

Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. When upgrading, the device will be reboot and readopted by the controller. You can also check the box of Upgrade all devices of the same model in the site after the firmware file is uploaded.
Move to Site	Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.
Force Provision	Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.
Forget	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.

■ **Common Settings**

In Common Settings, you can click the path to jump to corresponding modules quickly.

Common Settings   ≪

Settings->Wired Networks->Internet

To configure the network of the WAN port, go to the **Settings->Wired Networks->Internet** page.

Settings->Wired Networks->LAN

To view and configure the settings of the network interfaces, go to the **Settings->Wired Networks->LAN** page.

Settings->VPN

To view and configure the VPN network, go to the **Settings->VPN** page.

Settings->Network Security

To view and configure the Firewall and ACL rules for the network, go to the **Settings->Network Security** page.

Settings->Transmission->Routing

To view and configure Routing on the gateway, go to the **Settings->Transmission->Routing** page.

Settings->Transmission->NAT

To view and configure NAT on the gateway, go to the **Settings->Transmission->NAT** page.

Settings->Services

To view and configure the network services, go to the **Settings->Services** page.

1. 2. 2   Monitor the Gateway

One panel and three tabs are provided to monitor the device in the Properties window: Monitor Panel, Details, Networks, and Statistics.

14

Monitor Panel

The monitor panel displays the router's ports, and it uses colors and icons to indicate different connection status and port types. When the router is pending or disconnected, all ports are disabled.

You can hover the cursor over the port icon for more details.

Details

In Details, you can view the basic information of the router and statistics of WAN ports to know the device's running status briefly.

■ **Overview**

In Overview, you can view the basic information of the device. The listed information varies due to the device's status.

■ **SFP WAN/WAN/USB Modem**

In SFP WAN/WAN/USB Modem, you can view the basic information and statistics of the WAN port, such as the IP address, speed, duplex, and upload and download traffic. You can also click Connect or Disconnect to manually turn on/off the internet.

Networks

In Networks, you can view the network information of the router, including the Network name, IP address, transmitted and received traffics of LAN interfaces in the network, and number of clients.

Network	IP Address	Tx Bytes	Rx Bytes	Clients
LAN	192.168.0.1	596.1 MB	1.0 GB	0

Statistics

In Statistics, you can monitor the CPU and memory of the device in last 24 hours via charts. To view statistics of the device in a certain period, click the chart to jump to 8. 2 View the Statistics of the Network.

◆ 1.3 Configure and Monitor Switches

In the Properties window, you can configure one or some switches connected to the controller and monitor the performance and statistics. Configurations changed in the Properties window will be applied only to the selected switch(es). By default, all configurations are synchronized with the current site.

To open the Properties window, click the entry of a switch, or click Batch Action, and then Batch Config to select switches for batch configuration. A monitor panel and several tabs are listed in the Properties window. Most features to be configured are gathered in the Ports and Config tab, such as the port mirroring, IP address, and Management VLAN, while other tabs are mainly used to monitor the devices.

ⓘ Note:

- The available functions in the window vary due to the model and status of the device.

- In Batch Config, you can only configure the selected devices, and the unaltered configurations will keep the current settings.

1.3.1   Configure Switches

In the Properties window, you can view and configure the profiles applied to ports in Ports, and in Config, you can configure the switch features.

Ports

Port and LAG are two tabs designed for physical ports and LAGs (Link Aggregation Groups), respectively. Under the Port tag, all ports are listed but you can configure physical ports only, including overriding the applied profiles, configuring Port Mirroring, and specifying ports as LAGs. Under the LAG tag, all LAGs are listed and you can view and modify the configurations of existing LAGs.

■ **Port**

In Port, you can view and configure all ports' names and applied profiles.

	#	Name	Status	Profile	ACTION ⋮
☐	1	Port1	■	All	✎
☐	2	Port2	■	All	✎
☐	3	Port3	■	All	✎ ⏻
☐	4	Port4	■	All	✎
☐	5	Port5	■	All	✎
☐	6	Port6	■	All	✎
☐	7	Port7	■	All	✎
☐	8	Port8	■	All	✎
☐	9	Port9	■	All	✎
☐	10	Port10	■	All	✎

Status	Displays the port status in different colors.
	■: The port profile is Disabled. To enable it, click ✎ to change the profile.
	■: The port is enabled, but no device or client is connected to it.
	■: The port is running at 1000 Mbps.
	■: The port is running at 10/100 Mbps.
Profile	Displays the profile applied to the port.
Action	✎: Click to edit the port name and configure the profile applied to the port.
	⏻: (For PoE ports) Click to reboot the connected powered devices (PDs).

19

To configure a single port, click ✎ in the table. To configure ports in batches, click the checkboxes and then click Edit Selected. Then you can configure the port name and profile. By default, all settings are Keep Existing for batch configuration.

Edit Port1

Name:

Port1

Profile:

All ∨   Manage Profiles

☐ Profile Overrides

Apply   **Cancel**

Name	Enter the port name.
Profile	Select the profile applied to the port from the drop-down list. Click Manage Profiles to jump to view and manage profiles. For details, refer to 4. 3 Configure Wired Networks.
Profile Overrides	Click the checkbox to override the applied profile. The parameters to be configured vary in Operation modes,

With Profile Overrides enabled, select an operation mode and configure the following parameters to override the applied profile, configure a mirroring port, or configure a LAG.

- Override the Applied Profile

    If you select Switching for Operation, configure the following parameters and click Apply to override the applied profile. To discard the modifications, click Remove Overrides and all profile configurations will become the same as the applied profile.

Edit Port1

Name:

Port1

Profile:

All ⌄   Manage Profiles

☑ Profile Overrides

Operation:

◉ Switching

◯ Mirroring   ⓘ

◯ Aggregating

PoE Mode:

◯ Off

◉ 802.3at/af

802.1X Control:

◯ Auto

◉ Force Authorized

◯ Force Unauthorized

Link Speed:

◯ Auto

◉ Manual

Auto / Auto ⌄

Port Isolation: ☐ Enable ⓘ

Flow Control: ☐ Enable

EEE: ☐ Enable

Loopback Control:

◯ Off

◯ Loopback Detection Port Based

◉ Loopback Detection VLAN Based

◯ Spanning Tree

LLDP-MED: ☑ Enable

Bandwidth Control: ⓘ

◉ Off

◯ Rate Limit

◯ Storm Control

DHCP L2 Relay: ☑ Enable

Format:

Normal ⌄

Circuit ID:

[   ] (Optional)

Remote ID:

[   ] (Optional)

