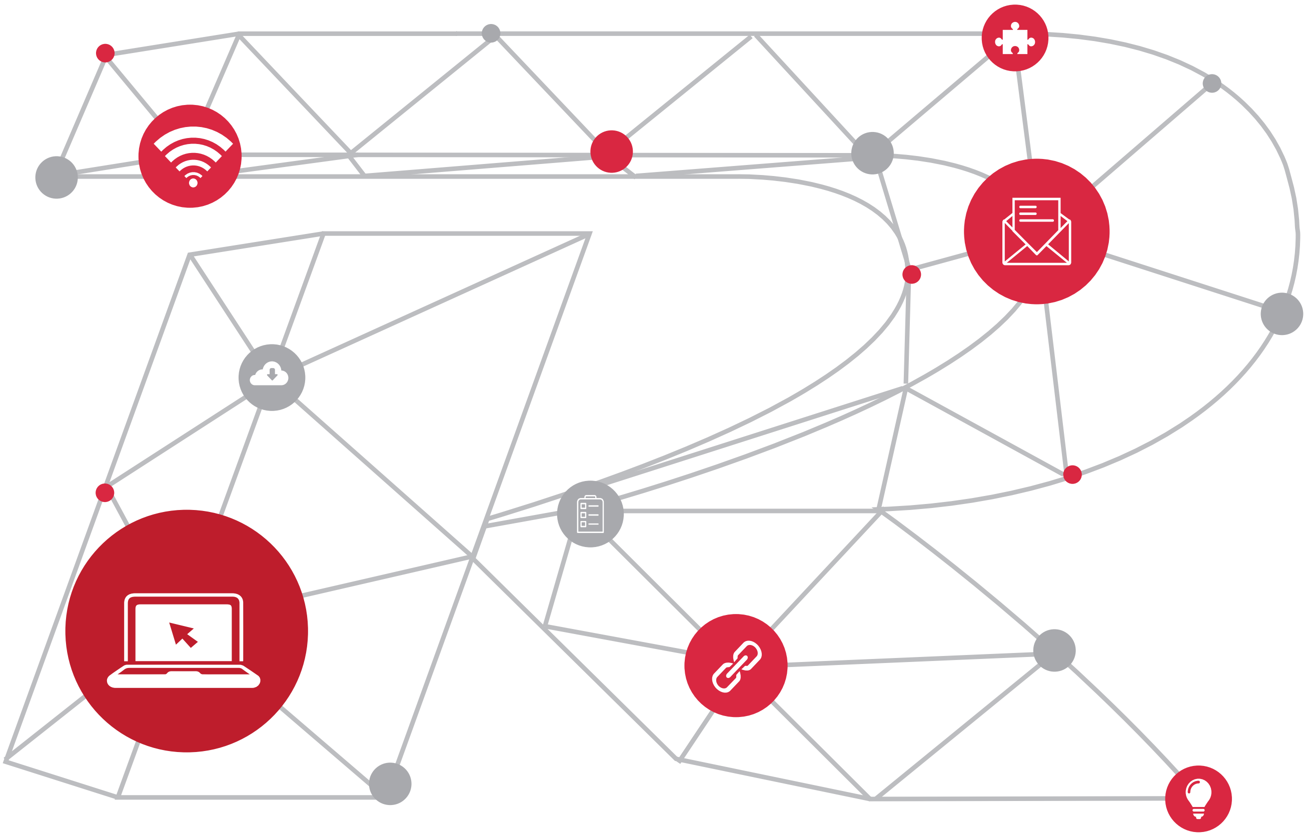
Ruijie Multi-AC Layered Architecture

White Paper



Contents

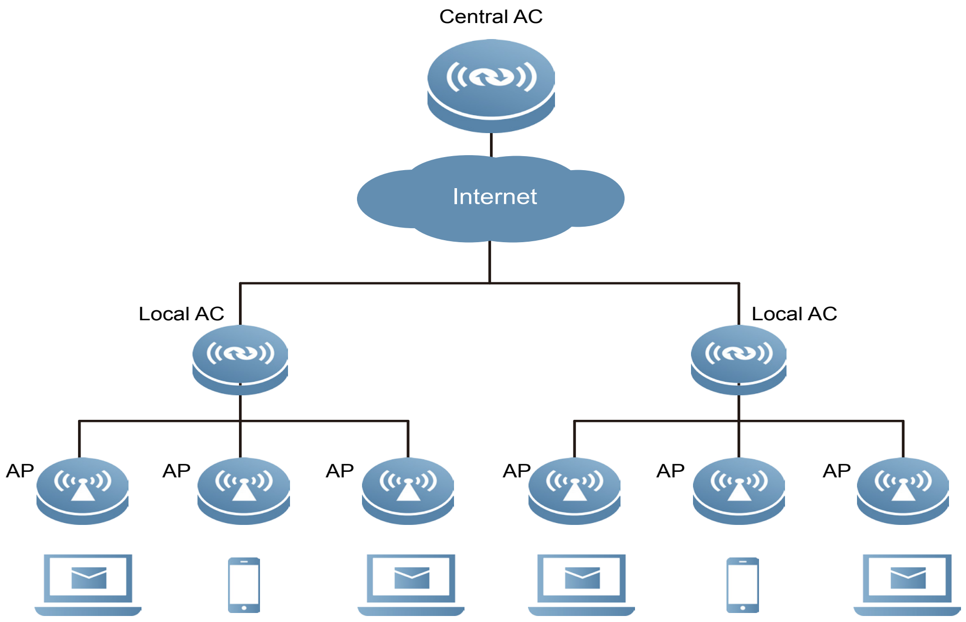
Introduction

This document describes a multi-access-controller (AC) layered architecture designed to address branch management and backup issues.

• Background

The multi-AC layered architecture integrates centralized management and distributed forwarding. (Centralized or distributed control is implemented at the control layer.) This architecture consists of a central AC (with high performance) and multiple local ACs (small-sized). The central AC manages central access points (APs) and local ACs, whereas local ACs manage only local APs. The following figure shows the network diagram of the multi-AC layered architecture.

Figure 1



This architecture is applicable in the following scenarios:

Scenario 1: Metropolitan area network (MAN) for general education

A high-performance AC (stand-alone AC or virtual access controller [VAC]) is deployed at the bureau of education, and small-sized ACs (stand-alone ACs) are deployed at schools. The requirements are as follows:

* **Disaster recovery**

When local ACs fail, local APs can connect to the central AC to continue to use the wireless network. The central AC may be a stand-alone AC or a VAC. The central AC controls network access and supports two types of authentication account. One is the account granted by the bureau of education, the other is the account used under Ruijie SMP+ESS+IPC solution, whereby the Identity & Policy Center (IPC) synchronizes the local ESS account and central SMP account so that the local account can be authenticated at the central AC. Disaster recovery does not require smooth switchover. That is, local ACs do not need to synchronize entries with the central AC online in real time. Users can directly go online after switchover.

