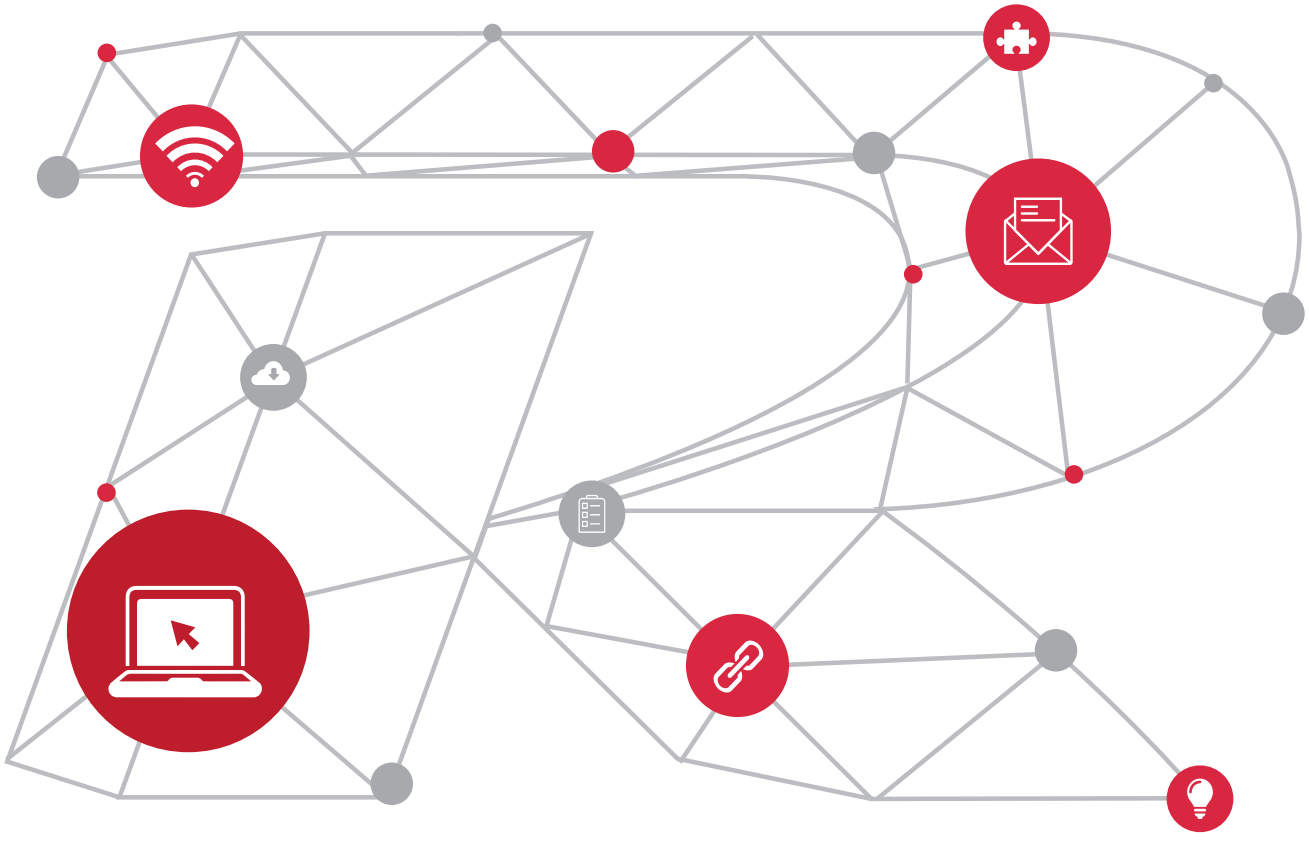
Ruijie Remote Intelligent Perceptive Technology

White Paper



Contents

Introduction

The Remote Intelligent Perceptive Technology (RIPT) prevents the unavailability of a Wireless Local Area Network (WLAN) when the tunnel between an Access Point (AP) and an Access Controller (AC) is interrupted accidentally, thereby improving the availability of WLAN.

• Background

As the core device of a WLAN, an AC is responsible for processing management packets of all subordinate APs and therefore easily causes a Single Point of Failure (SPOF) of the entire WLAN. Once the AC malfunctions or the CAPWAP tunnel is interrupted due to a fault occurring in the link between the AC and the APs, all APs managed by the AC will fail and the WLAN is unavailable to provide services. RIPT aims at maintaining the availability of WLAN when the CAPWAP tunnel between an AC and an AP is interrupted due to a fault, thereby improving the stability and reliability of the WLAN.

