IGNITION
DESIGN LABS

MAC Authentication-based Transparent Authentication

Technical White Paper V1.1

Disclaimer

Limitation of Liability

Website:

https://ignitiondl.com/

Table of Contents

Chapter 1 Background

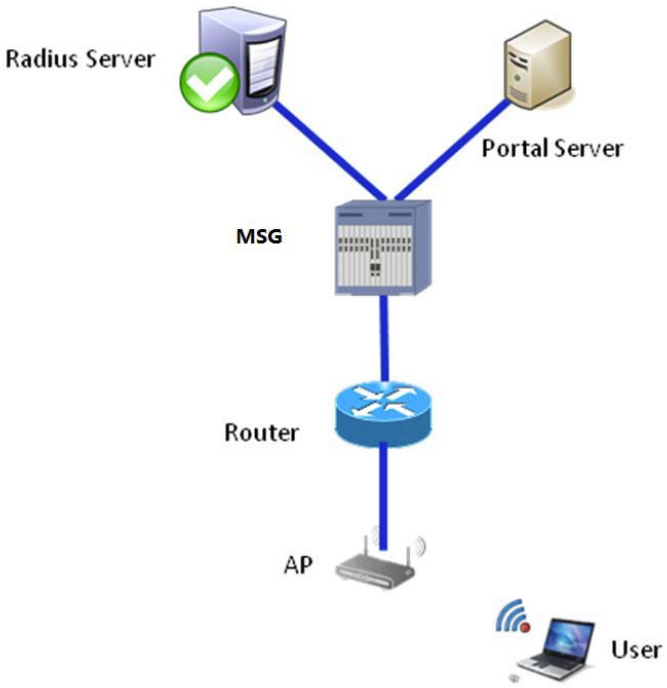
Nowadays user experience has gradually become the hot spot of wireless communication market competition. User experience quality becomes an important standard of wireless access. However, at present, the development of the WLAN network is still in its infancy. The Web-based authentication is not convenient for users and the tedious certification process of the traditional Portal authentication mode does not only reduce the network efficiency, but also affects user experience, restricting the development of WLAN users. If the user online time and quantity cannot rapidly increase, the network construction investment cost recovery period extends and the user ARPU value reduces.

Chapter 2 Scenario

MAC-based transparent authentication integrates the features and advantages of Portal/Web authentication and the MAC authentication. When a user connects to the network for the first time, the user needs to pass the Portal/Web authentication. After the Portal/Web authentication, the RADIUS server saves the MAC information of the user. The user does not need to perform Portal/Web authentication when accessing the network again after a period of time, directly authenticating through the user MAC address. The user can configure this time interval on the RADIUS server.

The MSG series multiple service gateway (MSG) provides the following authentication method.

Figure 2-1 Transparent authentication



Chapter 3 Advantages and Implementation

3.1 Advantages

MAC authentication-based transparent authentication has the following advantages:

- Easy operation: After a user connects to the network for the first time, the backstage automatically deals with the authentication, ensuring user experience.
- Automatic authentication, authorization and accounting with the RADIUS Server.
- Avoiding frequent authentication due to frequent disconnection under poor wireless environment.
- Transparent authentication process.

3.2 Implementation

In a large or medium scale wireless network, users may have their own unique data center, working as a wireless network identity authentication and a centralized controller. The MSG series can provide fast and convenient features based on user authentication, such as transparent authentication.

The MSG series supports the following authentication protocols:

- RFC 2865 RADIUS Authentication
- RFC 3576 Dynamic Authorization Extensions to RADIUS

First-time Login

The first-time authentication process is as follows:

Step 1 A WLAN terminal associates with an AP to complete the open + web authentication and other forms of authentication.

Step 2 The MSG sends an access-request to the RADIUS Server to complete MAC authentication.

Step 3 The RADIUS user authentication server determines whether the user is legal according to the user information and responds the authentication failure packets to the MSG.

Step 4 If the user is legal, the user gets the planned IP address from the MSG through the standard DHCP protocol.

Step 5 The user opens the Web browser, accesses to any site, and launches a HTTP request.

Step 6 The MSG intercepts the user's HTTP request. Because the user has not passed the authentication, the MSG is forced to jump to the Web page to the Portal Server.

Step 7 The Portal Server pushes the customized Web authentication to the WLAN terminal user.

Step 8 The user enters the username, password, and other information in the browser and submits it to the Portal Server.

Step 9 The Portal Server receives the username and password information, encapsulates in compliance with the RFC 3576 format, submits it to the MSG, and starts the authentication.

Step 10 The MSG sends the access-request to the RADIUS Server (including username, password, user ID, and user MAC) to authenticate by the RADIUS user authentication server.

Step 11 The RADIUS user authentication server determines whether the user is legal according to the user information and responds the authentication success/failure packets to the MSG. If the authentication success packets are sent, authenticate the user with the negotiate parameters and the related service properties.

Step 12 The MSG feedbacks the authentication result to the Portal Server.

Step 13 If the authentication is successful, the Portal Server pushes the Portal page to the user and records the user's MAC address. If the authentication fails, the Portal Server gets back to the page where the user fails the authentication.

Step 14 The Portal Server responds the authentication result packets from the MSG. If the authentication fails, the process ends.

Step 15 Meantime, the MSG sends Accounting-Request/start packets to the RADIUS Server.

Step 16 The RADIUS Server responds the Accounting-Request/start packets to the MSG.

The user completes online authentication.

Re-login

If the user goes online again after a period of time, the authentication process is as follows:

Step 1 The WLAN terminal associates with the AP to complete the open + web authentication and other forms of authentication.

Step 2 The MSG sends an access-request to the RADIUS Server to complete MAC authentication.

Step 3 The RADIUS user authentication server determines whether the user is legal according to the user information and responds the authentication success packets to the MSG. If the authentication success packets are sent, authenticate the user with the negotiate parameters and the related service properties

Step 4 The user gets the planned IP address from the MSG through the standard DHCP protocol.

Step 5 Meantime, the MSG sends Accounting-Request/start packets to the RADIUS Server. The RADIUS Server responds the Accounting-Request/start packets to the MSG.

The user completes the online authentication.

Chapter 4 Conclusion

The MSG series provide a convenient MAC authentication-based transparent authentication:

- Simple and convenient: do not need to configure the client.
- Authentication and accounting without user perception.
- Automatic authentication, authorization and accounting with the RADIUS Server.
- User access and privilege control.

A Terminology

Terminology	Explanation
AAA	• Authentication: Verify the identity of the user and the available network service. • Authorization: Open network services to the user according to the authentication. • Accounting: Record the network service usage of users and provide it to the accounting system.
RADIUS	Remote Authentication Dial in User Service is an AAA based protocol.
Portal	The Portal server completes to push the specified authentication page to the user.
MAC authentication	A MAC address-based authentication, which controls the network access privilege of users.