Apply   **Cancel**   **Remove Overrides**

22

PoE Mode	(Only for PoE ports) Select the PoE (Power over Ethernet) mode for the port.
	Off: Disable PoE function on the PoE port.
	802.3at/af: Enable PoE function on the PoE port.
802.1X Control	Select 802.1X Control mode for the ports. To configure the 802.1X authentication globally, go to Settings > Authentication > 802.1X.
	Auto: The port is unauthorized until the client is authenticated by the authentication server successfully.
	Force Authorized: The port remains in the authorized state, sends and receives normal traffic without 802.1X authentication of the client.
	Force Unauthorized: The port remains in the unauthorized state, and the client connected to the port cannot authenticate with any means. The switch cannot provide authentication services to the client through the port.
Link Speed	Select the speed mode for the port.
	Auto: The port negotiates the speed and duplex automatically.
	Manual: Specify the speed and duplex from the drop-down list manually.
Port Isolation	Click the checkbox to enable Port Isolation. An isolated port cannot communicate directly with any other isolated ports, while the isolated port can send and receive traffic to non-isolated ports.
Flow Control	With this option enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion.
EEE	Click the checkbox to enable EEE (Energy Efficient Ethernet) to allow power reduction.
Loopback Control	Loopback refers to the routing of data streams back to their source in the network. You can disable loopback control for the network or choose a method to prevent loopback happening in your network.
	Off: Disable loopback control on the port.
	Loopback Detection Port Based: Loopback Detection Port Based helps detect loops that occur on a specific port. When a loop is detected on a port, the port will be blocked.
	Loopback Detection VLAN Based: Loopback Detection VLAN Based helps detect loops that occur on a specific VLAN. When a loop is detected on a VLAN, the VLAN will be blocked.
	Spanning Tree: Select STP (Spanning Tree Protocal) to prevent loops in the network. STP helps block specific ports of the switches to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology. To make sure Spanning Tree takes effect on the port, go to the Config tab and enable Spanning Tree on the switch.

LLDP-MED	Click the checkbox to enable LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) for device discovery and auto-configuration of VoIP (Voice over Internet Protocol) devices.
Bandwidth Control	Select the type of Bandwidth Control functions to control the traffic rate and specify traffic threshold on each port to make good use of network bandwidth. Off: Disable Bandwidth Control for the port. Rate Limit: Select Rate limit to limit the ingress/egress traffic rate on each port. With this function, the network bandwidth can be reasonably distributed and utilized. Storm Control: Select Storm Control to allow the switch to monitor broadcast frames, multicast frames and UL-frames (Unknown unicast frames) in the network. If the transmission rate of the frames exceeds the specified rate, the frames will be automatically discarded to avoid network broadcast storm.
Ingress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.
Egress Rate Limit	When Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port.
Broadcast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving broadcast frames. The broadcast traffic exceeding the limit will be processed according to the Action configurations.
Multicast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving multicast frames. The multicast traffic exceeding the limit will be processed according to the Action configurations.
Unknown Unicast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving unknown unicast frames. The traffic exceeding the limit will be processed according to the Action configurations.
Action	When Storm Control selected, select the action that the switch will take when the traffic exceeds its corresponding limit. Drop: With Drop selected, the port will drop the subsequent frames when the traffic exceeds the limit. Shutdown: With Shutdown selected, the port will be shutdown when the traffic exceeds the limit.
Recover Time	With Shutdown selected as the Action, specify the recover time, and the port will be opened after the specified time.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network.
Format	Select the format of option 82 sub-option value field. Normal: The format of sub-option value field is TLV (type-length-value). Private: The format of sub-option value field is just value.

24

Circuit ID	(Optional) Enter the customized circuit ID. The circuit ID configurations of the switch and the DHCP server should be compatible with each other. If it is not specified, the switch will use the default circuit ID when inserting Option 82 to DHCP packets.
Remote ID	(Optional) Enter the customized remote ID. The remote ID configurations of the switch and the DHCP server should be compatible with each other. If it is not specified, the switch will use its own MAC address as the remote ID.

- Configure a Mirroring Port

  If you select Mirroring as Operation, the edited port can be configured as a mirroring port. Specify other ports as the mirrored port, and the switch sends a copy of traffics passing through the mirrored port to the mirroring port. You can use mirroring to analyze network traffic and troubleshoot network problems.

  To configure Mirroring, select the mirrored port or LAG, specify the following parameters, and click Apply. To discard the modifications, click Remove Overrides and all profile configurations become the same as the applied profile.

Note that the mirroring ports and the member ports of LAG cannot be selected as mirrored ports.

PoE Mode	(Only for PoE ports) Select the PoE mode for the port.
	Off: Disable PoE on the PoE port.
	802.3at/af: Enable PoE on the PoE port.
Link Speed	Select the speed mode for the port.
	Auto: The port negotiates the speed and duplex automatically.
	Manual: Specify the speed and duplex from the drop-down list manually.

Bandwidth Control	Bandwidth control optimizes network performance by limiting the bandwidth of specific sources.

Off: Disable bandwidth control on the port.

Rate Limit: Enable bandwidth control on the port, and you need to specify the ingress and/or egress rate limit. |
| Ingress Rate Limit | With Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port. With this function, the network bandwidth can be reasonably distributed and utilized. |
| Egress Rate Limit | With Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port. With this function, the network bandwidth can be reasonably distributed and utilized. |

- Configure a LAG

    If you select Aggregating as Operation, you can aggregate multiple physical ports into a logical interface, which can increase link bandwidth and enhance the connection reliability.

    💡 Configuration Guidelines:

    - Ensure that both ends of the aggregation link work in the same LAG mode. For example, if the local end works in LACP mode, the peer end should also be set as LACP mode.

    - Ensure that devices on both ends of the aggregation link use the same number of physical ports with the same speed, duplex, jumbo and flow control mode.

    - A port cannot be added to more than one LAG at the same time.

    - LACP does not support half-duplex links.

    - One static LAG supports up to eight member ports. All the member ports share the bandwidth evenly. If an active link fails, the other active links share the bandwidth evenly.

    - One LACP LAG supports multiple member ports, but at most eight of them can work simultaneously, and the other member ports are backups. Using LACP protocol, the switches negotiate parameters and determine the working ports. When a working port fails, the backup port with the highest priority will replace the faulty port and start to forward data.

    - The member port of an LAG follows the configuration of the LAG but not its own. Once removed, the LAG member will be configured as the default All profile and Switching operation.

    - The port enabled with Port Security, Port Mirror, MAC Address Filtering or 802.1X cannot be added to an LAG, and the member port of an LAG cannot be enabled with these functions.

    To configure a new LAG, select other ports to be added to the LAG, specify the LAG ID, and choose a LAG type. Click Apply. To discard the modifications, click Remove Overrides and all

profile configurations become the same as the applied profile. For other parameters, configure them under the LAG tab.