In distributed networks where ACs are deployed in the headquarters while APs are deployed in branches, ACs and APs are connected across the Wide Area Network (WAN), the links between the ACs and the APs may be instable, and the CAPWAP tunnels are frequently disconnected. In this case, RIPT is significant in improving network availability.

• Implementation

There is no available RIPT-related standard.

• Device Support

RIPT requires support from both ACs and APs. All Ruijie ACs support RIPT, and most of Ruijie APs support RIPT.

The software platform later than RGOS 11.X supports RIPT.

Technical Principles

The basic operating principles of RIPT are described as follows: In connection mode, an AC provides the user access service while an AP forwards data. If the AP is disconnected from the AC, the AP enters the independent mode, and provides the user access service and forwards data. After the connection is restored, the AP switches back to the connection mode.

If a WLAN is configured to work in centralized forwarding mode, a RIPT-AP working in dependent mode fails to forward data and users are forced offline.

The following first divides RITP implementation into several processes: AC connection establishment, disconnection, and connection restoration to describe the basic principles of RIPT, without considering 802.1x authentication and Web authentication, and then describes the statues and principles of RIPT support for 802.1x authentication and Web authentication.

• Connection Establishment Between a RIPT-AP and an AC

After a RIPT-AP establishes a connection with an AC and the configurations are delivered, the RIPT-AP enters the connection mode. In this mode, the AC backs up user information to the RIPT-AP in real time, to ensure that the RIPT-AP can continue to provide network services for users once the RIPT-AP is disconnected from the AC.

In connection mode, the work state of a WLAN is identical to that of fit APs. On WLANs in centralized forwarding mode, user access processing and user data forwarding are performed by ACs, and the WLANs work in the "centralized authentication/centralized forwarding" state. On WLANs in local forwarding mode, ACs process the user access service and APs forward user data, and the WLANs work in the "centralized authentication/local forwarding" state.

• Disconnection Between the RIPT-AP and the AC

When the AC is restarted or the network between the AC and the RIPT-AP is faulty, the RIPT-AP detects disconnection from the AC via the CAPWAP keepalive mechanism. After disconnecting from the AC, the RIPT-AP enters the independent mode. In this mode, on WLANs in centralized forwarding mode, user data fails to be forwarded, online users are forced offline, and new users are not allowed to go online.

On WLANs in local forwarding mode, the RIPT-AP takes over the user access service, keeps online users still online, and allows new users to go online.

Note that the RIPT-AP is in the connected state but the AC is actually unreachable in a case in which the link is disconnected but the disconnection has not been detected via the CAPWAP detection mechanism. New users cannot go online in this period of time.

• Restoration of Connection Between the RIPT-AP and the AC

In independent mode, the RIPT-AP keeps its IP address unchanged and continuously detects whether the AC is reachable. Once the AC becomes reachable, the RIPT-AP re-establishes a connection with the AC. After the connection is re-established, the RIPT-AP first detects whether the AC configurations change in the disconnection period, and then backs up user information on the RIPT-AP to the AC in batches. After the backup is complete, the RIPT-AP switches back to the connection mode. On WLANs in local forwarding mode, the AC begins to process the user access service.

When the RIPT-AP re-establishes a connection with the AC, the AC checks whether the configurations on the RIPT-AP are consistent with those on the AC to determine whether to keep online users still online. If the configurations on the AC change in the disconnection period, the AC clears the configurations on the RIPT-AP and forces online users associated with the RIPT-AP offline.

After the connection between the RIPT-AP and the AC is restored, the RIPT-AP backs up user entries to the AC in batches, to ensure that online users are not forced offline after the AC takes over the user access service. After the batch backup is complete, the RIPT-AP switches to the connection mode. On WLANs in local forwarding or centralized forwarding mode, the AC processes the user access service.

• Support from RIPT-APs for 802.1x Authentication

The RIPT-AP functions as a fit AP in connection mode.

In independent mode, the RIPT-AP keeps online users still online but disallows new users to go online.

