Configuring an IoT VLAN on TP-Link Omada SDN (Wi-Fi 7 Environment)

Isolating Internet of Things (IoT) devices on a dedicated VLAN is a fundamental network security practice. Smart home devices, sensors, and appliances often utilize weaker security protocols and receive infrequent firmware updates, making them vulnerable if breached.

This guide details the best-practice setup for an IoT VLAN using the TP-Link Omada Software-Defined Networking (SDN) platform, specifically tailored for environments utilizing tri-band Wi-Fi 7 Access Points.

Prerequisites

- An Omada Software or Hardware Controller (v5.9 or newer recommended).
- An Omada-compatible Router/Gateway and Switch.
- Tri-band Wi-Fi 7 Omada Access Points (e.g., EAP773, EAP783, EAP789).

Step 1: Create the IoT Local Area Network (LAN)

First, establish a logical network foundation to assign IP addresses that are entirely separate from those of your trusted personal devices.

1. Navigate to **Settings** > **Wired Networks** > **LAN**.
2. Click **Create New LAN**.
3. Configure the following settings:
   - **Purpose:** VLAN
   - **Name:** `IoT_VLAN`
   - **VLAN ID:** Choose a unique ID (e.g., `40`).
   - **Gateway/Subnet:** Enter a dedicated subnet (e.g., `10.0.40.1/24`).
   - **DHCP Server: Enable**. Ensure the DHCP range does not overlap with your main LAN.
4. Click **Save**.

Step 2: Create the Dedicated IoT Wireless Network

IoT devices are notoriously sensitive to modern Wi-Fi standards. The cutting-edge features of your Wi-Fi 7 APs must be carefully managed for this specific SSID to ensure compatibility and network stability.

1. Navigate to **Settings** > **Wireless Networks** > **WLAN**.
2. Click **Create New Wireless Network**.
3. Configure the following basic settings:
   - **Network Name (SSID):** `IoT-Network`
   - **Band:** Select **2.4 GHz** only. *(Note: You may enable 5 GHz if you have high-bandwidth devices like 4K video doorbells, but 2.4 GHz provides the widest compatibility for standard smart plugs and sensors.*
4. Configure Wi-Fi 7 and Security Settings:
   - **6 GHz: Leave unchecked.** Legacy IoT devices lack the hardware to see this spectrum, and enabling it can cause broadcasting overhead.
   - **MLO (Multi-Link Operation): Disable**. MLO allows devices to connect across multiple bands simultaneously. Cheaper IoT microcontrollers often fail to associate when MLO is broadcast on the SSID.
   - **Security: WPA2-Personal**. While WPA3 is the modern standard, many IoT devices will fail to connect to a WPA3 or WPA2/WPA3 transition network due to Protected Management Frame (PMF) requirements.
5. Expand **Advanced Settings**:
   - **VLAN:** Enable and enter the VLAN ID created in Step 1 (e.g., `40`).
6. Click **Save**.

Step 3: Implement Access Control Lists (ACLs)

By default, Omada routers allow inter-VLAN routing. To properly isolate the IoT devices, you must restrict traffic using Gateway ACLs.

Navigate to **Settings** > **Network Security** > **ACL** > **Gateway ACL**. Create the following rules in this exact top-to-bottom order:

1. **Permit Gateway Services (DNS/DHCP):**
   - **Direction:** LAN -> LAN

- **Policy:** Permit
- **Protocols:** UDP
- **Source:** Network -> `IoT_VLAN`
- **Destination:** IP Port Group -> Create a group for your Gateway IP (e.g., `10.0.40.1`) on Ports `53` (DNS) and `67` (DHCP).

2. **Deny Gateway Web UI Access:**
   - **Direction:** LAN -> LAN
   - **Policy:** Deny
   - **Protocols:** TCP
   - **Source:** Network -> `IoT_VLAN`
   - **Destination:** IP Port Group -> Gateway IP on Ports `80`, `443`, and `22`.
3. **Deny IoT to the Main LAN:**
   - **Direction:** LAN -> LAN
   - **Policy:** Deny
   - **Protocols:** All
   - **Source:** Network -> `IoT_VLAN`
   - **Destination:** Network -> `Main_LAN` (and any other trusted VLANs).
   - *Note: Omada's stateful firewall automatically allows return traffic for connections initiated by devices on your Main LAN, meaning you can still control your smart devices from your trusted network.*

Step 4: Configure mDNS Reflection (Optional)

If you have casting devices (Chromecast, Apple TV) or smart speakers (Sonos) on the IoT VLAN, devices on your Main LAN won't be able to discover them unless mDNS reflection is enabled.

1. Navigate to **Settings** > **Services** > **mDNS**.
2. **Enable** the mDNS service.
3. Select the **Bonjour** service.
4. Select both your `Main_LAN` and `IoT_VLAN` under the Client and Server networks.
5. Click **Save**.

Verification

You can verify that your WLAN configuration is correctly mapped to the appropriate VLAN and that Wi-Fi 7 features are properly disabled using the controller's CLI.

```
# Example output verifying WLAN to VLAN mapping and radio status
show wlan ssid "IoT-Network"
```

```
Status       : Active
VLAN ID      : 40
Security     : WPA2-PSK
Radios       : 2.4GHz
6GHz         : Disabled
MLO          : Disabled
```

Revision #1
Created 2026-03-21 22:39:53 UTC by Francis
Updated 2026-03-27 17:32:59 UTC by Francis