LAG ID	Specify the LAG ID of the LAG. Note that the LAG ID should be unique.
	The valid value of the LAG ID is determined by the maximum number of LAGs supported by your switch. For example, if your switch supports up to 14 LAGs, the valid value ranges from 1 to 14.
Static LAG	In Static LAG mode, the member ports are added to the LAG manually.
Active LACP/ Passive LACP	LACP extends the flexibility of the LAG configurations. In LACP, the switch uses LACPDU (Link Aggregation Control Protocol Data Unit) to negotiate the parameters with the peer end. In this way, the two ends select active ports and form the aggregation link. Active LACP: In this mode, the port will take the initiative to send LACPDU. Passive LACP: In this mode, the port will not send LACPDU before receiving the LACPDU from the peer end.

- **LAG**

  LAGs (Link Aggregation Groups) are logical interfaces aggregated, which can increase link bandwidth and enhance the connection reliability. You can view and edit the LAGs under the LAG tab. To configure physical ports as a LAG, refer to Configure a LAG.

LAG ID	Name	Status	Ports	Profile	ACTION
1	LAG1	🟩	Port 9,Port 10	All	✏️ 🗑️

Status	Displays the status in different colors.
	⬜: The LAG profile is Disable. To enable it, click ✏️ to change the profile.
	⬛: The port is enabled, but no device or client is connected to it.
	🟩: The LAG ports are running at 1000 Mbps.
	🟧: The LAG port are running at 10/100 Mbps.
Ports	Displays the port number of LAG ports.
Profile	Displays the profile applied to the port.
Action	✏️: Click to edit the port name and configure the profile applied to the port.
	🗑️: Click to delete the LAG. Once deleted, the ports will be configured as the default All profile and Switching operation. You can configure the ports under the Port tab.

Click ☑ to configure the LAG name and the applied profile.

Edit LAG1

Name:

LAG1

Profile:

All   ∨   Manage Profiles

ⓘ   Configurations of PoE, 802.1x and LLDP-MED in
       the profile do not take effect on LAG ports.

☐ Profile Overrides

Apply   **Cancel**

Name	Enter the port name.
Profile	Select the profile applied to the port from the drop-down list. Click Manage Profiles to jump to view and manage profiles. For details, refer to 4. 3 Configure Wired Networks.
Profile Overrides	Click the checkbox to override the applied profile. The parameters to be configured vary in Operation modes.

With Profile Overrides enabled, you can reselect the LAG members and configure the following parameters.

Link Speed	Select the speed mode for the port.
	Auto: The port negotiates the speed and duplex automatically.
	Manual: Specify the speed and duplex from the drop-down list manually.
Port Isolation	Click the checkbox to enable Port Isolation. An isolated port cannot communicate directly with any other isolated ports, while the isolated port can send and receive traffic to non-isolated ports.
Flow Control	With this option enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion.
EEE	Click the checkbox to enable EEE (Energy Efficient Ethernet) to allow power reduction.

Loopback Control	Loopback refers to the routing of data streams back to their source in the network. You can disable loopback control for the network or choose a method to prevent loopback happening in your network.
	Off: Disable loopback control on the port.
	Loopback Detection Port Based: Loopback Detection Port Based helps detect loops that occur on a specific port. When a loop is detected on a port, the port will be blocked.
	Loopback Detection VLAN Based: Loopback Detection VLAN Based helps detect loops that occur on a specific VLAN. When a loop is detected on a VLAN, the VLAN will be blocked.
	Spanning Tree: Select STP (Spanning Tree Protocal) to prevent loops in the network. STP helps block specific ports of the switches to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology. To make sure Spanning Tree takes effect on the port, go to the Config tab and enable Spanning Tree on the switch.
Bandwidth Control	Select the type of Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance.
	Off: Disable Bandwidth Control for the port.
	Rate Limit: Select Rate limit to limit the ingress/egress traffic rate on each port. With this function, the network bandwidth can be reasonably distributed and utilized.
	Storm Control: Select Storm Control to allow the switch to monitor broadcast frames, multicast frames and UL-frames (Unknown unicast frames) in the network. If the transmission rate of the frames exceeds the specified rate, the frames will be automatically discarded to avoid network broadcast storm.
Ingress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.
Egress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port.
Broadcast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving broadcast frames. The broadcast traffic exceeding the limit will be processed according to the Action configurations.
Multicast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving multicast frames. The multicast traffic exceeding the limit will be processed according to the Action configurations.
Unknown Unicast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving unknown unicast frames. The traffic exceeding the limit will be processed according to the Action configurations.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network.

Action	With Storm Control selected, select the action that the switch will take when the traffic exceeds its corresponding limit.
	Drop: With Drop selected, the port will drop the subsequent frames when the traffic exceeds the limit.
	Shutdown: With Shutdown selected, the port will be shutdown when the traffic exceeds the limit.
Recover Time	With Shutdown selected as the Action, specify the recover time, and the port will be opened after the specified time.

Config

In Config, click the sections to configure the features applied to the selected switch(es), including the general settings, services, and networks.

- **General**

    In General, you can specify the device name and LED settings of the switch, and categorize it via device tags.

Name	(Only for configuring a single device) Specify a name of the device.

LED	Select the way that device's LEDs work.
	Use Site Settings: The device's LED will work following the settings of the site. To view and modify the site settings, refer to 4. 2. 2 Services.
	On/Off: The device's LED will keep on/off.
Device Tags	Select a tag from the drop-down list or create a new tag to categorize the device.
Jumbo	Configure the size of jumbo frames. By default, it is 1518 bytes.
	Generally, the MTU (Maximum Transmission Unit) size of a normal frame is 1518 bytes. If you want the switch supports to transmit frames of which the MTU size is greater than 1518 bytes, you can configure the MTU size manually here.
Hash Algorithm	Select the Hash Algorithm, based on which the switch can choose the port to forward the received packets. In this way, different data flows are forwarded on different physical links to implement load balancing.
	SRC MAC: The computation is based on the source MAC addresses of the packets.
	DST MAC: The computation is based on the destination MAC addresses of the packets.
	SRC MAC+DST MAC: The computation is based on the source and destination MAC addresses of the packets.
	SRC IP: The computation is based on the source IP addresses of the packets.
	DST IP: The computation is based on the destination IP addresses of the packets.
	SRC IP+DST IP: The computation is based on the source and destination IP addresses of the packets.

■ **VLAN Interface**

In VLAN Interface, you can configure Management VLAN and different VLAN interface for the switch. The general information of the existing VLAN interface are displayed in the table.

To configure a single VLAN interface, hover the mouse on the entry and click ✎ to edit the settings.

VLAN Interface > Edit Interface   ≪

Management VLAN: ☑ Enable ⓘ

⚠ The controller will fail to manage your devices
with wrong Management VLAN configurations. If
you are not sure about your network conditions
and the potential impact of any configurations, we
recommend that you keep the default
configurations. Refer to the Configuration Guide
before you configure this feature.

