Compatibility List

Print Server Compatibility List

<table>
<thead>
<tr>
<th>TL-WR2543ND</th>
<th>TL-WR842ND</th>
<th>TL-WDR4300</th>
<th>TL-WR1042ND</th>
</tr>
</thead>
<tbody>
<tr>
<td>TD-W8968</td>
<td>TL-WDR3600</td>
<td>TL-WDR3500</td>
<td>TD-W8970</td>
</tr>
<tr>
<td>TD-W8980</td>
<td>TD-VG3631</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| TL-WDR4900  | TL-WR1043ND | Archer C7  | C2 Archer D7 |
| Archer C9   | C20i Archer  | C5 Archer   | C8 Archer    |
| TL-PS110P   | TL-PS310U   | D2 Archer   | C20 TL-WPS510U |
| TD-W8970B   | TD-W8980B   | D9 Archer   | TL-PS110U    |
| D20 Archer  | D2 Archer   | Touch P5    | TD-W9970 Archer |
| D7b Archer  | D9 Archer   | Archer C50  | VR900        |
| Archer C50  | Archer C50  | Archer C50  | Archer C2600 |
| Archer C3200| Archer CR700| Archer C3200| Archer C2300 |
| C5400 Archer| C3150 Archer| Archer C59  | Archer C2300 |
| C1200 TC-W7960| Archer A2300| Archer C1900| Archer C3150 V2 |
| TL-WR1043N  | Archer C1900|             |             |

3G/4G Compatibility List


IPv6 Support

| TL-WR940N |

ISP Compatibility List

| TC-7620 | TC-W7960 Archer CR700 | TC-7610 Archer CR500 | CR1900 TC7650 |
### Windows 10 Compatibility for TP-Link network adapters

In our effort to continue providing end users with excellent experiences and satisfactory service, TP-Link is working to provide Windows 10 compatibility for as many of our products as possible.

The list below provides information regarding product compatibility and will be updated frequently to reflect driver availability.

**Notes:**

1. Models marked with "Yes" can work with Windows 10 automatically. For models marked "No", Windows 10 users can try to install the Windows 8 or Windows 8.1 driver manually. For models marked "Partial", only the 2.4GHz band can be used with the Plug & Play driver on Windows 10. Installing the Windows 8.1 driver may allow you to use both bands. TP-Link will release official Windows 10 drivers for these models as soon as possible. Review the FAQ for more information about installing drivers manually.

2. How do I determine the hardware version of my TP-Link product?

<table>
<thead>
<tr>
<th>Model &amp; Version</th>
<th>Plug &amp; Play on Windows 10</th>
<th>New Driver Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archer T4UH V1</td>
<td>Yes</td>
<td>Released</td>
</tr>
<tr>
<td>Archer T4UH V2</td>
<td>Yes</td>
<td>Released</td>
</tr>
<tr>
<td>Archer T4U V1</td>
<td>Yes</td>
<td>Released</td>
</tr>
<tr>
<td>Archer T2U V1</td>
<td>Yes</td>
<td>Released</td>
</tr>
<tr>
<td>Archer T2UH V1</td>
<td>Yes</td>
<td>Released</td>
</tr>
<tr>
<td>Archer T2UHP V1</td>
<td>Yes</td>
<td>Released</td>
</tr>
<tr>
<td>Archer T9UH V1</td>
<td>Yes</td>
<td>Released</td>
</tr>
<tr>
<td>Archer T1U V1</td>
<td>No</td>
<td>Released</td>
</tr>
<tr>
<td>TL-WDN4200 V1/3200 V1</td>
<td>Partial</td>
<td>N/A</td>
</tr>
<tr>
<td>TL-WN821N V5</td>
<td>Yes</td>
<td>Released</td>
</tr>
<tr>
<td>TL-WN822N V4</td>
<td>Yes</td>
<td>Released</td>
</tr>
<tr>
<td>TL-WN823N V2</td>
<td>Yes</td>
<td>Released</td>
</tr>
<tr>
<td>TL-WN722N V1</td>
<td>No</td>
<td>N/A (V2 Will Support)</td>
</tr>
<tr>
<td>TL-WN723N V3</td>
<td>Yes</td>
<td>Released</td>
</tr>
<tr>
<td>TL-WN725N V2</td>
<td>Yes</td>
<td>Released</td>
</tr>
<tr>
<td>TL-WN7200ND V1/8200ND V1</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>TL-WN727N V4</td>
<td>Yes</td>
<td>Released</td>
</tr>
<tr>
<td>Archer T9E V1</td>
<td>No</td>
<td>Released</td>
</tr>
</tbody>
</table>
Adapters

<table>
<thead>
<tr>
<th>Model</th>
<th>Hardware version</th>
<th>Compatibility</th>
<th>Release status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archer T8E V1</td>
<td>No</td>
<td></td>
<td>Released</td>
</tr>
<tr>
<td>Archer T6E V1</td>
<td>No</td>
<td></td>
<td>Released</td>
</tr>
<tr>
<td>TL-WDN4800 V1</td>
<td>Yes</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>TL-WN881ND V1</td>
<td>Yes</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>TL-WN781ND V2</td>
<td>Yes</td>
<td></td>
<td>Released</td>
</tr>
</tbody>
</table>

Microsoft Windows 10 drivers are part of the Windows 10 operating system. TP-Link does not have the access to these drivers and cannot support them at this time. For help and more information about Microsoft Windows 10 drivers, please refer to http://windows.microsoft.com/en-us/windows-10/support

IFTTT Compatibility for TP-Link Wi-Fi products

IFTTT, short for IF This Then That, is a free web-based service which help you do more with the services you love. TP-Link Wi-Fi products now provide the IFTTT services which you can use to make your life easier and smarter.

The list below provides information regarding product compatibility and will be updated frequently since TP-Link is working to make more products support IFTTT.

Notes:

1. Please make sure the product is updated with latest firmware.

2. A TP-Link ID must be bound to the product. No TP-Link ID?

Wi-Fi Routers product

<table>
<thead>
<tr>
<th>Model</th>
<th>Hardware version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archer C5400V2</td>
<td></td>
</tr>
<tr>
<td>Archer C3150V2</td>
<td></td>
</tr>
</tbody>
</table>

Whole Home Wi-Fi product

<table>
<thead>
<tr>
<th>Model</th>
<th>Hardware version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deco M5</td>
<td>V1</td>
</tr>
</tbody>
</table>
How to build a Factory Network using TP-Link products?

A modernized factory can’t be running without network. Normally a factory network will be separate into working network and entertainment network. Considering the security of the information and the safety of the work, network in the offices and workshops are usually deployed with Ethernet cable. While in the dormitory and the mess hall, wireless access point should be installed as the entertainment network for the workers. It would greatly inspire the enthusiasm of the workers for hard working and make them feel happy so that improving the efficient. This article is going to talk about an entire wireless network deployment solution for the factory.

What the basic needs of factory network?

Normally, a factory network should meet the following needs:

1. No blind zone. All the areas of lives should be covered with WiFi.
2. Wireless roaming. The clients can switch to another AP automatically while moving.
3. Centralized management. It is not convenient to configure the APs one by one, so all the APs should be managed and monitored by one controller.
4. Network security. The entertainment network should be isolated from the working network by VLAN. All the clients should be isolated to each other logically.
5. Flexible authorization method allows the user to access internet only in proper time.

What kind of solution can meet the needs of factory network?

Here we provide a full solution including the network topology, product features and parameters.
**Topology**

![Network Topology Diagram](Image)

**Tips for deploying this network topology:**

- In a factory, the distance between the workshop and dormitory is always far more than 100 meters. In this case, fiber with SFP module is the recommended transmission way. Link aggregation could help to break the Ethernet 1Gbps limitation.

- Wireless network is more convenient and flexible, while the wired network is more stable and securer. For the transmission related to the confidential information, wired connection is suggested. And for the entertainment network environment such as dormitory and mess hall, wireless access points are suggested. Besides, the refectory MIS should be connected to the enterprise network and isolated from the working network and entertainment network.

