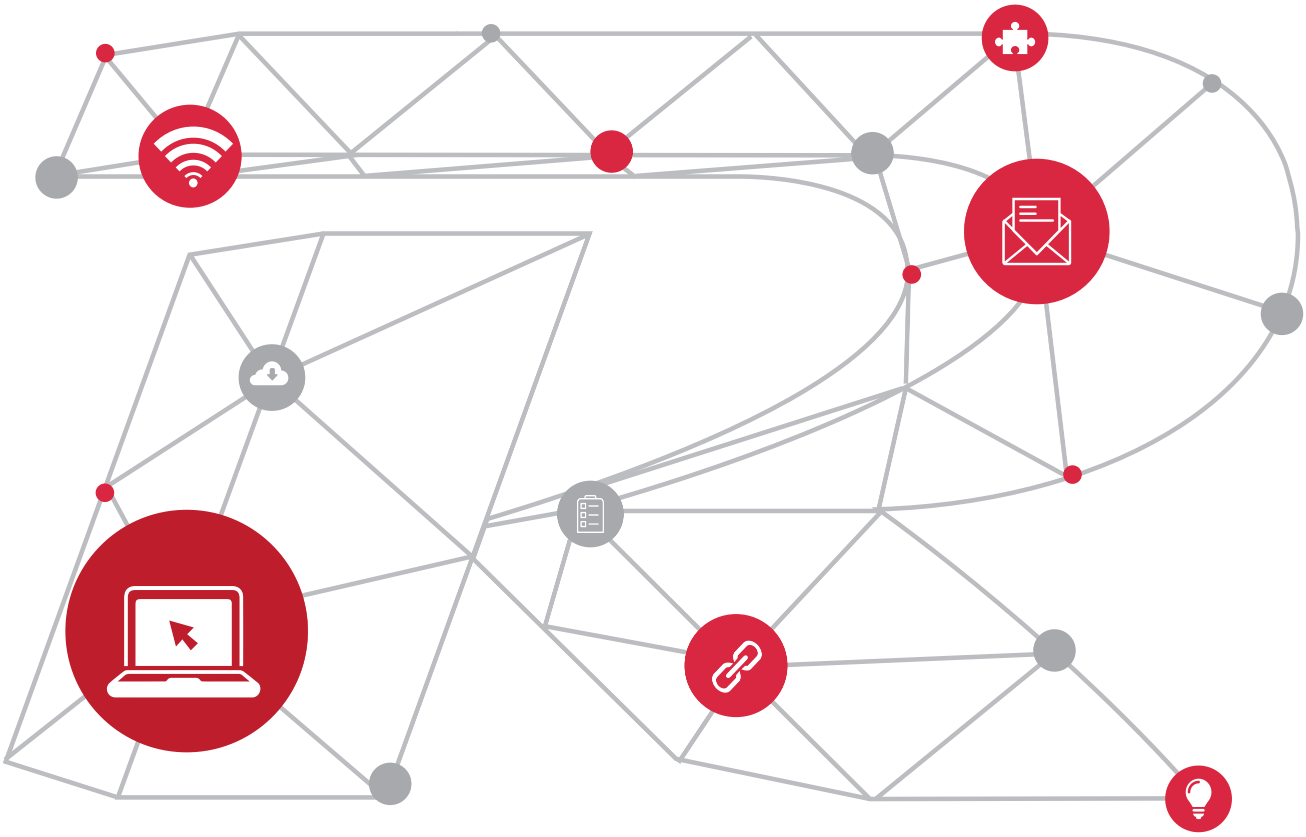
Ruijie Wireless Web Authentication

White Paper



Contents

Introduction

This document describes the basic technologies, principles, and typical application scenarios of wireless Web authentication.

Web authentication is an identity authentication method used to control users' network access. It does not require users to install any authentication software on their STAs but complete identity authentication only via browsers. When unauthenticated users access the Internet by using a browser, the access device uses the redirection technology to force the browser to access a specified website, which is often a portal server or portal. Users can enjoy services (for example, downloading security patches and viewing notices) on the portal server with no need to perform authentication. When in a need to access other network resources, users must pass identity authentication on the portal server via a browser. Only authenticated users can use network resources. Web authentication can provide convenient management functions for users, and users can launch advertisements and apply community services and personalized services on portals.