IP Address Mode:

○ Static

◉ DHCP

Use Fixed IP Address: ☑ Enable

📍 Gateway Required

Network:

Please Select...   ⌄

IP Address:

____ . ____ . ____

Fallback IP Address: ☑ Enable ⓘ

Fallback IP Address:

192 . 168 . 0 . 1

Fallback IP Mask:

255 . 255 . 255 . 0

Fallback Gateway:

____ . ____ . ____   (Optional)

DHCP Option12:

_____   (Optional)

DHCP Mode:

◉ None

○ DHCP Server

○ DHCP Relay

Apply   Cancel

Management VLAN	Click the checkbox if you want to use the VLAN interface as Management VLAN. Note that the controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations.
	The management VLAN is a VLAN created to enhance the network security. Without Management VLAN, the configuration commands and data packets are transmitted in the same network. There are risks of unauthorized users accessing the management page and modifying the configurations. A management VLAN can separate the management network from the data network and lower the risks.
IP Address Mode (when Management VLAN enabled)	Select a mode for the interface to obtain its IP address, and the VLAN will communicate with other networks including VLANs with the IP address.
	Static: Assign an IP address to the interface manually, specify the IP Address and Subnet Mask for the interface.
	When the VLAN interface is set as the Management VLAN, it is optional for you to specify the Default Gateway and Primary/Secondary DNS for the interface.
	DHCP: Assign an IP address to the interface through a DHCP server.
	When you want to let device use a fixed IP address, enable Use Fixed IP Address and specify the Network and IP Address based on needs.
	When the VLAN interface is set as the Management VLAN, you can further enable Fallback IP Address, and specify the Fallback IP Address, Fallback IP Mask, and Fallback Gateway (optional). If the VLAN interface fails to get an IP address from the DHCP server, the fallback IP address will be used for the interface.
DHCP Option 12	When DHCP is selected as the IP Address Mode, you can specify the hostname of the DHCP client in the field. The DHCP client will use option 12 to tell the DHCP server their hostname.
DHCP Mode	Select a mode for the clients in the VLAN to obtain their IP address.
	None: Do not use DHCP to assign IP addresses.
	DHCP Server: Assign an IP address to the clients through a DHCP server.
	When DHCP Server is selected, you can specify the DHCP Range, and the IP addresses in the range can be assigned to the clients in the VLAN. Also, it is optional for you to specify the DHCP Option 138, Primary/Seconday DNS, Default Gateway, and Lease Time. DHCP Option 138 informs the DHCP client of the controller's IP address when the client sends a request to the DHCP server, and specify Option 138 as the controller's IP address here. Lease Time decides how long the client can use the assigned IP address.
	DHCP Relay: It allows clients in the VLAN to obtain IP addresses from a DHCP server ion different subnet. When DHCP Relay is selected, specify the IP address of the DHCP server in Server Address.

■ **Static Route**

In Static Route, you can configure entries of static route for the switch. The general information of the existing static route entries are displayed in the table. For an existing static route, click ☑ to edit the settings, and click 🗑 to delete it.

To add a new static route entry, click `+ Add` and configure the parameters.

Status	Click the checkbox to enable or disable the static route.
IP Version	Select IPv4 or IPv6.
Destination IP/ Subnet / Destination IP/ Prefix Length	When IP Version is IPv4, specify Destination IP/Subnet. When IP Version is IPv6, specify Destination IP/Prefix Length. They identify the network traffic which the Static Route entry controls. You can click + Add Subnet to specify multiple entries or click 🗑 to delete them.
Next Hop	Specify the IP address for your devices to forward the corresponding network traffic.

Distance	Specify the priority of a static route. It is used to decide the priority among routes to the same destination. Among routes to the same destination, the route with the lowest distance value will be recorded into the routing table.

■ **Services**

In Services, you can configure Management VLAN, Loopback Control and SNMP.

Management VLAN	Display the name of the current Management VLAN. To configure the Management VLAN, please go to Config > VLAN Interface. Note that the controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations. The management VLAN is a VLAN created to enhance the network security. Without Management VLAN, the configuration commands and data packets are transmitted in the same network. There are risks of unauthorized users accessing the management page and modifying the configurations. A management VLAN can separate the management network from the data network and lower the risks.
Loopback Detection	When enabled, the switch checks the network regularly to detect the loopback. Note that Lopback Detection and Spanning Tree are not available at the same time.
Spanning Tree	Select a mode for Spanning tree. This feature is available only when Loopback Detection is disabled. Off: Disable Spanning Tree on the switch. STP: Enable STP (Spanning Tree Protocal) to prevent loops in the network. STP helps to block specific ports of the switches to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology. RSTP: Enable RSTP (Rapid Spanning Tree Protocal) to prevent loops in the network. RSTP provides the same features as STP with faster spanning ree convergence. Priority: When STP/RSTP enabled, specify the priority for the swith in Spanning Tree. In STP/RSTP, the switch with the highest priority will be selected as the root of the spanning tree. The switch with the lower value has the higher priority.
SNMP	(Only for configuring a single device) Configure SNMP to write down the location and contact detail. You can also click Manage to jump to Settings > Services > SNMP, and for detailed configuration of SNMP service, refer to 4. 10. 4 SNMP.

■ **IP Settings (Only for configuring a single device)**

In IP Settings, select an IP mode and configure the parameters for the device.

If you select DHCP as the mode, make sure there is a DHCP server in the network and then the device will obtain dynamic IP address from the DHCP server automatically. You can set a fallback IP

address to hold an IP address in reserve for the situation in which the device fails to get a dynamic IP address. Enable Fallback IP and then set the IP address, IP mask and gateway.

IP Settings

Mode:

- ● DHCP
- ○ Static

Fallback IP: ☑ Enable ⓘ

Fallback IP Address:

| 192 | . | 168 | . | 0 | . | 25 |

Fallback IP Mask:

| 255 | . | 255 | . | 255 | . | 0 |

Fallback Gateway:

| . | . | . | (Optional) |

Apply   Cancel

If you select Static as the mode, set the IP address, IP mask, gateway, and DNS server for the static address.

IP Settings   ⌃

Mode:
◯ DHCP
⦿ Static

IP Address:

[.   .   .   ]

IP Mask:

[.   .   .   ]

Gateway:

[.   .   .   ]

Primary DNS Server:

[.   .   .   ]   (Optional)

Secondary DNS Server:

[.   .   .   ]   (Optional)

Apply   **Cancel**

■ **Manage Device**

In Manage Device, you can upgrade the device's firmware version manually, move it to another site, synchronize the configurations with the controller and forget the switch.

Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. When upgrading, the device will be reboot and readopted by the controller. You can also check the box of Upgrade all devices of the same model in the site after the firmware file is uploaded.
Copy Configuration	Select another device at the current site to copy its configurations.
Move to Site	Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.

Force Provision	(Only for configuring a single device) Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.
Forget This Device	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.
Download Device Info	If the device has an abnormality, you can download the device information and provide it to our R&D personnel to analyze the problem.

- Note:

Firmware updates are required for earlier Omada devices to obtain complete information.

1. 3. 2   Monitor Switches

One panel and four tabs are provided to monitor the device in the Properties window: Monitor Panel, Details, Clients, and Statistics.

Monitor Panel

The monitor panel displays the switch's ports and uses colors and icons to indicate the connection status and port type. When the switch is pending or disconnected, all ports are disabled.

⚡ PoE	A PoE port connected to a powered device (PD).
∧ Uplink	An uplink port connected to WAN.
👁 Mirroring	A mirroring port that is mirroring another switch port.
⊘ STP Blocking	A port in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocol Data Unit) packets to maintain the spanning tree. Other packets are dropped.

You can hover the cursor over the port icon (except disabled ports) for more details. The displayed information varies due to connection status and port type.

Port	3
Name	Port3
Status	1000 Mbps Full Duplex
Tx Bytes	343.59 MB
Rx Bytes	353.98 MB
Profile	All
PoE Power	4.3 W

Status	Displays the negotiation speed of the port.
Tx Bytes	Displays the amount of data transmitted as bytes.
Rx Bytes	Displays the amount of data received as bytes.
Profile	Displays the name of profile applied to the port, which defines how the packets in both ingress and egress directions are handled. For detailed configuration, refer to 4. 8 Create Profiles.
PoE Power	Displays the PoE power supply for the PD device.
Uplink	Displays the name of device connected to the uplink port.
Mirroring From	Displays the name of port that is mirrorred.
LAG ID	Displays the name of ports that are aggregated into a logical interface.

Details

In Details, you can view the basic information, traffic information, and radio information of the device to know the device's running status.

45

■   **Overview**

In Overview, you can view the basic information of the device. The listed information will be varied due to the device's model and status.

■   **Uplink (Only for the switch connected to an Omada-managed router/switch in Connected status)**

Click Uplink to view the uplink information, including the uplink port, the uplink device, the negotiation speed, and transmission rate.

■ **Downlink (Only for the switch connected to Omada-managed devices in Connected status)**

Click Downlink to view the downlink information, including the downlink ports, devices name and model as well as negotiation speed.

Downlink			⌃
Port	**Model**	**Device-MAC**	**Status**
3	EAP660 HD	B0-95-75-E6-48-3C	1000 Mbps Full Duplex

Showing 1-1 of 1 records   ‹ 1 ›

Clients

In Clients, you can view the information of clients connected to the switch, including the client name, IP address and the connected port. You can click the client name to open its Properties window.

#	Name	IP Address
7	OC200_72C6FB	192.168.0.132
8	TP-Link-PC	192.168.0.145

Showing 1-2 of 2 records   ‹ 1 ›

Statistics

In Statistics, you can monitor the CPU and memory of the device in last 24 hours via charts. To view statistics of the device in certain period, click the chart to jump to 8. 2 View the Statistics of the Network.

◆ 1. 4 Configure and Monitor EAPs

In the Properties window, you can configure one or some EAPs connected to the controller and monitor the performance and statistics. Configurations changed in the Properties window will be applied only to the selected AP(s). By default, all configurations are synchronized with the current site.

To open the Properties window, click the entry of an AP, or click Batch Action, and then Batch Config to select APs for batch configuration. A monitor panel and several tabs are listed in the Properties window. Most features to be configured are gathered in the Config tab, such as IP, radios, SSID, and VLAN, while other tabs are mainly used to monitor the device.

ⓘ Note:

- The available functions in the window vary due to the model and status of the device.

- In Batch Config, you can only configure the selected devices, and the unaltered configurations will keep the current settings.

- In Batch Config, if some functions, such as the 5 GHz band, are available only on some selected EAPs, the corresponding configurations will not take effect. To configure them successfully, check the model of selected devices first.

1. 4. 1   Configure EAPs

In the Properties window, click Config and then click the sections to configure the features applied to the selected AP(s).

■ **General**

In General, you can specify the device name and LED settings of the AP, and categorize it via device tags.

General	⌃
Name:	
B0-95-75-E6-48-44	
LED:	
⦿ Use Site Settings	
○ On	
○ Off	
Wi-Fi Control: ☐ Enable ⓘ	
Device Tags:	
Please Select... ⌄	
Apply **Cancel**	

Name	(Only for configuring a single device) Specify a name of the device.
LED	Select the way that device's LEDs work.
	Use Site Settings: The device's LED will work following the settings of the site. To view and modify the site settings, refer to 4. 2. 2 Services.
	On/Off: The device's LED will keep on/off.
Wi-Fi Control	(Only for Certain wall plate APs) Enable Wi-Fi Control, and it will take effect only when the LED feature is enabled. After enabling Wi-Fi Control, you can press the LED button on the AP to turn on/off the Wi-Fi and LED at the same time.
Device Tags	Select a tag from the drop-down list or create a new tag to categorize the device.

■ **IP Settings (Only for configuring a single device)**

In IP Settings, select an IP mode and configure the parameters for the device.

If you select DHCP as the mode, make sure there is a DHCP server in the network and then the device will obtain dynamic IP address from the DHCP server automatically. If you want to let the device use a fixed IP address, you can enable Use Fixed IP Address, and set the network and IP address based on needs. Also, you can set a fallback IP address to hold an IP address in reserve for

the situation in which the device fails to get a dynamic IP address. Enable Fallback IP and then set the IP address, IP mask and gateway.

If you select Static as the mode, set the IP address, IP mask, gateway, and DNS server for the static address.

IP Settings   ⌃

Mode:

○ DHCP

⦿ Static

IP Address:

[.   .   .   ]

IP Mask:

[.   .   .   ]

Gateway:

[.   .   .   ]

Primary DNS Server:

[.   .   .   ] (Optional)

Secondary DNS Server:

[.   .   .   ] (Optional)

Apply   Cancel

■ Radios

In Radios, you can control how and what type of radio signals the EAP emits. Select each frequency band and configure the parameters. Different models support different bands.

ⓘ Note:

The 6 GHz band is only available for certain devices.

Radios   ⌃

| 2.4 GHz | 5 GHz-1 | 5 GHz-2 | 6 GHz |

Status: ☑ Enable

Channel Width:

Auto   ⌄

Channel

Auto   ⌄

Tx Power (EIRP):

High   ⌄

Note : The EIRP transmit power includes the antenna gain.