- The mess hall and the dormitory is not all the same while deploying the wireless access points, but there are always mainly 3 points should be considered, they are the coverage, the interference and the clients number. For the mess hall, it has large people flow at dining time, so there will be high burst flow. This require the capacity to handle large number of clients and high speed connection. For the dormitory, the clients’ number is fixed and the flow is more stable, we should think about how to deploy the APs reasonably to cost down the investment. Please refer to *Dormitory solution* for the dormitory deployment.

What are the highlights of this solution?

- **Easy to install**

  The EAP is celling mount designed, PoE supported, good looking and easy to install.
• **Full Coverage Wireless**

EAP is very suitable for large area coverage solution like mess hall or dormitory. It can reach up to 1900Mbps by using 802.11ac/802.11n technique.

• **Wireless roaming**

All the EAP use unified SSID and security method, clients can switch to other EAP automatically while moving.

• **Easy to manage**

EAPs are centralized managed by EAP controller software, which is free for use. All the EAP status can be monitored on the web GUI of the controller.

• **Security network environment**

TP-link switch supports standard VLAN function, it can isolate different departments into different VLANs. Multi-SSID working with VLAN is supported, so clients can be isolated from other hosts by VLAN. AP isolation can help to isolate clients to each other. WPA-Enterprise security makes the network securer.

• **Flexible access control**

EAP provides 802.1x, portal authentication and access voucher, it can prevent unauthorized connection, and limit the access time for each client as well. People can’t connect to the network if the voucher expired.

• **Link aggregation**

TP-link switch link aggregation makes the link bandwidth together. There are two 10Gbps SFP ports on T3700G-28TQ, and it can be used either for trunk port or stack port.
Which products should I choose to build the dormitory wireless network?

Here is a list which includes the TP-LINK devices for reference:

<table>
<thead>
<tr>
<th>Model</th>
<th>Brief Introduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP330</td>
<td>Ceiling mount 802.11AC dual band enterprise AP, speed up to 1900Mbps, managed by EAP controller software, 802.3at PoE supported with good looking surface</td>
</tr>
<tr>
<td>TL-SG3424P</td>
<td>Standard PoE switch with 24 gigabit ports. 802.1q 802.3af/at PoE L2 switch, VLAN, IGMP snooping, QoS, LACP supported, variety management methods, easy to configure, suitable for managed PoE network</td>
</tr>
<tr>
<td>T3700G-28TQ</td>
<td>Stackable L3 switch, 2 10Gps SFP ports, 4 Gigabits SFP ports, support IP routing, DHCP, VLAN, LACP, ACL and etc.</td>
</tr>
<tr>
<td>TL-SG3424</td>
<td>Standard L2 switch with 24 gigabit ports. VLAN, IGMP snooping, QoS, LACP supported, variety management methods, easy to configure.</td>
</tr>
</tbody>
</table>

How to build a Campus Network using TP-LINK products?

In campus, both teachers and students have Internet access requirement whenever and whatever possible. To help build a Campus Network, TP-LINK has provided a full solution.

What are the Basic needs of Campus Network?

Normally, a campus network should meet the following needs:

1. Both wired and wireless access available, teachers can have online teaching and researching, for students they can google for what they need.
2. Network should be fast and stable.
3. Allow remote access of campus Intranet resources.
4. Authority level for sensitive information.
5. Simple management and low cost of maintenance.

What kind of solution can meet the needs of Campus Network?

Here we provide a full solution including the network topology, product features and parameters.
Features

The solution we provided has the following features:

- A wide range of wireless coverage both indoor and outdoor

Various optional Access Point, and all kinds of installation methods including ceiling/wall mount, desktop and pole mount make it flexible to adapt to different environment such as classroom, dormitory, playground and canteen.

- Central management and configuration

Adopt Software Controller, can be installed on any PCs as command center.

Automatically discover all TP-LINK EAP series devices, configure and manage all APs together. Support L2 networking between controller and AP, also support L3 networking even if the controller is behind NAT devices.

- Full Gigabit wired network, redundancy design, fast and stable

Support gigabit wired-speed forwarding, especially on core switch, forwarding speed reaches up to 10Gbps

Support STP on Core Layer and Convergence Layer switches, easy design of redundancy as well as link backup
- Client to LAN VPN provide remote access to Campus Intranet Resources

Support IPSec/PPTP/L2TP, for students or teachers outside campus can visit intranet whenever and whatever possible through IPSec/PPTP/L2TP VPN.

- Multiple functions available including L3 routing, VLAN and DHCP Relay

Support L3 Routing and Static Routing, which can separate the network into different subnets and set different VLAN for each subnets.

Support DHCP Relay so that clients in different network segment can share the same DHCP Server.

- High network security features such as IP-MAC-Port-VID Binding, IEEE802.1X Authentication, make the network security issue easy to maintain.

Support IP-MAC-Port-VLAN Binding, 802.1X Authentication, ARP inspection, which can provide authentication and higher security to the Campus Network.

IP source guard can guarantee each PC with a specific IP address with a specific VLAN, that is to say, illegal user do not have network access key unless the administrator permits.

- Multiple wireless authentication methods, strictly control the access permission

Support Multi-SSID, each SSID maps to a certain VLAN for VLAN partition in wireless side

Support multiple authentication methods like Portal and Radius authentication

Support AP Isolation to ban communication among different wireless clients

Which product should I choose to set up the Campus Network?

Here is a list which includes the TP-LINK devices for reference:

<table>
<thead>
<tr>
<th>Device</th>
<th>Model</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Switch</td>
<td>Stackable L3 Managed Switch</td>
<td>Stackable</td>
</tr>
<tr>
<td></td>
<td>(T3700G-28TQ)</td>
<td>Support L3 Routing, Static Routing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pluggable, Redundant power module design, working around the clock</td>
</tr>
<tr>
<td>Convergence Switch</td>
<td>Gigabit L2 Managed Switch</td>
<td>Full gigabit ports, wired-speed forwarding</td>
</tr>
<tr>
<td></td>
<td>(T2600G-28TS)</td>
<td></td>
</tr>
</tbody>
</table>
## Access Switch

- **Unmanaged Switch (TL-SG1024)**
  - Full gigabit ports, wired-speed forwarding

- **Unmanaged PoE Switch (TL-SG1008P)**
  - Full gigabit ports, wired-speed forwarding
  - 4*PoE ports, transfer data and power on one single cable

## Wireless AP

- **EAP220**
  - 11n dual band with maximum speed of 600Mbps
  - Ceiling/Wall mounting
  - Supports 802.3af Standard PoE

- **EAP320**
  - 11ac dual band with maximum speed of 1200Mbps
  - Ceiling/Wall mounting
  - Supports 802.3at Standard PoE

- **EAP330**
  - 11ac dual band with maximum speed of 1900Mbps
  - Ceiling/Wall mounting
  - 2*gigabit ports, ETH1 supports 802.3at Standard PoE

---

**Note:** Refer to Appendix table for select EAP model selection.

---

**Can I know any detailed information about the EAPs?**

By referring to the appendix shown below, you can know the detailed information and parameters of our EAP products.

### Auranet EAP series specification

<table>
<thead>
<tr>
<th>Model</th>
<th>Items</th>
<th>EAP330</th>
<th>EAP320</th>
<th>EAP220</th>
<th>EAP120</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wireless Throughput</strong></td>
<td></td>
<td>2.4GHz:600Mbps</td>
<td>2.4GHz:300Mbps</td>
<td>2.4GHz:300Mbps</td>
<td>N300</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5GHz:1300Mbps</td>
<td>5GHz:867Mbps</td>
<td>5GHz:300Mbps</td>
<td>2.4GHz:300Mbps</td>
</tr>
</tbody>
</table>
How to build a Network for Restaurant & Cafe using tp-link products?