Technical Principles

• Wireless Web Authentication

Redirection Technology of Wireless Web Authentication

HTTP Interception

Hyper Text Transfer Protocol (HTTP) interception refers that wireless access devices (such as ACs) intercept the HTTP packets to be forwarded. These HTTP packets are sent by the browsers of the STAs connected to the wireless access devices, for accessing the network, but they are not destined for the wireless access devices.

After HTTP interception is enabled, a wireless access device directs HTTP connection requests of a STA to the wireless access device itself. Then, a Transmission Control Protocol (TCP) connection session is established between the wireless access device and the STA. The wireless access device uses the HTTP redirection function to push a redirection page to the STA. Then, a page pops up on the browser of the STA. The page may be an authentication page or a page that provides a link for downloading software or presents advertisements.

The Web authentication function allows specifying the STAs whose HTTP packets need or do not need to be intercepted as well as the destination ports of these HTTP packets. In general, HTTP requests from unauthenticated STAs are intercepted while those from authenticated users are not. HTTP interception is the basis of the Web authentication function. The interception of an HTTP packet sent by a browser automatically triggers the Web authentication process.

HTTP Redirection

According to HTTP, in normal cases, after the browser of an STA sends an HTTP Get or Head request, if the receiver has available resources, it returns the 200 response; if the receiver has no available resources, it returns the 302 response. In the 302 response, a new site path is provided. After receiving the response, the STA re-sends the HTTP Get or Head request to the new site to request resources. This process is called redirection.

HTTP redirection is an important part of Web authentication and occurs after HTTP interception. It utilizes the feature of the HTTP 302 response. A connection session is established between a wireless access device and an STA during HTTP interception. Afterwards, the STA sends the HTTP Get or Head request (originally destined for another site) to the wireless access device. After receiving the request, the wireless access network responds with the 302 response and adds the site path of the redirection page to the 302 response. In this way, the STA re-sends the request to the site path to access the redirection page.

Ruijie iPortal Web Authentication

Roles of Web Authentication

1. Authentication client: Usually refers to a browser running HTTP. When an STA needs to access the Internet via a browser, the browser sends HTTP requests.
2. NAS: Is an access-layer device in a network. It is directly connected to clients in wired or wireless networks and must be enabled with Ruijie iPortal Web Authentication. The NAS resolves the account information that clients enter on a Webpage and sends authentication requests to the RADIUS server. It determines whether clients can access the Internet according to authentication results and pushes the authentication results to the browsers.
3. RADIUS server: Provides the RADIUS-based authentication service to remote clients.

Web Authentication Process

1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication page is displayed on the browser.

2. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the iPortal server (NAS)

3. The NAS initiates authentication to the RADIUS server and displays the authentication result (success or failure) to the client on a page.

STA Go-offline Process

1. The NAS gets a client offline after the Logout button on the Web page is clicked.

2. The NAS gets a client offline with traffic lower than the threshold based on the parameters of user online traffic detection.

3. When the RADIUS server forces a client offline based on a certain policy, the NAS pushes a logout page to the client.

WiFiDog Web Authentication

Roles of Web Authentication

1. Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.

2. NAS: Is an access-layer device in a network (for example, an AP on a wireless network). The NAS is directly connected to clients and must be enabled with Web authentication. The NAS controls users' Internet access permissions, receives the token check requests or Internet access requests from authentication clients, and initiates identity check to the portal server.

3. Portal server: Provides a Web page for Web authentication and related operations. The portal server receives the HTTP-based authentication requests from authentication clients and extracts account information from the requests. When authentication is complete in the background, the authentication clients forward the authentication results to the NAS. The NAS redirects the authentication clients to a Webpage provided by the portal server.

4. Authentication server: Provides the authentication service. The authentication server negotiates with the portal server to determine the protocol (for example, RADIUS) used by authentication.