Apply   **Cancel**

Status	If you disable the frequency band, the radio on it will turn off.
Channel Width	Specify the channel width of the band. Different bands have different available options. We recommend using the default value.
Channel	Specify the operation channel of the EAP to improve wireless performance. If you select Auto for the channel setting, the EAP scans available channels and selects the channel where the least amount of traffic is detected.
Tx Power	Specify the Tx Power (Transmit Power) in the 4 options: Low, Medium, High and Custom. The actual power of Low, Medium and High are based on the minimum transmit power (Min. Txpower) and maximum transmit power (Max. TxPower), which may vary in different countries and regions. Low: Min. TxPower + (Max. TxPower-Min. TxPower) * 20% (round off the value) Medium: Min. TxPower + (Max. TxPower-Min. TxPower) * 60% (round off the value) High: Max. TxPower Custom: Specify the value manually.

■ **WLANs**

In WLANs, you can apply the WLAN group to the EAP and specify a different SSID name and password to override the SSID in the WLAN group. After that, clients can only see the new SSID and use the new password to access the network. To create or edit WLAN groups, refer to 4. 4 Configure Wireless Networks.

ⓘ Note:

The 6 GHz band is only available for certain devices.

WLANs			⌃
WLAN Group:			
Please Select... ⌄			
Name	**Band**	**Overrides**	**Enable**
EAP_test	2.4 GHz, 5 GHz, 6 GHz		⬤
EAP_test_IPC	2.4 GHz, 5 GHz, 6 GHz		⬤
EAP_test_gue...	2.4 GHz, 5 GHz, 6 GHz		◯

Showing 1-3 of 3 records   ‹ 1 ›

Apply   **Cancel**

(Only for configuring a single device) To override the SSID, select a WLAN group, click ✐ in the entry and then the following page appears.

WLANs>SSID Override

SSID Override:	☑ Enable	
SSID:		
tp-link		
Password:		
••••••••	∅	
VLAN:	☑ Enable	
VLAN ID:		
1	(1-4094)	

Save   **Cancel**

SSID Override	Enable or disable SSID Override on the EAP. If SSID Override enabled, specify the new SSID and password to override the current one.
VLAN	Enable or disable VLAN. If VLAN enabled, enter a VLAN ID to add the new SSID to the VLAN.

■ **Services**

In Services, you can enable Management VLAN to protect your network and configure SNMP and web server parameters.

Management VLAN	To configure Management VLAN, create a network in LAN first, and then select it as the management VLAN on this page. For details, refer to 4. 3 Configure Wired Networks.
	The management VLAN is a VLAN created to enhance the network security. Without Management VLAN, the configuration commands and data packets are transmitted in the same network. There are risks of unauthorized users accessing the management page and modifying the configurations. A management VLAN can separate the management network from the data network and lower the risks.
SNMP	(Only for configuring a single device) Configure SNMP to write down the location and contact detail. You can also click Manage to jump to Settings > Services > SNMP, and for detailed configuration of SNMP service, refer to 4. 10. 4 SNMP.

Layer-3 Accessibility	With this feature enabled, devices from a different subnet can access Omada managed devices.
LLDP	LLDP (Link Layer Discovery Protocol) can help discover devices.

■ **Smart Antenna**

In Smart Antenna, you can turn on the function to improve Wi-Fi performance for user-heavy scenarios through antenna array and intelligent algorithm. This help overcome obstacles and signal interference.

Smart Antenna   ≫

Smart Antenna:

◉ On

◯ Off

ⓘ Smart Antenna improves Wi-Fi performance for user-heavy scenarios through antenna array and intelligent algorithm, and it helps overcome obstacles and signal interference.

Apply   **Cancel**

■ **Advanced**

In Advanced, configure Load Balance and QoS to make better use of network resources. Load Balance can control the client number associated to the EAP, while QoS can optimize the performance when handling differentiated wireless traffics, including traditional IP data, VoIP (Voice-over Internet Protocol), and other types of audio, video, streaming media.

Select each frequency band and configure the following parameters and features.

Advanced

| 2.4GHz | 5GHz |

Load Balance

Maximum Associated Clients: ☑ Enable

1   (1-511)

RSSI Threshold: ☑ Enable ⓘ

0   (-95-0 dBm)

ETH Port Settings

ETH1 VLAN: ☑ Enable

1   (1-4094)

ETH2 VLAN: ☐ Enable

ETH3 VLAN: ☐ Enable

ETH3 PoE Out: ☐ Enable

QoS

Wi-Fi Multimedia (WMM):   ☑ Enable ⓘ

No Acknowledgement: ☐ Enable ⓘ

Unscheduled Automatic Power Save Delivery: ☑ Enable ⓘ

OFDMA

OFDMA: ☐ Enable ⓘ

Apply   **Cancel**

Max Associated Clients	Enable this function and specify the maximum number of connected clients. If the connected client reaches the maximum number, the EAP will disconnect those with weaker signals to make room for other clients requesting connections.
RSSI Threshold	Enable this function and enter the threshold of RSSI (Received Signal Strength Indication). If the client's signal strength is weaker than the threshold, the client will lose connection with the EAP.
ETH VLAN/ETH2 VLAN/ETH3 VLAN	(Only for Wall Plate AP) Enable this function and add the corresponding AP's LAN port to the VLAN specified here. Then the hosts connected to this EAP can only communicate with the devices in this VLAN.
ETH3 PoE Out	(Only for Wall Plate AP with the PoE out port) Enable this function to supply power to the connected device on this port.
Wi-Fi Multimedia (WMM)	With WMM enabled, the EAP maintains the priority of audio and video packets for better media performance.
No Acknowledgment	Enable this function to specify that the EAPs will not acknowledge frames with QoS No Ack. Enabling No Acknowledgment can bring more efficient throughput, but it may increase error rates in a noisy Radio Frequency (RF) environment.
Unscheduled Automatic Power Save Delivery	When enabled, this function can greatly improve the energy-saving capacity of clients.
Non-PSC Channels	(Only for AP supporting 6GHz band) When enabled, the AP can use both non-PSC channels and PSC channels. Note that some clients may not discover 6GHz networks using non-PSC channels.
OFDMA	(Only for AP supporting 802.11 ax) Enable this feature to enable multiple users to transmit data simultaneously, and it will greatly improves speed and efficiency. Note that the benefits of OFDMA can be fully enjoyed only when the clients support OFDMA.

■ **Manage Device**

In Manage Device, you can upgrade the device's firmware version manually, move it to another site, synchronize the configurations with the controller and forget the AP.

Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. When upgrading, the device will be reboot and readopted by the controller. You can also check the box of Upgrade all devices of the same model in the site after the firmware file is uploaded.
Copy Configuration	Select another device at the current site to copy its configurations.
Move to Site	Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.