To operate a restaurant or Cafe successfully, the key is to attract new customers and keep the old ones. Providing wireless internet access may help achieve the two goals. Many business people, tourists and students always need to keep in contact with their friends, families or cooperators online even if they are on holidays. More and more people, like the sales, they would prefer to get out of the office to meet their customers at a comfortable environment. In such case, fast-speed and stable Wi-Fi definitely gives them an extra reason to patronize your place, and even makes them to consume more. Besides, an advanced restaurant MIS (Management Information System) also needs a stable network. The network requirements of a restaurant MIS should be fully considered. TP-LINK can provide professional wired and wireless solution for such requirements.

What are the needs of the network for restaurant and café?

A network for restaurant and café should meet the following needs:

1. Concise layout, good looking AP design, and PoE power supply are supported;
2. Centralized management, monitoring the working status of each AP, easy-to-operate feature should be available.
3. No blind zone. All the corners should be covered with Wi-Fi;
4. Load balance and high clients capacity are required to handle the burst flow;
5. Higher security level such as Portal, voucher and 802.1x authentication are supported. VLAN can help to isolate hosts in dealing with security.
6. Automatic roaming. The clients can switch to other APs automatically when moving around.

What kind of solution can meet the needs of the restaurant and café network?

Here we provide a full solution including the network topology, product features and parameters.

**Topology**

[Diagram of network topology]

**Tips for deploying this network topology:**

Customers in Cafe/restaurant always require for high quality wireless connection. Clients’ capacity and Wi-Fi interference are the main factors which need to be considered. To improve the clients capacity covered by per unit area, more APs should be installed. We
should avoid to use the same channel on the APs which are close to each other to reduce the interference. As for cafe and restaurant, they are always designed in different patterns, so only field measurement can help to determine the best deployment solution.

What are the highlights of this solution?

This solution combines TP-LINK managed switches, EAPs as well as EAP controller software. And the main features are listed as below:

- **High Availability**

  EAP is designed with professional antennas whose power is variable. To deal with different environment, we can adjust the transmit power to a proper value.

- **Flexible roaming**

  In the EAP wireless framework, different APs can broadcast the same SSID. Clients will switch to different AP automatically while moving around.

- **High reliability**

  Load balance is supported among EAPs, when one AP is overload, the clients will be assigned to other AP nearby to balance the load.

- **High security**

  By using VLAN and multi-SSID, the management network can be isolated from client’s network, so this would greatly help to protect the inner network. Each client is safe as AP isolation feature could help to isolate each other.

- **High expansibility**

  Voucher and portal authentication are supported. The administrator can customize any information such as ads and special offers on the portal page, and redirect the URL as wish. Combined with external portal/radius server, counting and timing functions can be used.

- **Easy to deploy**

  The EAP is ceiling mount designed, PoE supported, good looking and easy to install.

- **Easy Management**

  No need to buy the expensive hardware AC. All the EAPs could be centralized managed by EAP controller software. All the EAP status can be monitored on the web GUI of the controller.
Which product should I choose to build network?

<table>
<thead>
<tr>
<th>Type</th>
<th>Model</th>
<th>Brief Introduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>High performance solution</td>
<td>EAP330</td>
<td>Ceiling mount 802.11AC dual band enterprise AP; speeds up to 1900Mbps; managed by EAP controller software; 802.3at PoE supported with good looking appearance</td>
</tr>
<tr>
<td></td>
<td>TL-SG3424P</td>
<td>Standard PoE switch with 24 gigabit ports. 802.1q 802.3af/at PoE L2 switch, VLAN, IGMP snooping, QoS, LACP supported, variety management methods, easy to configure, suitable for managed PoE network</td>
</tr>
<tr>
<td>Cost effective solution</td>
<td>EAP220</td>
<td>Ceiling mount 802.11N dual band enterprise AP; speed up to 600Mbps; managed by EAP controller software; 802.3af PoE supported with good looking surface</td>
</tr>
<tr>
<td></td>
<td>T1600G-28PS</td>
<td>Standard PoE switch with 24 gigabit ports. 802.1q 802.3af/at PoE L2+ switch, support static routing, VLAN, IGMP snooping, QoS, LACP and ACL etc. variety management methods; easy to configure; suitable for managed PoE network</td>
</tr>
</tbody>
</table>

When deploying a wireless network, various products can be chosen according to the different environment, for example:

- Small Cafe: 802.11n single band ceiling mount designed AP can also meet the demands. It can cover most of the areas as required, enough for normal use.
- Large restaurant: 802.11AC dual band ceiling mount designed AP is recommended. It has stronger anti-interference capacity and can handle more clients, provides better network experience.

How to build a Wireless Network for Chain Store using tp-link products?

Nowadays, retail chains are seen everywhere. They are not large enough, but could provide a wide range of goods or convenient service. In order to provide more attraction and satisfaction to customers, chain store need to consider building an easy-to-use, stable, and affordable wireless network which provides excellent customer experience. tp-link SMB routers and indoor access points are designed with simplicity, high stability and high performance which is a best choice for chain store use.

What are the basic needs of chain store wireless network?

Normally, a chain store wireless network should meet the following needs:
1. Wireless network should cover all over the store without any blind zone.

2. It is the HQ that arranges each store with the same business policy and marketing plan. And wireless network should be designed with the same wireless name, security and the portal authentication rules in different chains.

3. Simple layout, good looking design, PoE supported, and easy to install.

4. Centralized control. We needs all APs to be managed & configured by the HQ uniformly. And only one administrator in HQ could monitor all the APs and give a feedback.

What kind of solution can meet the needs of chain store wireless network?

Here we provide a full solution including the network topology, product features and parameters.

Topology
Tips for deploying this network topology:

When starting to deploy the wireless APs, the location and the amount mainly depend on the signal strength and the interference nearby. The solution is always different due to the variety environment, so it is strongly suggested to deploy the APs and adjust the transmit power and fix signal channel after field measurement. Normally the three points below should be mainly considered:

1. Transmit Power and Coverage

The coverage of an AP is limited, but we can finely adjust the transmit power to optimize it. Because of the limitation of the lobe pattern of the ceiling mount AP, one AP can cover 10-14 meters. While a real coverage for deployment should be decided after the field measurement.

2. Signal Channel Distributing

Another factor must be considered in wireless network deployment is channel collision. Among the 13 channels in 2.4GHz frequency range, only 3 of them won’t overlap with another, and they are well-known channel 1, 6, 11. To avoid channel collision, we should choose channel 1, 6, 11 and place them alternately.

3. Clients number

The AP should have the ability to handle all the clients in its coverage.

One of the schematic diagram shows as below:
What are the highlights of this solution?

The solution we provided has the following features:

- Easy to be deployed
- The EAP adopts ceiling mount design with elegant appearance. It supports PoE standard so that could be deployed easily.
- Auto roaming
- EAP Controller could manage many EAPs with the same SSID, and clients would switch to the other EAPs automatically when they come near.
- High availability
- Support Load Balance that could restrict the maximum number of the clients connected to one signal EAP to avoid overload; Support Band Steering that could lead the clients to connect to 5G network. Support Airtime fairness that could improve the whole network throughput.
- High development
- Support radius, portal, voucher authentication and many other methods. And it could work with the external portal server and external certificate server.
- Easy to manage
- No need to buy the expensive hardware AC. All the EAPs could be centralized managed and monitored on the web GUI of the controller.

Which product should I choose to build the chain store wireless network?