Web Authentication Process

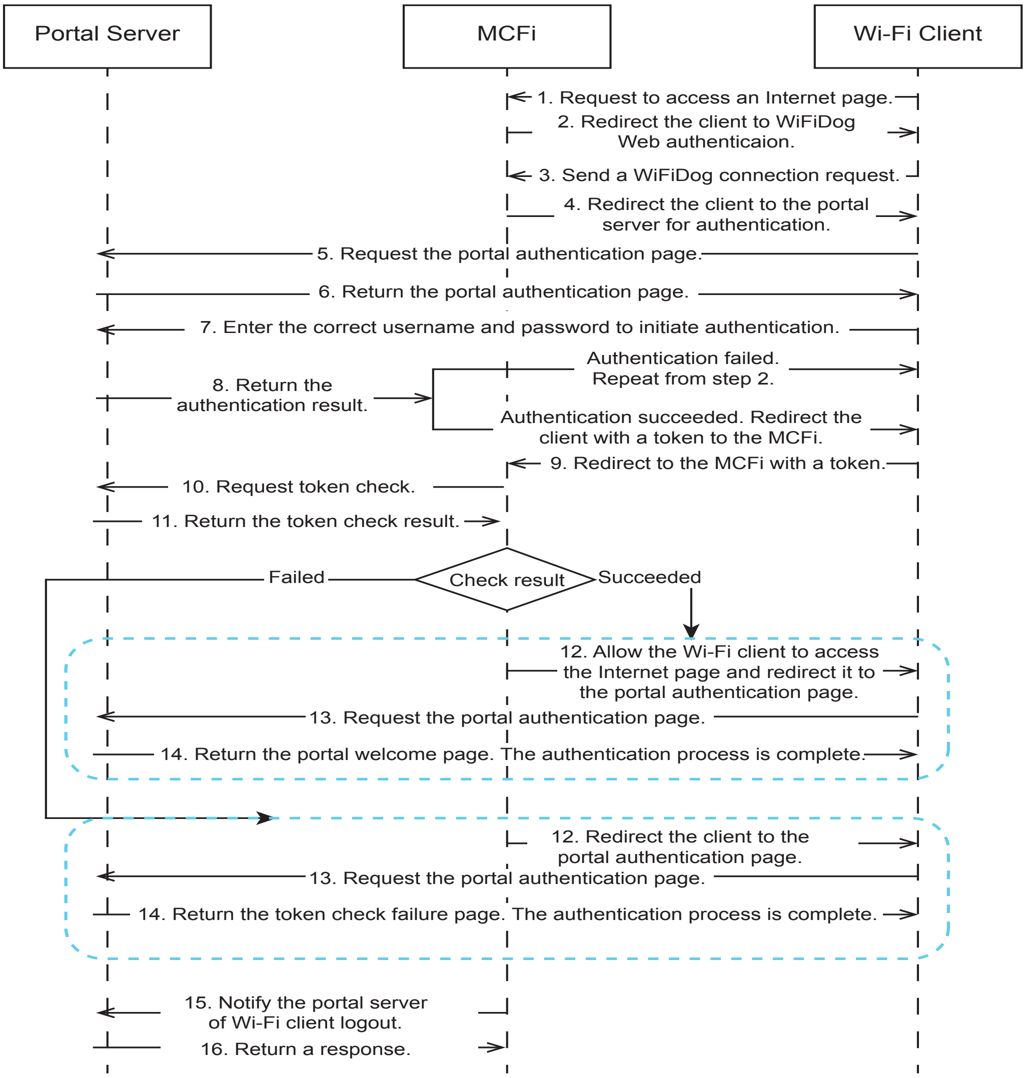
1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication page is displayed on the browser.

2. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the portal server.

3. The portal server checks the validity of the client information in the background. If authentication fails, the portal server displays the failed authentication result to the client on a Web page. If authentication is successful, the portal server redirects the client to the NAS.

4. After receiving a request from the client, the NAS initiates check to the portal server. The NAS redirects the client to a Webpage provided by the portal server based on the check result. Figure 2-1 shows the process in detail.