* **Unified upgrade**

Local ACs and APs can be upgraded in a unified manner from the central AC. (Major version upgrade and patch upgrade are supported.) The models of local ACs and APs may be diverse.

* **License sharing**

The central AC and local ACs share the AP license. Purchase of two licenses is not required.

* **Account roaming**

The bureau of education requires each school to issue a service set identifier (SSID) to be authenticated at the bureau of education so that a station (STA) can use one account to perform access authentication with the bureau of education and schools for inter-school roaming (not 802.11 roaming). The bureau of education has its own authentication server, for example, SMP. After authentication, data may be forwarded locally or centrally.

* **Permission management**

The bureau of education conducts weak management of schools. Each school has its own permissions and can set a local SSID and implement authentication. The bureau of education does not interfere but only needs to know the online status of small-sized ACs, APs, and STAs.

Scenario 2: Wireless office network interconnecting the headquarters and branches

A high-performance AC (stand-alone AC or VAC) is deployed at the headquarters, and small-sized, stand-alone ACs are deployed at branches. The requirements are as follows:

* **Disaster recovery**

Same as the general education scenario

* **Unified upgrade**

Same as the general education scenario

* **License sharing**

Same as the general education scenario

* **Unified authentication**

The headquarters conducts strong management of wireless access by branches. Accounts are managed on the authentication server of the headquarters in a unified manner. Branches must be authenticated at the headquarters for network access. After authentication is passed, data is forwarded locally.