Here is a list which includes the TP-LINK devices for reference:

<table>
<thead>
<tr>
<th>Solution Type</th>
<th>Product classification</th>
<th>Model Number</th>
<th>Solution Type</th>
</tr>
</thead>
</table>
| High performance solution | Router | TL-ER6120 | - Support Intelligent Load Balance, Policy Routing and Link Backup  
- IPsec VPN, PPTP VPN, L2TP VPN  
- Abundant security features including ARP Inspection, DoS Defense, URL/Keyword Domain Filter and Access Control  
- True Physical Stacking technology supports up to 8 units and 320Gbps backplane bandwidth for high scalability and efficient redundancy  
- Support Static Routing and VLAN |

| Core switch | T2700G-28TQ |
- Complete safety protection strategy
- Support Access Control

PoE switch  TL-SG3424P
- Supports 24 802.3at/af-compliant POE+ ports with a total power supply of 320W
- Support Access Control and VLAN
- IP-MAC-Port-VID Binding, ACL, Port Security, DoS Defend, Storm control, DHCP Snooping, 802.1X Authentication and Radius provide you robust security strategies
- Speeds of up to 1.9Gbps over concurrent dual band 802.11ac Wi-Fi with MIMO and Turbo QAM technologies
- Airtime Fairness, Beam forming, and Band Steering Technologies guarantee optimal RF performance for business-level applications
- Link aggregation joins two gigabit Ethernet ports to break the bottleneck in network backhaul capacity
- Power over Ethernet (802.3at) support and simple mounting design allow flexible deployment and convenient installation

EAP  EAP330
- Support Intelligent Load Balance, Policy Routing and Link Backup
- IPsec VPN, PPTP VPN, L2TP VPN
- Abundant security features including ARP Inspection, DoS Defense, URL/Keyword Domain Filter and Access Control

Cost effective solution  Router  TL-ER6020
- True Physical Stacking technology supports up to 8 units and 320Gbps backplane bandwidth for high scalability and efficient redundancy
- Support Static Routing and VLAN
- Complete safety protection strategy
- Support Access Control

- Equipped with 8+ PoE-supported ports to transfer data and power over a single cable
- Plug and play design, no configuration required

- Power over Ethernet (802.3af) support and simple mounting design allow for flexible deployment and convenient installation
- Captive portal provides one convenient method of authentication for Wi-Fi guests

- WPA/WPA2-enterprise, 802.1X with RADIUS secure authentication and rogue access point detection ensure the security of WLAN
- Gigabit Ethernet port enables bandwidth-intensive application or multimedia transferring

Note: When deploying a wireless network, variety of products can be chosen according to the different environment and your own needs. Please don’t use the same mentioned products rigidly.
How to configure Multiple SSIDs with Multiple Subnets on EAP products

In enterprise network, we usually need to divide the network into different VLANs to isolate broadcast domain, suppressing the bad influence of broadcast traffic on network’s performance. The enterprise network is usually divided by different apartments, such as R&D, Marketing, and Product, etc. While nowadays since the wireless devices (like smartphone and laptop) are being used more and more frequently in office, the IT department has to configure each VLAN with the different wireless network (SSID) to meet these office needs. In this document, we will give you a simple step-by-step guide to this kind of configuration by use of TP-Link SMB router/switch and EAP/EAP Controller solution.

Included devices:

AP: EAP Products, such as EAP225

SMB Switch: L2+or L3 Switches, such as T2600-28TS

SMB Router: Multi-net NAT Available Routers, such as TL-ER6120

Topology:
Step 1. Configure Multi-Nets NAT and Static Route on the Gateway Router

(1) Multi-Nets NAT Configuration:

Since there are multiple subnets requiring NAT service, the gateway which works as a NAT device needs to support Multi-Nets NAT. In gateway router’s Web UI, you can configure it in Advanced -> NAT -> Multi-Nets NAT as the figure shows below.

Configure the IP and subnet mask of each subnet, and each item works for one subnet. Leave Interface as LAN.

(2) Static Route configuration

In Advanced -> Routing -> Static Route, you can configure the static route items, the static route configuration helps the data packet from WAN find the next hop, the L3 switch. So in this part, the Destination is the subnet’s network address, and Next Hop is the switch’s IP, and Interface is still LAN.
Now the configuration on the gateway router is done, next we will configure the switch.

**Step2. Configure VLAN and Port Attribute on Switch**

(1) Port Attribute Configuration:

In **VLAN -> 802.1q VLAN -> Port Config**, set the ports connected to EAP as Trunk mode (Port 1/0/10 and 1/0/12 in this topology). The port in Trunk mode can transmit data packets with different VLAN tags. Set PVID as 1.
(2) VLAN Configuration

In VLAN -> 802.1q VLAN -> VLAN Config, add the ports connecting the switch and EAP to VLAN, here we take VLAN 10 and VLAN 20 as examples. VLAN10 and VLAN20 both have member ports 1/0/10 and 1/0/12.
Step 3. Configure L3 Interface and DHCP Server for VLAN on Switch.

(1) VLAN’s L3 Interface Configuration:

In Routing -> Interface -> Interface Config, add L3 interface for the VLAN configured in previous steps. So VLAN can communicate like a normal subnet on IP Layer. **IP Address Mode** usually is selected as **Static**. IP Address and Subnet Mask specify the default gateway and network size for the subnet.
DHCP Server Configuration for each subnet:

After configuring L3 interface for VLAN, we also need to set up DHCP Server for each subnet to assign IP for the wireless clients. In Routing -> DHCP Server -> Pool Setting, you can configure IP address pool for each subnet. Network Address and Subnet Mask specify the size of the address pool. Default Gateway specifies the default gateway for the subnet to which the address pool is bound. The DNS server specifies the corresponding DNS server. These configurations will be sent to the clients during DHCP process.
Note: The **DHCP Server** is **disabled** by default, so after configuring the DHCP address pool, please don’t forget to enable the DHCP Server. Or your wireless devices connected to the SSID can’t obtain an IP address.

**Step4. Static Route Item Configuration on Switch**

In **Routing -> Static Routing -> IPv4 Static Routing Config**, you can add the static route items like the following figure shows. The purpose of this static route item is to forward all the data packets received by the switch to the front gateway router successfully. So the Destination IP 0.0.0.0 means any data packets with any destination IP will be forwarded to 192.168.0.1 (the gateway router).

Then the configuration on the gateway router is also done, and next we will configure the EAP Controller.

**Step5. Configure SSID items with VLAN ID on EAP Controller**

Run EAP Controller and after successfully Adopt EAP, add new SSID in Setting -> Wireless Settings. Add the previously configured VLAN ID in the Wireless VLAN ID section.
Configure two SSIDs, name them as VLAN10 and VLAN20. Use the terminal device to connect the two SSIDs and we can see the IP addresses assigned to the terminal device are 172.16.10.3 and 172.16.20.3. And the terminal can access the Internet which means the configuration has been successful.

How to manage EAPs at different sites across Internet using EAP Controller (via NAT Port Forwarding for Controller Host with DHCP Option138)?

This Article Applies to:

As shown below, HQ and Branch Office are connected with each other. In HQ, there are TP-Link EAP controller, EAP1 and TL-ER6120 (VPN Router) in subnet 192.168.1.0/24. In branch office, there are EAP2, layer 3 switch T2600G-28TS as DHCP Server (supporting DHCP option138) and TL-ER6120 (VPN router) in subnet 192.168.0.0/24.
This document will introduce how to manage EAPs at different sites across Internet using TP-LINK EAP controller (via NAT port forwarding with DHCP option138).

**Step1. Configure Port Forwarding rules on TL-ER6120 in HQ for Controller Host (192.168.1.253)**

1.1 Configure virtual server for TCP&&UDP port, ranging from 29810 to 29814.
Step 2. Disable DHCP Server function on TL-ER6120 in Branch Office.

Step 3. Configurations on T2600G-28TS in Branch Office
3.1 Change switch’s default IP address from 192.168.0.1 to 192.168.0.2 to avoid IP conflict with gateway router.