Force Provision	(Only for configuring a single device) Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.
Forget this AP	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.
Download Device Info	If the device has an abnormality, you can download the device information and provide it to our R&D personnel to analyze the problem.

ⓘ **Note:**

Firmware updates are required for earlier Omada devices to obtain complete information.

1. 4. 2   Monitor EAPs

One panel and four tabs are provided to monitor the device in the Properties window: Monitor Panel, Details, Clients, Mesh, and Statistics.

Monitor Panel

The monitor panel illustrates the active channel information on each radio band, including the EAP's operation channel, radio mode and channel utilization. Four colors are used to indicate the percentage of Rx Frames (blue), Tx Frames (green), Interference (orange), and Free bandwidth (gray).

6	b/g/n/ax mixed 2.4 GHz	(88% Utilized)
		High
40	a/n/ac/ax mixed 5 GHz-1	(20% Utilized)
		Acceptable
100	a/n/ac/ax mixed 5 GHz-2	(6% Utilized)
		Good
37	ax only 6 GHz	(0% Utilized)
		Good

▮ Rx Frames   ▮ Tx Frames   ▮ Interference   ▮ Free

You can hover the cursor over the channel bar for more details.

Ch.Util.(Busy/Rx/Tx)	**51% / 32% / 4%**
Tx Pkts/Bytes	**4195 / 847.04 KB**
Rx Pkts/Bytes	**24247 / 6.47 MB**
Tx Error/Dropped	**0.0% / 0.0%**
Rx Error/Dropped	**0.0% / 0.0%**

Ch.Util.(Busy/Rx/Tx)	Displays channel utilization statistics.
	Busy: Displays the sum of Tx, Rx, and also non-WiFi interference, which indicates how busy the channel is.
	Rx: Indicates how often the radio is in active receive mode.
	Tx: Indicates how often the radio is in active transmit mode.
Tx Pkts/Bytes	Displays the amount of data transmitted as packets and bytes.
Rx Pkts/Bytes	Displays the amount of data received as packets and bytes.
Tx Error/Dropped	Displays the percentage of transmit packets that have errors and the percentage of packets that were dropped.
Rx Error/Dropped	Displays the percentage of receive packets that have errors and the percentage of packets that were dropped.

Details

In Details, you can view the basic information, traffic information, and radio information of the device to know the device's running status.

■ **Overview**

In Overview, you can view the basic information of the device. The listed information varies due to the device's status.

Overview	⌃
MAC Address:	IP Address:
40-3F-8C-00-01-10	192.168.0.100
Model:	Firmware Version:
EAP690E HD(EU) v1.0	1.0.0 Build 20220708 Rel. 3 6560
CPU Utilization:	Memory Utilization:
4%	22%
Uptime:	
--	

■ **LAN (Only for devices in the Connected status)**

Click LAN to view the traffic information of the LAN port, including the total number of packets, the total size of data, the total number of packets loss, and the total size of error data in the process of receiving and transmitting data.

LAN	⌃
Rx Packets:	Rx Bytes:
4724	936.73 KB
Rx Dropped Packets:	Rx Errors:
0	0
Tx Packets:	Tx Bytes:
822	647.23 KB
Tx Dropped Packets:	Tx Errors:
0	0

■   **Uplink (Wireless) (Only for devices in the Connected 🛜 status)**

Click Uplink (Wireless) to view the traffic information related to the uplink AP, including the signal strength, transmission rate, ratio of packets number and size, and dynamic downstream rate.

Uplink (Wireless)	⌃
Uplink Device:	**Signal:**
CC-32-E5-F7-DD-1C	-22 dBm
Tx Rate:	**Rx Rate:**
104Mbps	526Mbps
Down Pkts/Bytes:	**Up Pkts/Bytes:**
29 / 9.11 KB	18 / 2.50 KB
Activity Speed: ⓘ	
1.16 KB /s	

■ **Radios (Only for devices in the Connected status)**

Click Radio to view the radio information including the frequency band, the wireless mode, the channel width, the channel, and the transmitting power. You can also view parameters of receiving/transmitting data on each radio band.

ⓘ Note:

The 6 GHz band is only available for certain devices.

Radios

| 2.4 GHz | 5 GHz-1 | 5 GHz-2 | 6 GHz |

Mode:	Channel Width:
802.11b/g/n/ax mixed	20/40MHz
Channel:	Tx Power:
6 / 2437MHz	20
Rx Packets:	Rx Bytes:
0	0
Rx Dropped Packets:	Rx Errors:
0	0
Tx Packets:	Tx Bytes:
2550	726.87 KB
Tx Dropped Packets:	Tx Errors:
0	0

Clients

In Clients, you can view the information of users and guests connecting to the AP, including client name, MAC address and the connected SSID. Users are clients connected to the AP's SSID with Guest

Network disabled, while Guests are clients connected to that with Guest Network enabled. You can click the client name to open its Properties window.

All (4)	Users (4)	Guests (0)		History >

Client name or MAC

Name	MAC	SSID
Client_0	20-47-DA-2E-23-1D	EAP_test
Client_3	44-55-C4-06-EF-75	EAP_test
Client_6	D4-62-EA-B4-21-E8	EAP_test
Client_9	C0-9F-05-24-0C-EF	EAP_test

Showing 1-4 of 4 records   <   1   >

Click History to view the client history. In the History page, you can specify the date or time period to view the clients connected during specific time, and click Export to download the list of clients.

History   ×

Oct 22, 2022 - Oct 29, 2022			Export

START TIME	END TIME	Name	MAC
Dec 20, 2020 01:10:46 am	Dec 20, 2020 01:10:46 am	Client_0	20-47-DA-2E-23-1D
Jan 21, 2021 03:34:29 am	Jan 21, 2021 03:34:29 am	Client_1	9C-28-F7-9B-9B-08
Jan 24, 2021 03:52:33 pm	Jan 24, 2021 03:52:33 pm	Client_2	A4-F1-E8-C2-FC-3F

Showing 1-3 of 3 records   <   1   >   10 /page   ⌄   Go To page: GO

Mesh (Only for pending/connected/isolated devices supporting Mesh)

Mesh is used to establish a wireless network or expand a wired network through wireless connection on 5 GHz radio band. In practical application, it can help users to conveniently deploy APs without requiring Ethernet cable. After mesh network establishes, the EAPs can be configured and managed in Omada controller in the same way as wired EAPs. Meanwhile, because of the ability to self-organize and self-configure, mesh also can efficiently reduce the configuration.

Note that only certain EAP models support Mesh, and the EAPs should be in the same site to establish a Mesh network.