Figure 1 Flowchart of Ruijie iPortal Web Authentication


Portal Server
MCFi
Wi-Fi Client
1. Request to access an Internet page.
2. Redirect the client to WiFiDog Web authenticaion.
3. Send a WiFiDog connection request.
4. Redirect the client to the portal server for authentication.
5. Request the portal authentication page.
6. Return the portal authentication page.
7. Enter the correct username and password to initiate authentication.
8. Return the authentication result.
Authentication failed. Repeat from step 2.
Authentication succeeded. Redirect the client with a token to the MCFi.
9. Redirect to the MCFi with a token.
10. Request token check.
11. Return the token check result.
Failed
Check result
Succeeded
12. Allow the Wi-Fi client to access the Internet page and redirect it to the portal authentication page.
13. Request the portal authentication page.
14. Return the portal welcome page. The authentication process is complete.
12. Redirect the client to the portal authentication page.
13. Request the portal authentication page.
14. Return the token check failure page. The authentication process is complete.
15. Notify the portal server of Wi-Fi client logout.
16. Return a response.

STA Go-offline Process

There are two scenarios of client logout. One scenario is detected by the NAS that a client gets offline for the maximum online time is out, the upper traffic limit is reached, or the link is disconnected. The other scenario is detected by the portal server that a client logs out by clicking the Logout button on the logout page.

1. When a client clicks the Logout button, a logout request is sent to the portal server and NAS. (The logout request to the portal server and NAS may not be simultaneous, depending on the capability of the portal server.)
2. The NAS gets a client offline with traffic lower than the threshold based on the parameters of user online traffic detection.

2nd-Generation Wireless Web Authentication

Roles of Web Authentication

1. Authentication client: Usually refers to a browser running HTTP. When an STA needs to access the Internet via a browser, the browser sends HTTP requests.

2. Access device: Usually refers to an access layer device (for example, APs/ACs in WLANs). Generally, an access device is directly connected to STAs and the Web authentication function needs to be enabled on the access device. The access device receives STA authentication information from the portal server and initiates an authentication request to the RADIUS server. It determines whether to allow the STA to access the Internet based on the authentication result, and returns the authentication result to the portal server.

3. Portal server: Provides the authentication UI and relevant operations for Web authentication. The portal server receives an HTTP-based authentication request from an authentication client, extracts account information from the request, and sends the information to the network device. The portal server feeds back, to the STA via a page, the authentication result returned by the network device. The portal server shown in Figure 2-2 is a Ruijie ePortal server.

4. RADIUS server: Provides RADIUS-based remote user authentication. The RADIUS server shown in Figure 2-2 is a Ruijie SAM server.

Web Authentication Process

1. Before authentication, the access device intercepts all HTTP requests sent by unauthenticated STAs and redirects the requests to the portal server. In this way, an authentication page pops up on the browser of the STA.

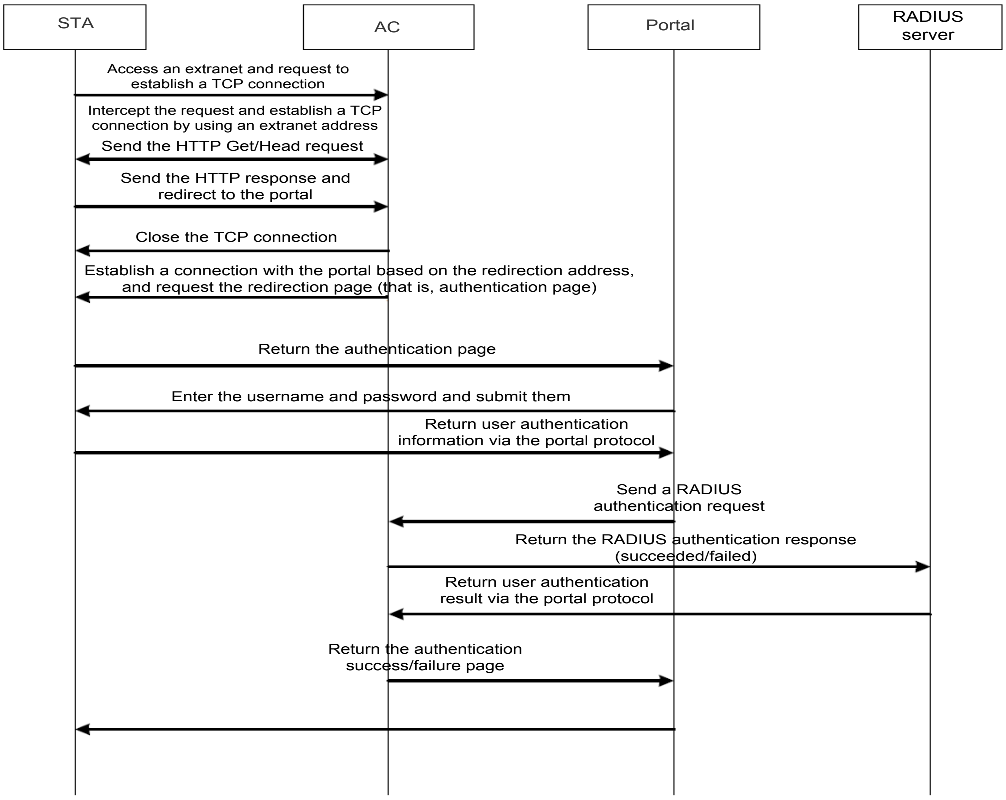
2. The user enters authentication information (username, password, and verification code) on the authentication page for the STA to interact with the portal server.