3.2 Enable DHCP Server Function on T2600G-28TS, and set DHCP Option138 as the WAN IP (172.30.30.138) address of the router that is behind the EAP Controller.
3.3 Configure DHCP IP Address Pool (192.168.0.0/24) for EAP in branch office.
Step 4. Run EAP Controller. The EAP will appear in EAP controller’s “pending” list, which means you can use EAP controller to adopt and manage this EAP now shown as below.
How to manage EAPs at different sites across Internet using EAP Controller (via NAT Port Forwarding for Controller Host with EAP Discover Utility)

This Article Applies to:

As shown below, HQ and Branch Office are connected with each other. In HQ, there are TP-Link EAP controller, EAP1 and TL-ER6120 (VPN Router) in subnet 192.168.1.0/24. In branch office, there are TP-Link EAP discover utility, EAP2 and TL-ER6120 (VPN router) in subnet 192.168.0.0/24.
This document will introduce how to manage EAPs at different sites across Internet using TP-LINK EAP controller (via NAT port forwarding with EAP discover utility).

**Step1. Configure Port Forwarding rules on TL-ER6120 in HQ for Controller Host (192.168.1.253)**

Please go to Advanced – NAT – Virtual Server and configure virtual server for TCP&&UDP port, ranging from 29810 to 29814.
Step2. Settings on PC that is running EAP Discover Utility in Branch Office

Run EAP discover utility, and fill in the Controller Hostname/IP with the WAN IP address of TL-ER6120 in HQ which is 172.30.30.138) and the Username/Password of the EAP (admin/admin by default). At last, click “Apply”.

![EAP Discovery Utility](image-url)
Note: After EAP successfully adopted by EAP Controller, you don’t need EAP Discover Utility any more, thus you can remove the PC which is running the EAP discover utility from the network.

Step3. Run EAP Controller. The EAP which has been configured by EAP discover utility just now will appear in EAP controller’s “pending” list, which means you can use EAP controller to adopt and manage this EAP now shown as below.
How to manage EAPs at different sites across Internet using EAP Controller (via VPN Tunnel with DHCP Option138)?

This Article Applies to:

As shown below, HQ and Branch Office are connected with each other through IPSec VPN tunnel. In HQ, there are TP-Link EAP controller, EAP1 and TL-ER6120 (VPN Router) in subnet 192.168.1.0/24. In branch office, there are EAP2, layer 3 switch T2600G-28TS as DHCP Server (supporting DHCP option138) and TL-ER6120 (VPN router) in subnet 192.168.0.0/24.
This document will introduce how to manage EAPs at different sites across Internet using TP-LINK EAP controller (via VPN Tunnel with DHCP option138). About how to choose VPN Router and set up site to site IPSec VPN tunnel, please refer to: Setting up Site-to-Site IPsec VPN on TP-Link Router

**Step1. Configurations on T2600 switch in Branch Office**

**1.1** Change switch’s default IP address from 192.168.0.1 to 192.168.0.2 to avoid IP conflict with gateway router.
1.2 Enable DHCP Server Function on T2600G-28TS, and set DHCP Option138 as the IP address of Remote EAP Controller Host (192.168.1.253). And then the DHCP Server will tell the EAPs where the EAP Controller is, so that the EAP Controller and EAPs can communicate with each other among different subnets.
1.3 Configure DHCP IP Address Pool (192.168.0.0/24) for EAP in branch office.
Step2. VPN Settings on TL-ER6120 in Branch Office

2.1 Disable DHCP server function on TL-ER6120 in Branch Office.
2.2 Go to VPN -> IKE -> IKE Proposal, and complete IKE Proposal settings shown as below.

2.3 Go to VPN -> IKE -> IKE Policy, and complete IKE Policy settings shown as below.
2.4 Go to VPN -> IPsec -> IPsec Proposal, and complete IPSec Proposal settings shown as below.

2.5 Go to VPN -> IPsec -> IPsec Policy, and complete IPsec Policy settings shown as below. Note: “Remote Gateway” should be the WAN IP address of TL-ER6120 in HQ.
Step 3. VPN settings on TL-ER6120 in HQ are similar with “Step 2”. Here we don’t describe them in detail any more. After all settings, the VPN tunnel will be established between HQ and Branch Office shown as below.

Step 4. Run EAP Controller. The EAP will appear in EAP controller’s “pending” list, which means you can use EAP controller to adopt and manage this EAP now shown as below.
How to manage EAPs at different sites across Internet using EAP Controller (via VPN Tunnel with EAP Discover Utility)?

This Article Applies to:

As shown below, HQ and Branch Office are connected with each other through IPsec VPN tunnel. In HQ, there are TP-Link EAP controller, EAP1 and TL-ER6120 (VPN Router) in subnet 192.168.1.0/24. In branch office, there are TP-Link EAP discover utility, EAP2 and TL-ER6120 (VPN router) in subnet 192.168.0.0/24.

Step1. VPN Settings on TL-ER6120 in Branch Office

1. Go to VPN -> IKE -> IKE Proposal, and complete IKE Proposal settings shown as below.
2. Go to VPN -> IKE -> IKE Policy, and complete IKE Policy settings shown as below.
3. Go to VPN -> IPsec -> IPsec Proposal, and complete IPsec Proposal settings shown as below.

![IPsec Proposal Settings](image)

4. Go to VPN -> IPsec -> IPsec Policy, and complete IPsec Policy settings shown as below. Note: “Remote Gateway” should be the WAN IP address of TL-ER6120 in HQ.
Step 2. VPN settings on TL-ER6120 in HQ are similar with “Step 1”. Here we don’t describe them in detail any more. After all settings, the VPN tunnel will be established between HQ and Branch Office shown as below.
Step 3. Configurations on PC that is running EAP Discover Utility in Branch Office

Run EAP discover utility, and fill in EAP controller’s IP address (192.168.1.253) and the Username/Password of the EAP (admin/admin by default). At last, click “Apply”.

![EAP Discover Utility](image)

**Note:** After EAP successfully adopted by EAP Controller, you don’t need EAP Discover Utility any more, thus you can remove the PC which is running the EAP discover utility from the network.

Step 4. Run EAP Controller. The EAP will appear in EAP controller’s “pending” list, which means you can use EAP controller to adopt and manage this EAP now shown as below.
How to manage EAPs in different subnets using EAP Controller (via DHCP option 138)?

This Article Applies to:

In the network topology below, there are three VLANs (three subnets), which are VLAN1 (192.168.0.0/24), VLAN2 (192.168.1.0/24) and VLAN3 (172.30.30.0/24). These three VLANs (three subnets) are divided by TP-Link L3 Switch (T2600G-28TS). Now we want TP-Link EAP Controller in VLAN1 (192.168.0.0/24) to manage EAP in VLAN2 (192.168.1.0/24). The gateway Router is TP-Link SMB router TL-ER6120.

This document will introduce how to manage EAPs in different subnets using TP-Link EAP controller (via DHCP option 138). For the configurations of multi-nets NAT function on TP-LINK SMB router, please refer to:

How to build up a multi-nets network using the Multi-nets NAT feature on TP-Link router with a L3 switch?
Step 1. Configurations on Layer 3 switch

1. Create VLAN2 & VLAN3. VLAN2 includes port 4, and VLAN3 includes port 7. The detailed VLAN settings are shown as below. Note: port 4/7/16 should be configured as "Access" type.

2. Enable IP interface for VLAN1 & VLAN2 & VLAN3, and configure relevant IP addresses for these three interfaces shown as below.
3. Configure the static default routing entry which leads to the gateway router.

4. Enable DHCP Server function, and configure 192.168.1.0/24 IP address pool for EAPs. For Option138, you should fill in the IP address of EAP Controller Host which is “192.168.0.253”. And then the DHCP Server will tell the EAPs will the EAP Controller is, so that the EAP Controller and EAPs can communicate with each other among different subnets. **Note:** don’t forget to fill in the DNS server address.
### DHCP Server Configuration

**Global Config**

- **DHCP Server**: Enable/Disable
  - Option 60: (Optional)
  - Option 138: 192.168.0.253 (Optional. Format: 192.168.0.1)

**Ping Time Config**

- Ping Packets: (0-10 packets, 0 for disable ping)
- Ping Timeout: 100 (100-10000 milliseconds)

**Excluded IP Address**

- **Start IP Address**: (Format: 192.168.0.1)
- **End IP Address**: (Format: 192.168.0.1)

**Excluded IP Address Table**

<table>
<thead>
<tr>
<th>Select</th>
<th>ID</th>
<th>Start IP Address</th>
<th>End IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No entry in the table.
Step2. Configurations on SMB Router

1. Configure Static Routing for VLAN1 and VLAN2 subnets.
2. Configure multi-nets NAT for 192.168.0.0/24 and 192.168.1.0/24 subnets.