To understand how mesh can be used, the following terms used in Omada Controller will be introduced:

Root AP	The AP is managed by Omada Controller with a wired data connection that can be configured to relay data to and from mesh APs (downlink AP).
Isolated AP	When the EAP which has been managed by Omada Controller before connects to the network wirelessly and cannot reach the gateway, it goes into the Isolated state.
Mesh AP	An isolated AP will become a mesh AP after establishing a wireless connection to the AP with network access.
Uplink AP/Downlink AP	Among mesh APs, the AP that offers the wireless connection for other APs is called uplink AP. A Root AP or an intermediate AP can be the uplink AP. And the AP that connects to the uplink AP is called downlink AP. An uplink AP can offer direct wireless connection for 4 downlink APs at most.
Wireless Uplink	The action that a downlink AP connects to the uplink AP.
Hops	In a deployment that uses a root AP and more than one level of wireless uplink with intermediate APs, the uplink tiers can be referred to by root, first hop, second hop and so on. The hops should be no more than 3.

A common mesh network is shown as below. Only the root AP is connected by an Ethernet cable, while other APs have no wired data connection. Mesh allows the isolated APs to communicate with pre-configured root AP on the network. Once powered up, factory default or unadopted EAPs can detect the EAP in range and make itself available for adoption in the controller.

After all the EAPs are adopted, a mesh network is established. The EAPs connected to the network via wireless connection also can broadcast SSIDs and relay network traffic to and from the network through the uplink AP.

To build a mesh network, follow the steps below:

1) Enable Mesh function.

2) Adopt the Root AP.

3) Set up wireless uplink by adopting APs in Pending(Wireless) or Isolated status.

1. Go to Settings > Site to make sure Mesh is enabled.

2. Go to Devices to make sure that the Root AP has been adopted by the controller. The status of the Root AP is Connected.

3. Install the EAP that will uplink the Root AP wirelessly. Make sure the intended location is within the range of Root AP. The EAPs that is waiting for Wireless Uplink includes two cases: factory default EAPs and EAPs that has been managed by the controller before. Go to Devices to adopt an EAP in Pending (Wireless) status or link an isolated AP.

    1) For the factory default EAP, after powering on the device, the EAP will be in Pending (Wireless) status with the icon PENDING 📶 in the controller. Click ✓ to adopt the EAP in Pending (Wireless) status in the Devices list.

After adoption begins, the status of Pending (Wireless) EAP will become Adopting (Wireless) and then Connected (Wireless). It should take roughly 2 minutes to show up Connected (Wireless) with the icon `CONNECTED` 📶 within your controller.

2) For the EAP that has been managed by Omada Controller before and cannot reach the gateway, it goes into Isolated status when it is discovered by controller again. Click 🔗 to connect the Uplink AP in the Devices list.

DEVICE NAME	IP ADDRESS	STATUS	MODEL	VERSION	UPTIME	ACTION ⋮
00-EA-DE-5B-E3-11	192.168.0.1	CONNECTED	TL-R605 v1.0	1.0.0	24 days 21:49:55	⏻
60-32-B1-8D-3D-F6	192.168.0.133	CONNECTED	TL-SG2008 v3.0	3.0.0	8 days 04:28:00	⦿ ⏻
EA-23-51-06-22-52	192.168.0.7	ISOLATED	EAP225-Outdoor(EU) v1.0	5.0.0	0 days 00:02:53	🔗
EA-33-51-A8-22-A0	192.168.0.187	CONNECTED	EAP225-Outdoor(EU) v1.0	5.0.0	1 days 08:15:23	⦿ ⏻

Showing 1-4 of 4 records ‹ 1 ›   5 /page ▾   Go To page: GO

The following page will be shown as below, click Link to connect the Uplink AP.

Once mesh network has been established, the EAP can be managed by the controller in the same way as a wired EAP. You can click the EAP's name in the Devices list, and click Mesh to view and configure the mesh parameters of the EAP in the Properties window.

In Mesh, if the selected AP is an uplink AP, this page lists all downlink APs connected to the AP.

If the selected AP is a downlink AP, this page lists all available uplink APs and their channel, signal strength, hop, and the number of downlink APs. You can click Rescan to search the available uplink APs and refresh the list, and click Link to connect the uplink AP and build up a mesh network.

Uplinks					⌃
AP Name	**Channel**	**Signal**	**Hop**	**Downlink**	**ACTION**
★ CC-32-E5-F7-DD-1C ●	36	-46 dBm	0	0	
EA-23-51-06-22-52	36	-40 dBm	0	0	**Link**

Showing 1-2 of 2 records   ‹ 1 ›   **Rescan**

★	The icon appears before the priority uplink AP of the downlink AP. If you want to set another AP as the priority AP, click Link in Action column.
●	The icon appears before the current uplink AP of the downlink AP.

💡 Tips:

- You can manually select the priority uplink AP that you want to connect in the uplink AP list. To build a mesh network with better performance, we recommend that you select the uplink AP with the strongest signal, least hop and least downlink AP.

- Auto Failover is enabled by default, and it allows the controller automatically select an uplink AP for the isolated AP to establish Wireless Uplink. And the controller will automatically select a new uplink AP for the mesh EAPs when the original uplink fails. For more details about Mesh global configurations, refer to the Mesh feature in 4. 2. 2 Services.

Tools

In Tools, you can enable RF Scanning to scan the RF (Radio Frequency) environments around the AP, which is useful for spectral analysis in channel selection and planning.

⚠ Note:

- The RF scanning may take several minutes. During the scanning, all clients using this AP will be disconnected, and the AP will be offline. You should select a spare time of network to start scanning.

- The APs in the mesh network do not support RF Scanning.

Select each frequency band to view and analyze the scan results.

Each colored bar graph displays the information about channel utilization and interference on a channel. The filling area of the bar represents the channel utilization. And the larger filling area means the higher utilization, which indicates the channel is busier in transmitting data. The color shade represents the level of interference. And the legend is displayed at the top.

The results of different bands are displayed in different channel widths.

The number below the bar graph displays the corresponding channel number for each channel width option. For example, channels 42, 58 and 106 are three of the 80 MHz channels. And the channel outline in blue is in use currently.

You can hover the cursor over a channel option for more details.

Radio	Displays the radio that the AP uses.
Channel Width	Displays the width of the channel.
Used Channels	Displays the channels in use.
Frequency Range	Displays the range of frequencies.
Utilization	Displays the percentage of the frequency range already in use.
Interference	Displays the level of interference.
Interference Type	Displays the type of interface, including MWO (Microwave Oven), CW (Continuous Wave), WLAN (Wi-Fi signals) and FHSS (Frequency Hopping Spread Spectrum).

Statistics

In Statistics, you can monitor the utilization of the device in last 24 hours via charts, including CPU/ Memory Monitor, Channel Utilization, Dropped Packets, and Retried Packets. To view statistics of the device in certain period, click the chart to jump to 8. 2 View the Statistics of the Network.