3. The portal server sends the authentication information to the device.

4. The device initiates an authentication request to the RADIUS server and returns the authentication result to the portal server.

5. The portal server presents the authentication result (succeeded or failed) to the STA on a page. Figure 2-2 shows the process in detail and an AC is used as an example.

Figure 2 Flowchart of 2nd-Generation Web Authentication


STA
AC
Portal
RADIUS server
Access an extranet and request to establish a TCP connection
Intercept the request and establish a TCP connection by using an extranet address
Send the HTTP Get/Head request
Send the HTTP response and redirect to the portal
Close the TCP connection
Establish a connection with the portal based on the redirection address, and request the redirection page (that is, authentication page)
Return the authentication page
Enter the username and password and submit them
Return user authentication information via the portal protocol
Send a RADIUS authentication request
Return the RADIUS authentication response (succeeded/failed)
Return user authentication result via the portal protocol
Return the authentication success/failure page

STA Go-offline Process

A STA goes offline in two cases: In one case, the access device detects that the STA goes offline, for example, the allowed access time of the STA is up, the STA runs out of traffic, or the link is interrupted. In the other case, the portal server finds that the STA goes offline, for example, the STA triggers a go-offline request on the go-offline page or the keepalive page becomes invalid.

In Case 1, when the AC detects that a STA goes offline, it notifies the portal server of the STA go-offline via the portal protocol, and deletes STA information. The portal server presents the go-offline page to the STA.

In Case 2, after the portal server detects that a STA goes offline, it notifies the AC of the STA go-offline via the portal protocol.

The portal server presents the go-offline page to the STA.

In both cases, the AC initiates a charging end request to the RADIUS server to notify the RADIUS server that the STA has gone offline.

Technical Features

• Redirection for Ruijie Wireless Web Authentication

Diversified Redirection Modes

In addition to standard HTTP 302 redirection, Ruijie wireless Web authentication supports HTTP 200 redirection.

The advantages of the HTTP 200 redirection are as follows: As only browsers can process script language, the browsers can filter out packets from non-browsers (for example, HTTP packets automatically sent by applications on mobile phones), to avoid redirection to the portal server, thereby greatly reducing the performance stress of the portal.

Configurable Format of Redirection URLs

Ruijie wireless Web authentication can be configured to support different customized redirection URL formats (with different parameters) and even different encryption algorithms, to meet service expansion requirements of various portals (such as the portal servers).

Support for STA Type Identification

Ruijie wireless Web authentication identifies the STA type by obtaining the User-Agent attribute in HTTP packets, and sends the STA type to the RADIUS server through authentication packets, implementing the STA real-name policy.

Support for DHCP Address Check

Ruijie wireless Web authentication allows users to configure static IP addresses or obtain IP addresses via DHCP. If the DHCP address check function is enabled, requests sent from STAs using static IP addresses cannot be redirected and the packets are directly discarded.

• Ruijie iPortal Web Authentication

Support for Specific Pages

Ruijie iPortal Web authentication supports popups of specific pages before and after authentication.