Step 3. Run EAP Controller. The EAP will appear in EAP controller’s “pending” list, which means you can use EAP controller to adopt and manage this EAP now shown as below.
How to manage EAPs in different subnets using EAP controller (via EAP Discover Utility)?

This Article Applies to:

In the network topology below, there are three VLANs (three subnets), which are VLAN1 (192.168.0.0/24), VLAN2 (192.168.1.0/24) and VLAN3 (172.30.30.0/24). These three VLANs (three subnets) are divided by TP-Link L3 Switch (T2600G-28TS). Now we want TP-Link EAP Controller in VLAN1 (192.168.0.0/24) to manage EAP in VLAN2 (192.168.1.0/24). The gateway Router is TP-Link SMB router TL-ER6120.

This document will introduce how to manage EAPs in different subnets using TP-Link EAP controller (via EAP discover utility). For the configurations of multi-nets NAT function on TP-LINK SMB router, please refer to:

How to build up a multi-nets network using the Multi-nets NAT feature on TP-Link router with a L3 switch?

Step1. Configurations on Layer 3 switch
1. Create VLAN2 & VLAN3. VLAN2 includes port 4 & port 5, and VLAN3 includes port 7. The detailed VLAN settings are shown as below. Note: port 4/5/7/16 should be configured as “Access” type.

2. Enable IP interface for VLAN1 & VLAN2 & VLAN3, and configure relevant IP addresses for these three interfaces shown as below.
3. Configure the static default routing entry which leads to the gateway router.

4. Enable DHCP Server function, and configure 192.168.1.0/24 IP address pool for EAPs. Note: don’t forget to fill in the DNS server address.
Step2. Configurations on SMB Router

1. Configure Static Routing for VLAN1 and VLAN2 subnets.
2. Configure multi-nets NAT for 192.168.0.0/24 and 192.168.1.0/24 subnets.

Step3. Configurations on EAP Discover Host

1. Connect the PC that is running EAP Discover Utility to switch’s port 5, and connect EAP to switch’s port 4. In this way, both EAP discover utility and EAP are in the same subnet (192.168.1.0/24). Now open EAP Discover Utility to let it discover EAP shown as below.
After EAP discover utility finds the EAP, click “Manage” icon, and then fill in the IP address of EAP controller Host and the Username/Password of the EAP (admin/admin by default) to let EAP controller finds & manages this EAP.
Note: After EAP successfully adopted by EAP Controller, you don’t need EAP Discover Utility any more, thus you can remove the PC which is running the EAP discover utility from the network.

Step4. Run EAP Controller. The EAP which has been configured by EAP discover utility just now will appear in EAP controller’s “pending” list, which means you can use EAP controller to adopt and manage this EAP now shown as below.
How to set up different SSIDs and Passwords for each EAP through EAP Controller?

This Article Applies to:

In many hotels and shopping malls, generally there is only one single SSID and Password for wireless network access with Portal authentication (FAQ896). However, when it turns to large-scale network deployment, a single SSID may not satisfy our requirement, since we shall have different management for different places. For instance, we want to allow people could access to the FTP server in site A while couldn’t in site B. In such case, we could set different SSIDs and Passwords for EAP in site A and site B, and set access control (FAQ1060).

Here are two ways to set up different SSIDs and Passwords via EAP Controller. Take two devices for example, we need to set different SSIDs and Passwords (SSID1 and SSID2) to them.

1. SSID Override
Note: SSID Override function is suitable for all versions of EAP Controller.

Configure the EAP Device 1, go to **Configuration -> WLANS**, choose the frequency 2.4GHz or 5GHz to be configured and click **Action**.

Enable **SSID Override on this AP** and type in the new SSID and Password you want to override the previous one in this configuring EAP device.

Similarly, we could set the SSID2 on the Device 2. And then we have different SSIDs and Passwords for the two EAP devices.

**Note:** If you set SSID Override for all EAP in this WLAN, then your EAP devices would not broadcast SSID as you set in Basic Wireless Setting.

**2. WLAN Group**
Note: WLAN Group function is suitable for EAP Controller V2.2.3 or higher version.

Configure WLAN Group on the EAP Controller to group your wireless network.

Go to **Wireless Settings -> Basic Wireless Setting**, choose the frequency 2.4GHz or 5GHz and then click **Add** in WLAN Group. Here we choose 2.4G for instance.

![Wireless Settings](image)

Type in the WLAN Group Name as you want. Here we take SSID1 as example.

![WLAN Group](image)

Then choose this group and add a new SSID account.

![Wireless Settings](image)

Fill in the SSID and Password that you like for Group SSID1.
After finish Group SSID1, we can set another WLAN Group as SSID2 with different SSID and Password.

Then go to Device 1 Configuration -> WLANS, select SSID1 in WLAN Group.
We choose SSID2 for Device 2. Then we can see Device 1 and Device 2 will have different WLAN Groups.

Comparing the two ways to set different SSID and Password for each EAP: the SSID Override is recommended if you just need to set different SSIDs and Passwords for a few devices; but when you need a large quantity of EAP devices to be set, the WLAN Group would be a better choice.

How to configure Link Aggregation for EAP330?

This Article Applies to:

**Introduction:** EAP330 has two gigabit Ethernet ports which can be used together after link aggregation (LAG) is configured. LAG can provide a more reliable wired connection. When one of the two links is down, there is another link available, so the EAP330 won’t lose wired connection. And LAG can also balance the load which can make full use of the two links.

The LAG setting is called “Trunk” in EAP330. This function can only be used along with a switch that can configure Static LAG rules on its ports.
Note: It is strongly recommended to only connect ETH1 to Port22 before you finish the whole configuration, because the two links without LAG configured will cause a loop problem which may reduce the performance of the switch.

Step 1:

Login the Web page of EAP330. Here is an introduction about how to login the Web page:

How do I login to the web management page of the EAP Series?

Step 2:

After login the management page of EAP330, you can find the Trunk configuration in Management -> Trunk -> Trunk Settings, then click Enable to enable this function on EAP330. About the Mode, you can select whichever mode available. And don’t forget to click Save to save your configuration.

After the configuration on EAP330 is finished, next step is to LAG on switch.

Step 3:

Login the interface of switch.
Since EAP330 only supports **Static Link Aggregation**, please doesn’t choose dynamic link aggregation like LACP (Link Aggregation Control Protocol).

In **Switching -> LAG -> Static LAG -> LAG Config**, you can choose any **Group Number** available. In **Member Port**, you are supposed to select the two ports connected to the EAP330 as the member ports of LAG group, in this case they are Port22 and Port24. And click **Apply**.

**Note:** In static link aggregation, the configuration of the member ports need to be identical.

**Step 4:**

Now you can connect ETH2 to Port24. So far all the settings are completed.

But how do I know if LAG is successfully configured?

When you connect ETH2 to Port24 without LAG configured, the light of the two ports on switch will keep flashing abnormally fast. After the successful configuration, the light will turn to be normal.
How to deploy EAP controller on a private cloud (AWS EC2)?

This Article Applies to:

Overview

EAP controller (2.0.3 and newer non-cloud versions) supports L3 management. An EAP controller can manage EAPs of multiple remote networks crossing internet. However, it will require to set up port-forwarding or VPN tunnels if there are NAT firewalls in front of EAP controller. (See FAQ913)
Some users may want to install the EAP controller on a private cloud platform, so as to achieve L3 management from anywhere without hosting a LAN PC. Moreover, if the cloud server comes with public IP addresses, it can also save the work of setting up port-forwarding or VPN tunnels for penetrating through NAT firewalls.