* **Permission management**

The headquarters manages branches in two modes:

Strong management. The central AC defines the wireless configurations of branch ACs. Branch ACs automatically download wireless configurations (AP group, WLAN mapping, SSID, and authentication data) after connecting to the central AC. Branch ACs only have the wired configuration permission, for example, configuring address pools and routes. The wireless configuration permission is disabled on branch ACs. For example, branch ACs cannot configure SSIDs.

Weak management. Branch ACs need to download wireless configurations from the headquarters and have specified wireless configuration permissions, for example, configuring SSIDs.

In both modes, the central AC needs to display the connection status of branch ACs, APs, and STAs.

Note: Branches can be connected to the headquarters through a virtual private network (VPN), internal routes, or egress network address translation (NAT) mapping configured on the central AC (branch ACs can connect to the mapping address).

Requirement summary:

Phase 1: Meet the common and basic requirements.

* **Disaster recovery**

The central AC supports the VAC architecture and 1:N hot standby between the central AC and local ACs. N is 128 currently.

* **Unified upgrade**

Local ACs and APs are upgraded in a unified manner from the central AC. (Major version upgrade and patch upgrade are supported.)

* **License sharing**

The central AC and local ACs share the AP license.

* **Basic management**

The central AC needs to display the connection status of branch ACs, APs, and STAs.

* **Distributed authentication**

Implemented by Ruijie SMP+ESS+IPC solution.

Phase 2: Deliver competitive values.

* **Unified authentication**

Authentication on local ACs is transferred to the central AC, which supports portal authentication, MAB authentication, and 802.1x authentication.

- **Strong management**

The central AC defines the wireless configurations of branch ACs. Local ACs automatically download wireless configurations from the central AC.

The central AC defines the permissions of local ACs, including whether to allow local ACs to perform wireless configuration. If the configurations on local ACs conflict with the configurations delivered by the central AC, the conflicting configurations are disabled.

The Per-user PSK (PPSK) solution is developed based on the preceding requirements. This solution has the following features:

- **Each STA has a key.**
- **No authentication server is required.**
- **External STAs cannot set up Wi-Fi connection even with the shared key.**
- **This solution is easy to use and delivers the same experience as that of WPA/WPA2-PSK.**

• Implementation

The multi-AC layered architecture is unavailable in China. Ruckus has a similar architecture with the following implementation:

- **Two SSIDs are created: employee-registered SSID and office SSID.**
- **Employee STAs log in to register an SSID, enter the account name, and obtain a password for network access.**
- **Employee STAs connect to the office SSID and enter the password.**

This solution enables the use of one key in the entire network, but does not support Wi-Fi master key sharing. An STA receives and memorizes two SSIDs. When entering the workplace, the STA may connect to either of the two SSIDs. If it connects to the registered SSID, it cannot set up a network connection. This problem is not easy to detect and will affect work.

• Application Prospect

The multi-AC layered architecture has a positive application prospect in medium- and small-sized enterprises for the following reasons:

- **Low cost: No authentication server is required.**
- **Low usage barrier: This architecture is easy to use and delivers the same experience as that of WPA/WPA2-PSK.**
- **High security: This architecture prevents Wi-Fi hacking.**

Basic Knowledge

Users only need to have knowledge of WPA/WPA2-PSK to understand PPSK. Complex wireless knowledge is not required.

Technical Principles

• Stand-alone

* Password acquisition for network access

The administrator allocates an account and a password to a new employee and imports this account and password on the AC. The AC automatically generates a unique Wi-Fi key for the account and then the administrator allocates this key to the employee. (The Wi-Fi keys generated for different accounts do not conflict with each other and have sufficient security strength.)