After the connection between the RIPT-AP and the AC is restored and the RIPT-AP enters the connection mode, the AC conducts 802.1x re-authentication on online users to recover 802.1x user entries on the AC and user entries on the Remote Authentication Dial In User Service (RADIUS) server.

New users need to access the network even when the RIPT-AP works in independent mode. Therefore, another WLAN is applied after the RIPT-AP is disconnected. Users can access the network temporarily through this WLAN.

When the RIPT-AP works in connection mode, this WLAN is unavailable and cannot be discovered by searching. When the RIPT-AP works in independent mode, this WLAN starts providing the user access service. After the RIPT-AP restores to the connection mode, this WLAN becomes unavailable, online users are forced offline and access the WLAN that requires 802.1x authentication. This temporary WLAN often adopts the Wi-Fi Protected Access II Pre-Shared Key (WPA2-PSK) encryption mode, which prevents 802.1x authentication and ensures network security. This WLAN can also adopts the OPEN mode, which allows users to access the network without using password, and this WLAN can be mapped to a VLAN with low access permissions (for example, VLANs used by visitors), to ensure the security of the entire network.

• Support from RIPT-APs for Web Authentication

The RIPT-AP functions as a fit AP in connection mode.

When a RIPT-AP works in independent mode, it keeps online users still online. If the online users already pass Web authentication, they can still access the network normally. When new uses go online, the new users cannot access the network because Web authentication is unavailable.

After the connection between the RIPT-AP and the AC is restored and the RIPT-AP enters the connection mode, online users can access the network normally only after passing the Web authentication again.

In consideration that new users need to access the network when the RIPT-AP works in independent mode, Web authentication exemption in RIPT-AP independent mode is provided. When the RIPT-AP works in independent mode, new users can access the network after going online, with no need to pass Web authentication.

When the RITP-AP switches back to the connection mode, users that successfully go online need to pass Web authentication before accessing the network. For this, Ruijie provides the Web + MAC Address Bypass (MAB) authentication solution. When Web authentication exemption in independent mode is enabled, MAB authentication is also exempted. In this case, users can directly access the network after going online. When the RIPT-AP switches back to the connection mode, MAB authentication is performed first, and users do not need to pass Web authentication after passing the MAB authentication. Users who access the network for the first time need to pass Web authentication to access the network if they fail the MAB authentication.

Technical Features

• RIPT-AP Disconnection Imperceptible by Users in Local Forwarding Mode

When a RIPT-AP detects the disconnection from an AC, online users in local forwarding mode are still kept online whereas users in centralized forwarding mode are forced offline.

• RIPT-AP Connection Restoration Imperceptible by Users

Users cannot perceive the process in which the RIPT-AP connection is restored from disconnection and user information is backed up from the RIPT-AP to the AC. The users do not need to go offline and then go online to access the network. In this entire process, users can access the network normally without interruption.

• Web Authentication Exemption upon RIPT-AP Disconnection

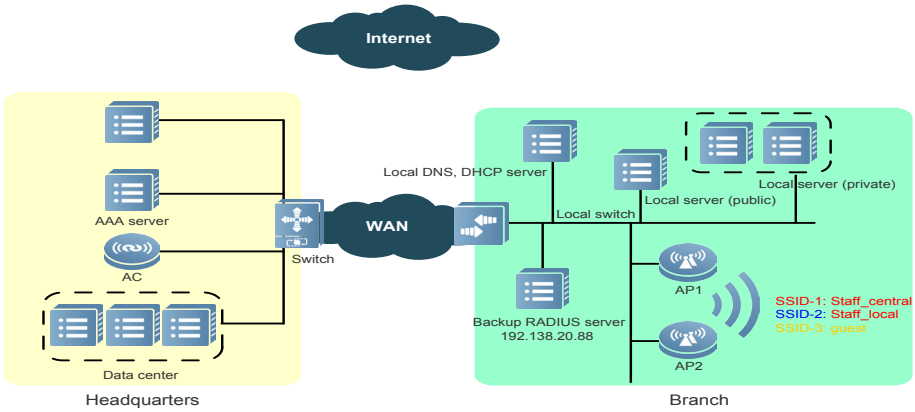
When the RIPT-AP is disconnected from the AC in a WLAN with the Web authentication function enabled, the link between the RIPT-AP and the authentication server is interrupted and authentication via Quick Response (QR) code is unavailable. New users cannot access the network after going online. In this case, Web authentication exemption can be configured to allow users to directly access the network after going online.