A Workaround

Although EAP controller is a non-cloud-application, it can still be installed on a cloud-based Windows host, which can be a workaround to achieve part of the demand.

In this article, readers will learn how to install and run an EAP controller on an AWS EC2 Windows host.
Note: TP-LINK will develop a true cloud-based EAP controller service in the future, so the workaround going to be introduced in this article is only an interim solution before the final release of the true cloud-based controller service.

About AWS EC2

Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) cloud. One significant feature of EC2 is virtual computing environments, known as instances, which includes Windows virtual hosts.

The Amazon Web Services (AWS) Free Tier provides new registered users with 750 hours per month of Windows t2.micro instance usage for free within certain usage limits. You are now strongly recommended to refer to the page of AWS Free Tier for detailed information. All information given herein are subject to changes or update by AWS without prior notice.

Here we take AWS EC2 as an example to introduce how to install and run an EAP controller on a private cloud.

Part 1: Get AWS EC2 Ready

1.1 Create an AWS account

Note: Skip this step 1 and login directly if you have already an AWS account.

- Open http://aws.amazon.com/, and then choose Create an AWS Account.
- Follow the online instructions to create an AWS account.

About Region

Amazon has data centers in different areas of the world (for example, North America, Europe, and Asia). Correspondingly, Amazon EC2 is available to use in different regions. By launching instances in separate regions, you can design your application to be closer to specific customers or to meet legal or other requirements.

You can choose a preferred region before creating a Windows instance.
1.2 Launch a Windows instance

Note: Skip this step 2 if you have already a Windows instance available for running an EAP controller.

- Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.

From the console dashboard, choose Launch Instance.

- The Choose an Amazon Machine Image (AMI) page displays a list of basic configurations, called Amazon Machine Images (AMIs), which serve as templates for your instance. Select the AMI for Microsoft Windows Server. Notice that in this tutorial we choose Windows Server 2012 R2 marked "Free tier eligible" as an example.

- On the Choose an Instance Type page, you can select the hardware configuration of your instance. Select the t2.micro type, which is selected by default. Notice that this instance type is eligible for the free tier.
Choose **Review and Launch** to let the wizard complete the other configuration settings for you.

On the **Review Instance Launch** page, under Security Groups, you'll see that the wizard created and selected a security group for you. Now choose **Edit security groups**.

**Security Group Settings (Important)**

A security group is a set of firewall rules that control the traffic for your instance. To achieve the goal of managing remote EAPs, add rules that allow unrestricted access to the following ports.

- TCP PORT 8088
- TCP PORT 8043
- UDP PORT 29810
- TCP PORT 29811
- TCP PORT 29812
- TCP PORT 29813

Also allow RDP access for Windows Remote Desktop access.

Then choose **Review and Launch**.

On the **Review Instance Launch** page, choose **Launch**.

When prompted for a key pair, select the key pair that you created if you have one. Otherwise, you can create a new key pair. Select **Create a new key pair**, enter a name for the key pair, and then choose **Download Key Pair**. This is the only chance for you to save the private key file, so be sure to download it. Save the private key file in a safe place. You'll need to provide the name of your key pair when you launch an instance and the corresponding private key each time you connect to the instance.

Note: Don't select the **Proceed without a key pair** option. If you launch your instance without a key pair, then you can't connect to it.

When you are ready, select the acknowledgement check box, and then choose **Launch Instances**.
A confirmation page lets you know that your instance is launching. Choose **View Instances** at the bottom of the page to close the confirmation page and return to the EC2 console.

Back to **EC2 console → Instances** menu, you can see that the newly launched Windows instance is now running.

1.3 Assign an Elastic IP address for the Windows host

Although it shows that the instance is assigned a public IP address now, but this default IP address is not permanent. Once you shut down or reboot the instance, it can be released or changed to another one.

To have static public IP address for the Windows, we need to create an Elastic IP address and assign it to the instance. An Elastic IP address is a static public IP address that you can allocate to your account. You can associate it to and from instances as you require, and it's allocated to your account until you choose to release it.

In the EC2 console, navigate to **NETWORK & SECURITY → Elastic IPs**, the list should be empty if you haven’t create any. Now click Allocate New Address, confirm to allocate when prompted.

Then a new Elastic IP address entry will be shown in the list.

Select the entry, click **Actions → Associate Address**.
Click the **Instance** input box and choose the Windows instance in the drop-down list. Click **Associate** to associate this Elastic IP address to the Windows instance.

Go back to Instances menu, now you can see the Windows instance is now associated with the Elastic IP address.

With all the above steps, the AWS EC2 Windows host is now ready.

**Part 2: Install EAP controller on EC2**

**2.1 Connect to Windows through Remote Desktop**
In EC2 console, select the Windows instance and click Connect.

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file as the prompted instruction says.

Before actually connect through RDP, you must Get Password using your Key file which is saved in previous steps. Upload the Key file and then choose Decrypt Password to get your password.

With the provided username/password now you can connect to the Windows instance through remote desktop (RDP) client from any remote PC at anywhere you like.
2.2 Download and Install EAP controller on EC2

Note: When the **IE ESC** is enabled, you get pop-up all the time and you are asked to add every new URL to the IE trusted sites zone. You may want to disable IE ESC temporarily for the convenience of downloading the EAP controller from TP-LINK official websites.

To disable IE enhanced security in windows server 2012 R2, launch the **Server Manager**, on the left hand side click on **Local Server**. On the right hand side click on the **On** link next to **IE Enhanced Security Configuration**.
In the prompted windows, click on **Off** to turn off the **IE ESC**.

Then visit **www.tp-link.com**, search any model of the EAP series, e.g. EAP220. In the product page, navigate to **Support** page and download the latest EAP controller under **Utility** tab.

After download, extra the zip and install the EAP controller through the setup wizard.

After installation, launch EAP controller.exe and finish the Quick Setup Wizard. Note down the **username/password** and then keep the EAP controller running.

Now, everything of the EC2 instance is ready. You can now leave the EC2 running since its settings are all finished.

You can access the controller’s web UI from a remote PC through the URL **Https://Elastic IP:8088**

The next steps are performed at the EAP sides.
Part 3: Settings at EAP side

Still take the following topology as an example.

First of all, the EAPs must have internet access, which means you should assign them correct IP/gateway parameters through DHCP (recommended) or manual configuration. The EAPs default to DHCP so this shouldn’t be a problem as long as there is proper DHCP service in LAN.

Then comes the most important part. At EAP sides the controller’s public IP address, in the above example 54.169.x.x need to be configured into each EAP device, so that the EAPs can know where to find the EAP controller through internet. There are two methods to configure the controller’s IP address into the EAPs.

Method 1. Via EAP Discover Utility
1. Download EAP controller from TP-LINK website. Install EAP controller on a PC at site Branch 1. The PC should be in the same IP subnet as EAPs. In the example it is PC1.

2. Run EAP Discover Utility (You will find it at C:\Program Files (x86)\TP-LINK\EAP Controller\bin if you haven’t changed the installation path). All the EAP devices in the local network will be listed.

3. Since all the EAPs have the same Username and Password, you may use Batch Setting to set controller IP for them all. If your EAP devices have different username and password you can use the manage button to set the controller hostname/IP respectively.

4. Wait until the status show as Setting Succeed.
5. A while later the EAPs will be displayed as pending APs on controller waiting for adoption and management. You can adopt them using the EAP’s username/password. (Default: admin/admin)

6. For EAPs located in Branch 2 use the same methods to set the controller’s IP address.

**Method 2. Set option 138 on DHCP server**

EAP devices can request controller IP via option 138 through DHCP.

Take Branch 1 as example.

1. Suppose the DHCP server in Branch 1 is capable of configure variable DHCP options. Set the controller IP as the option 138 value on it.
2. All the EAPs in the local network will be aware of the controller’s IP address automatically through DHCP communication right after boot up.