Support for A Customized Page Suite

Ruijie iPortal Web Authentication allows users to configure a page suite on the iPortal server and add special content or information to the page suite, such as, a logo or notice.

• Ruijie 2nd-Generation Wireless Web Authentication

CHAP Authentication

Ruijie 2nd-generation wireless Web authentication supports the Challenge Handshake Authentication Protocol (CHAP), to meet application requirements of public networks.

Support for CMCC MIB Specification

Rujie 2nd-generation wireless Web authentication complies with the "Test Specification for Network Management Interface of CMCC WLAN Equipments V1.0.4."

Support for CMCC IPv6 Restructuring

Ruijie 2nd-generation wireless Web authentication supports IPv6 address-based authentication and the coexistence of IPv4 and IPv6 addresses. However, a STA can use only one type of address for authentication.

Support for CMCC MAC SMS Specification

Ruijie 2nd-generation wireless Web authentication complies with the "CMCC WLAN Equipment Interface Specification V3.1.0_20130901 (MAC Authentication Extension)."

Portal Server Status Detection

Ruijie 2nd-generation wireless Web authentication supports the portal server status detection (reachable or unreachable), and implements relevant services based on the status of the portal server. For example, a customer may request that the Internet access service is free from impact when the portal server is unreachable. That is, when detecting that the portal server is unreachable, the Web authentication skips the authentication process and allows user packets to pass directly. When detecting that the portal server becomes reachable, the Web authentication forces the users who are exempted from authentication during the portal server unavailability to go offline and allows them to go online only after they pass authentication.

Active and Standby Portal Servers

Ruijie 2nd-generation wireless Web authentication supports the configuration of active and standby portal servers (one active portal server and up to four standby servers can be configured). In combination with the portal server status detection in Section 3.3.5, a reachable portal server can be selected for authentication.

• Coexistence of Multiple Authentication Modes

The 2nd-generation Web authentication, and embedded portal Web authentication can be deployed for different WLANs, and the multiple authentication modes can coexist.

Typical Application

• Wireless Web Authentication

Scenario

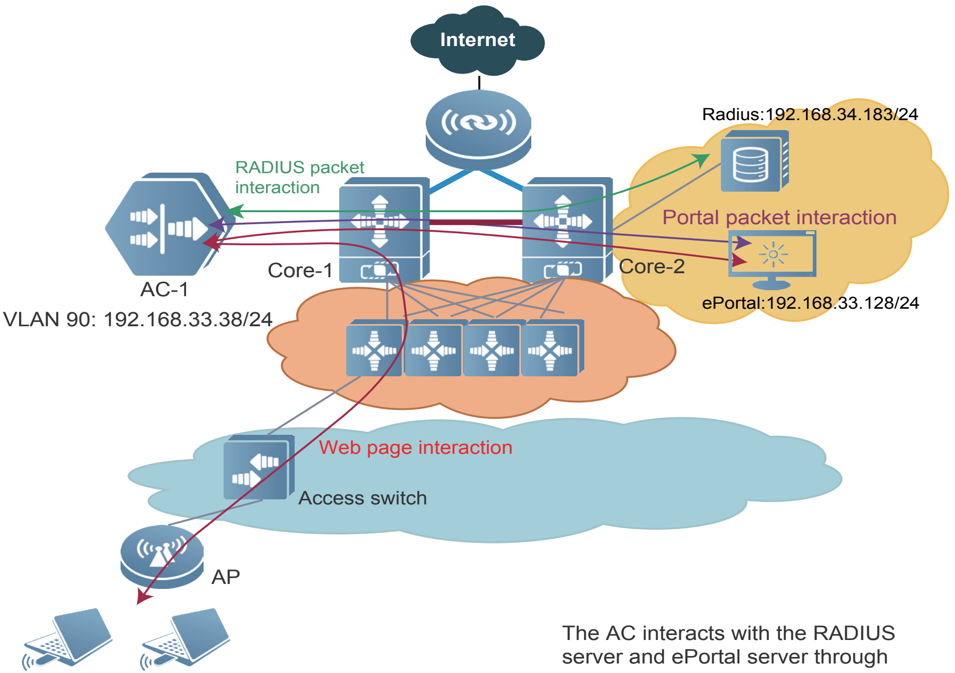
Wireless Web authentication is applicable to clients (especially mobile phones and tablet computers) on which the authentication client are undesired or cannot be installed but access control needs to be performed on network users.