Typical Application

• RIPT

RIPT is typically applied in headquarters-branch network scenarios, as shown in the figure below.

Figure 1



As shown in the figure above, the function deployment is as follows:

* **The AC is deployed in the data center in the headquarters and APs are deployed in the branch.**

* **The DHCP server serving users in the branch are deployed in the branch.**

* **The RADIUS server is deployed in the headquarters, to provide access authentication for users of the enterprise headquarters and all branches.**

* **When an AP in the branch is disconnected from the AC in the headquarters due to causes such as a WAN fault, users in the branch cannot perform access authentication.**

* **The traffic for accessing the data center in the headquarters is transmitted through the WAN that connects the branch and the headquarters, and the traffic for accessing local resources in the branch and Internet resources is forwarded by devices in the branch, without passing through the WAN that connects the branch and the headquarters.**

In such an application scenario, RIPT is enabled on APs in the branch. When the WAN link between the branch and the headquarters is interrupted, the RIPT-AP can still provide wireless services.

Limitations

• Local Forwarding Required and RIPT Unavailable in Centralized Forwarding Mode

In centralized forwarding mode, data packets of users are forwarded to an AC for centralized processing. When a RIPT-AP is disconnected from the AC, the RIPT-AP cannot process data packets of users. As a result, users cannot access the network. Therefore, RIPT needs to be deployed together with the local forwarding mode.

If RIPT is enabled in centralized forwarding mode, after the RIPT-AP is disconnected from the AC, online users will be forced offline.

• Online Users Becoming Offline Upon RIPT-AP Re-connection to the AC If AC Configurations Change During RIPT-AP Disconnection

In implementation, the CLI configuration on the AC and the set operation performed via SNMP are monitored to determine whether the configurations on the AC change. Administrators can control the configurations on the AC via Telnet, eWeb, or the MIB tool during RIPT-AP disconnection, and it is considered that the configurations change regardless of whether the configuration change is relevant to APs. After the RIPT-AP reconnects to the AC, online users are forced offline and then brought online again.

• Authentication Unavailable for New Users Adopting 802.1x Authentication During RIPT-AP Disconnection

After the RIPT-AP is disconnected from the AC, the access service of new users is provided by the RIPT-AP. The RIPT-AP is not an authorized authentication device, and STAs cannot interact with the authentication server through the RIPT-AP to complete authentication.

To cope with this issue, another WLAN can be deployed and the OPEN or WPA/WPA2-PSK mode can be adopted to provide the user access service. The WLAN provides the access service only when the RIPT-AP is disconnected from the AC. It does not work when the RIPT-AP connects to the AC normally.

• Layer-3 Roaming Unsupported in RIPT-AP Independent Mode

In independent mode, the RIPT-AP supports Layer-2 roaming but not Layer-3 roaming. In Layer-2 roaming, VLANs associated with users do not change before and after user roaming; in Layer-3 roaming, VLANs associated with users change before and after user roaming. RIPT-APs do not support roaming in independent mode, which indicates that new IP addresses need to be obtained after user roaming.

In addition, if 802.1x authentication is enabled, online users cannot roam. The users will fail the 802.1x authentication after roaming, and will be forced offline.

• Failure in Configuring the IP Address Pool Serving APs and Users on the AC

After the RIPT-AP is disconnected from the AC, the AP and users still need to lease IP addresses. Therefore, the IP address pool cannot be configured on the AC. Generally, the address pool can be configured on the switch in the branch or on a device reachable even if the RIPT-AP works in independent mode.

Conclusion

This document describes the implementation principles of RIPT as well as the statuses of support for 802.1x authentication and Web authentication. RIPT supports the OPEN/WPA-PSK/WPA2-PSK mode and some mitigation processing is adopted to support the 802.1x authentication and Web authentication, in an effort to improve network availability to the maximum and take one step forward to the ultimate user experience.

Ruijie Networks Co.,Ltd

For further information,please visit our website **http://www.ruijienetworks.com**
Copyright © 2018 RuijieNetworks Co.,Ltd.All rights reserved.Ruijie reserver the right to change, modify,transfer,or otherwise revise this publication without notice,and the most current version of the publication shall be applicable.