How to set option 138 on DHCP server varies from implementation to implementation which is out of the scope of this document. Please refer to DHCP server documentation for help. The below two examples used in our test are for your reference.

**Cisco IOS CLI:**

```
ip dhcp pool test

network 192.168.1.0 255.255.255.0

default-router 192.168.1.1
dns-server 8.8.8.8

option 138 ip 56.169.x.x
```

For more details please refer to [Cisco website](#).

**MikroTik RouterOS CLI:**

```
#Assume you have already setup a dhcp server with item number 0

#0xC0000002 equeals 56.169.x.x

/ip dhcp-server option add code=138 name=controller value=0xC0000002

/ip dhcp-server network set 0 dhcp-option=controller
```

For more details please refer to [MikroTik manual](#).

This article applies to EAP controller 2.0.3 and later non-cloud-based controller.
How to build a Wireless Network for School Canteen using tp-link products?

This Article Applies to:

Nowadays, more and more schools have the need to build up their own Canteens. When students waiting in line to get their food or eating, they would use smart phones to surf the internet and some may even use laptop. So if school could deploy wireless networks that would improve satisfaction of the students. What’s more, school may also publish announcements through wireless network.

What are the basic needs of school canteen wireless network?

A school canteen wireless network should meet the following needs:

1、Wireless network could cover all the store without any dead corner.

2、Auto switch access point when students are moving, network keeps fluent.

3、It is crowded when students eat lunch, so it requires that AP could support more clients and Load Balance feature.

4、Concise layout, good looking, PoE supported, and easy to install.

5、It needs all APs could be managed & configured uniformly. And just use one controller could monitor the whole APs and give a feedback.

What kind of solution can meet the needs of school canteen wireless network?

Topology
Tips for deploying this network topology:

When starting to deploy the wireless AP, the positions to deploy the AP and the amount needed depends on the signal strength and the interference. The result is always different due to different environment, so it is strongly suggested to deploy the AP and adjust the transmit power and signal channel after a professional field measurement. Normally the three points below should be mainly considered:

1. **Transmit Power and Coverage**

   The coverage of an AP is limited, but we can fine adjust it by the transmit power. As the limitation of the lobe pattern of the ceiling mount AP, one AP can cover 10-14 meter. While a real coverage deployment should be decided after the field measurement.

2. **Signal Channel Distributing**

   Another factor must be considered in wireless network deployment is channel collision. All over the 13 channels in 2.4GHz frequency range, only 3 channels won’t overlap each other, which are channel 1, 6, 11. To avoid channel collision, we should choose channel 1, 6, 11 and place them alternately.

3. **Clients number**

   The AP should have the ability to carry all the clients in its coverage in the dormitory.
What are the highlights of this solution?

- **Easy to deploy**

The EAP is ceiling mount designed with beautiful appearance. It supports PoE standard so that could be deployed easily.

- **Auto roaming**

EAP Controller could manage many EAPs with the same SSID, clients would switch to the other EAPs automatically when they come near the other EAPs.

- **High availability**

Support Load Balance that could restrict the maximum number of the clients connected to one signal EAP to avoid overload; Support Band Steering that could lead the clients connect to 5G network. Support Airtime fairness that could improve the whole network throughput.

- **High development**

Support radius, portal, voucher authentication and so on. And it could work with the external portal server and external certificate server.

- **Easy to manage**
No need to buy the expensive hardware AC. All the EAP could be centralized managed by a free EAP controller software. All the EAP status can be monitored on the web GUI of the controller.

Which product should I choose to build this school canteen wireless network?

Here is a list which includes the TP-LINK devices for reference:

<table>
<thead>
<tr>
<th>Type</th>
<th>Model</th>
<th>Brief Introduction</th>
</tr>
</thead>
</table>
| High performance solution     | TL-ER6120   | - Support Intelligent Load Balance, Policy Routing and Link Backup  
- IPsec VPN, PPTP VPN, L2TP VPN  
- Abundant security features including ARP Inspection, DoS Defense, URL/Keyword Domain Filter and Access Control  
- True Physical Stacking technology supports up to 8 units and 320Gbps backplane bandwidth for high scalability and efficient redundancy  
- Support Static Routing and VLAN  
- Complete safety protection strategy  
- Support Access Control |
|                               | T2700G-28TQ | - Supports 24 802.3at/af-compliant POE+ ports with a total power supply of 320W  
- Support Access Control and VLAN  
- IP-MAC-Port-VID Binding, ACL, Port Security, DoS Defend, Storm control, DHCP Snooping, 802.1X Authentication and Radius provide you robust security strategies  
- Speeds of up to 1.9Gbps over concurrent dual band 802.11ac Wi-Fi with MIMO and Turbo QAM technologies  
- Airtime Fairness, Beamforming, and Band Steering Technologies guarantee optimal RF performance for business-level applications  
- Link aggregation joins two gigabit Ethernet ports to break the bottleneck in network backhaul capacity  
- Power over Ethernet (802.3at) support and simple mounting design allow for flexible deployment and convenient installation |
|                               | TL-SG3424P  | - Support Access Control and VLAN  
- IP-MAC-Port-VID Binding, ACL, Port Security, DoS Defend, Storm control, DHCP Snooping, 802.1X Authentication and Radius provide you robust security strategies  
- Speeds of up to 1.9Gbps over concurrent dual band 802.11ac Wi-Fi with MIMO and Turbo QAM technologies  
- Airtime Fairness, Beamforming, and Band Steering Technologies guarantee optimal RF performance for business-level applications  
- Link aggregation joins two gigabit Ethernet ports to break the bottleneck in network backhaul capacity  
- Power over Ethernet (802.3at) support and simple mounting design allow for flexible deployment and convenient installation |
|                               | EAP330      | - Support Access Control and VLAN  
- IP-MAC-Port-VID Binding, ACL, Port Security, DoS Defend, Storm control, DHCP Snooping, 802.1X Authentication and Radius provide you robust security strategies  
- Speeds of up to 1.9Gbps over concurrent dual band 802.11ac Wi-Fi with MIMO and Turbo QAM technologies  
- Airtime Fairness, Beamforming, and Band Steering Technologies guarantee optimal RF performance for business-level applications  
- Link aggregation joins two gigabit Ethernet ports to break the bottleneck in network backhaul capacity  
- Power over Ethernet (802.3at) support and simple mounting design allow for flexible deployment and convenient installation |
<table>
<thead>
<tr>
<th>Model</th>
<th>Features</th>
</tr>
</thead>
</table>
| TL-ER5120 | • Support Intelligent Load Balance, Policy Routing and Link Backup  
               • Abundant security features including ARP Inspection, DoS Defense, URL/Keyword Domain Filter and Access Control  
               • True Physical Stacking technology supports up to 8 units and 320Gbps backplane bandwidth for high scalability and efficient redundancy |
| T1600G-28TS| • Support Static Routing and VLAN  
               • Complete safety protection strategy  
               • Support Access Control |
| Cost effective solution TL-SG1008PE | • Equipped with 8 PoE+ supported ports to transfer data and power over a single cable  
               • Plug and play design, no configuration required  
               • Power over Ethernet (802.3af) support and simple mounting design allow for flexible deployment and convenient installation  
               • Captive portal provides one convenient method of authentication for Wi-Fi guests  
               • WPA/WPA2-enterprise, 802.1X with RADIUS secure authentication and rogue access point detection ensure the security of WLAN  
               • Gigabit Ethernet port enables bandwidth-intensive application or multimedia transferring |
| EAP220    | • Support Access Control  
               • Plug and play design, no configuration required  
               • Power over Ethernet (802.3af) support and simple mounting design allow for flexible deployment and convenient installation  
               • Captive portal provides one convenient method of authentication for Wi-Fi guests  
               • WPA/WPA2-enterprise, 802.1X with RADIUS secure authentication and rogue access point detection ensure the security of WLAN  
               • Gigabit Ethernet port enables bandwidth-intensive application or multimedia transferring |