* STA access to the office network

Initial access:

1. The STA connects to the office SSID and enters the Wi-Fi key.
2. The AC checks the local database and finds that the STA is not bound. Then the AC traverses the Wi-Fi key list to find the matched Wi-Fi key and implements normal PSK authentication.
3. After the STA passes the authentication, the AC binds the MAC address of the STA to the corresponding account.
4. The AC determines that the STA accesses the network for the first time and continues to verify the user identity. Until now the STA still cannot access the network. The user needs to open the browser on the STA and enters the account name and password on the account verification page that appears after redirection. After the STA passes identity authentication, the AC permits the STA to pass and access the network. If authentication fails, the STA cannot access the network.

Subsequent access:

1. The STA connects to the office SSID.
2. The AC checks the MAC address of the STA and determines that the STA has been bound before. Then the AC uses the MAC address to quickly find the corresponding Wi-Fi key for PSK authentication.
3. After PSK authentication is passed, the AC determines that the STA has been bound before and permits the STA to access the network without identity authentication.

* STA unbinding

By default, one account can be bound with three STAs. If this limit is exceeded (for example, the user changes his/her mobile phone), excessive STAs must be unbound from the AC. The unbinding process is as follows:

1. The AC provides a self-service page.
2. The user opens the self-service page on a bound STA after connecting to the network and selects Unbind. When an STA connects to the network for the first time, a portal authentication page is pushed to this STA. After the user enters the account name and password, if the AC verifies that the maximum number of bound STAs is exceeded, it redirects the STA to the self-service page for deregistration.
3. The deregistration page lists the information of bound STAs, including the MAC address, STA type, and registration time. The user can select the STAs to be unbound. After unbinding, the AC can bind new STAs.

* **Password change**

An employee can open the self-service page on any bound STA to change the password. After the password is changed, all bound STAs need to perform identity authentication when connecting to the network next time.

* **Wi-Fi key lost**

The Wi-Fi key has length and complexity requirements for security protection. If it is lost, obtain a new one by the following methods:

-Obtain from the administrator

The administrator has access to the Wi-Fi key of each employee through EWeb or CLI. If the Wi-Fi key is lost, the employee can obtain a new one from the administrator. This method is applicable in the scenario where the Wi-Fi key has been lost from all bound STAs.

-Obtain in self-service mode

The employee can open the self-service page on a registered STA after connecting to the network and enters the account name and password. After identity authentication is passed, the employee will receive a new Wi-Fi key pushed by a Web page.

* **Manual binding**

The administrator can manually bind STAs (for example, printers) that cannot perform identity authentication. After successfully bound, these STAs do not need to perform identity authentication.

• MACC Version

When the MACC is deployed, the PPSK solution implements account management, key management, self-service management, and account verification on the MACC because no hardware AC exists. The experience process is the same as that described in section 6.1, with the only difference that hardware AC is replaced by MACC.

Typical Application

The PPSK solution is applicable to medium- and small-sized enterprises (with less than 500 employees) with Wi-Fi hacking prevention requirement.

Implementation Analysis

• Pros and Cons

The PPSK solution is designed to prevent Wi-Fi hacking.

* **Pros: ease of use and low cost.**

* **Cons: The PPSK solution is only applicable to medium- and small-sized enterprises (with less than 500 employees) because the solution is integrated in stand-alone mode with limited storage and computing capabilities. The PPSK solution may be cracked by means of key stealing and STA forgery.**

In terms of security, PPSK is inferior to 802.1x authentication but superior to portal authentication and WAP/WPA2-PSK. In terms of ease of use, PPSK surpasses 802.1x authentication and portal authentication and is similar to WPA/WPA2-PSK.

• Technical Dependency

The chips of APs must support the STA-based key computing system.

• Limitations

With limited storage and computing capabilities, the PPSK solution is only applicable to medium- and small-sized enterprises (with less than 500 employees). 802.1x authentication is recommended for larger enterprises.

Conclusion

PPSK is a security technique designed to prevent Wi-Fi hacking. In terms of security, PPSK is inferior to 802.1x authentication but superior to portal authentication and WAP/WPA2-PSK. In terms of ease of use, PPSK surpasses 802.1x and portal authentication and is similar to WPA/WPA2-PSK. PPSK is applicable to medium- and small-sized enterprises.

Ruijie Networks Co.,Ltd

For further information,please visit our website **http://www.ruijienetworks.com**