Advantage: The authentication client does not need to be installed on wireless STAs and Web browsers can be used.

Disadvantage: The portal server (for pushing the Web authentication page) and RADIUS server (for storing clients' usernames and passwords) are required.

Network Topology

Figure 3 Ruijie Wireless Web Authentication


Internet
Radius:192.168.34.183/24
RADIUS packet interaction
Portal packet interaction
AC-1
Core-1
Core-2
VLAN 90: 192.168.33.38/24
ePortal:192.168.33.128/24
Web page interaction
Access switch
AP

The AC interacts with the RADIUS server and ePortal server through VLAN 90 (192.168.33.38)

Configuration Steps of Ruijie iPortal Web Authentication

```
Ruijie#configure

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)#aaa new-model      //Enable AAA authentication.

Ruijie(config)#radius-server host 192.168.34.183 key ruijie

Ruijie(config)#aaa authentication iportal default group radius

Ruijie(config)#aaa accounting network default start-stop group radius

Ruijie(config)#web-auth template iportal     //Configure iPortal authentication template.

Ruijie(config.tmplt.iportal)#exit

Ruijie(config)# wlansec 1

Ruijie(config-wlansec)# web-auth portal iportal   //Enable iPortal authentication.

Ruijie(config-wlansec)# webauth

Ruijie(config-wlansec)# exit
```

Configuration Steps of WiFiDog Authentication

```
Ruijie# config

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)#web-auth template wifidog    //Configure WiFiDog template.

Ruijie(config.tmplt.wifidog)#ip 192.168.197.79

Ruijie(config.tmplt.wifidog)#url http://192.168.197.79/auth/wifidogAuth

Ruijie(config.tmplt.wifidog)#nas-ip 1.1.1.1

Ruijie(config.tmplt.wifidog)#exit

Ruijie(config)# wlansec 1

Ruijie(config-wlansec)# web-auth portal wifidog   //Enable WiFiDog authentication.

Ruijie(config-wlansec)# webauth

Ruijie(config-wlansec)# exit
```

Configuration Steps of Ruijie 2-Generation Wireless Web Authentication

```
Ruijie#configure

Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#aaa new-model //Enable AAA
authentication.

Ruijie(config)#radius-server host 192.168.34.183 key ruijie

Ruijie(config)#ip radius source-interface vlan 90 //The AC interacts with the RADIUS server by using the IP address
of VLAN 90.

Ruijie(config)#aaa authentication web-auth default group radius

Ruijie(config)#aaa accounting network default start-stop group radius

Ruijie(config)#web-auth portal key ruijie

Ruijie(config)#web-auth template eportalv2 Ruijie(config.tmplt.eportalv2)#ip 192.168.33.128

Ruijie(config.tmplt.eportalv2)#url                                                    http://

192.168.33.128:8080/eportal/index.jsp

 Ruijie(config.tmplt.eportalv2)#exit
Ruijie(config)#wlansec 1 //Enable Web authentication on WLAN 1.

Ruijie(config-wlansec)# web-auth portal eportalv2 //Enable 2nd-generation Web authentication.

Ruijie(config-wlansec)# webauth //Enable Web authentication.
```

Limitations

• Limitations on Wireless Web Authentication

1. Wireless Web authentication supports the HTTP 200 script redirection mode. The HTTP 302 redirection mode is supported only in 11.1PJ8 and later projects.
2. Ruijie 2nd-generation wireless Web authentication supports IPv6 addresses only in 11.1PJ8 and later projects.

Conclusion

As the "service-driven era" of WLAN arrives, portals focus on the customization of various customer service requirements. For control on the network ingress, wireless Web authentication must be integrated with these customized portals seamlessly. The powerful Ruijie wireless Web authentication can meet the requirements of these portals, to implement SM/verification code authentication, advertisement push authentication, QR code scanning authentication, and other variant Web authentication modes.

Ruijie Networks Co.,Ltd

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