Technical Guide

WISPr Message Types and Response Codes

Release: August 2015
Doc Rev No: R2
# Table of Contents

1. **Introduction** ................................................................................................................ 2
2. **WISPr Authentication Flow** .......................................................................................... 2
3. **WISPr Message Type and Response Code** ..................................................................... 3
   3.1 Redirect ........................................................................................................................... 4
   3.2 Login .................................................................................................................................. 4
   3.3 Logout .................................................................................................................................. 5
4. **WISPr Configuration Pages** ........................................................................................... 5
5. **Summary** ..................................................................................................................... 7
6. **Remarks** ...................................................................................................................... 7
1. Introduction

Wireless Internet Service Provider roaming (WISPr) authentication allows clients to roam between networks provided by different wireless ISPs. The controller supports basic messages for WISPr authentication. This document introduces the authentication flow of WISPr and the supported message types on the controllers.

2. WISPr Authentication Flow

The controllers support WISPr authentication method according to Wi-Fi Alliance WISPr protocol 1.0. Although WISPr authentication is based on web pages on the controllers, it is different from normal browser-based authentication (UAM). WISPr clients need not open a browser and enter username and password on login pages. With the help of WISPr utilities (such as iPass connector, Boingo, iOS Captive Network Support), authentication processes will be automatically executed when the username and password are properly stored in the utilities.

Take iPass connector (Windows 7 64bit) as an example, the following figure shows the WISPr authentication flow in the controllers.
a. When a client runs iPass on a device, it will automatically connect to http://sniff-1.ipass.com to test whether the device can connect to the Internet. If the device can reach the website, it will show “Link established” in the utility. Otherwise, the controller redirects to the login page (as step 2 in the figure).

b. When an iPass client requests the controller for “dns.shtml”, the controller will send a webpage with the WISPr XML embedded. This XML describes the location where iPass should POST the username and password for authentication (as step 3 and step 4 in the figure).

c. After the client sends the username and password, the controller will authenticate this user to the RADIUS server. The authentication result and logout address will be sent to the iPass client in XML format.

d. The iPass client can logout by connecting to the logout address. The controller then logs the client out and inform the client of the result.

3. WISPr Message Type and Response Code

The controllers support basic message types and response codes. Currently, only Wi-Fi Alliance WISPr 1.0 standard is supported. In the implementation of WISPr authentication, we can separate them into three
different actions: redirect, login, and logout.

3.1 Redirect

When redirecting HTTP requests to the login page, the controller will inform the WISPr utility the location by XML format. An example is shown below.

```
<Redirect>
    <AccessProcedure>1.0</AccessProcedure>
    <AccessLocation>$AccessLocation</AccessLocation>
    <LocationName>$LocationName</LocationName>
    <LoginURL>$LoginURL</LoginURL>
    <MessageType>100</MessageType>
    <ResponseCode>0</ResponseCode>
</Redirect>
```

Message Type and Response Code can be found in the example. The supported values of Message Type and Response Code for redirection message are shown in the following table.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>100</th>
<th>110</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Code</td>
<td>0</td>
<td>200</td>
</tr>
<tr>
<td>Meaning</td>
<td>The client sends the username and password with “POST” method to the built-in web page of the controller directly.</td>
<td>The client sends the username and password to the external web page.</td>
</tr>
</tbody>
</table>

3.2 Login

An example of XML format used during login is shown as follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam>
    <AuthenticationReply>
        <MessageType>120</MessageType>
        <ResponseCode>$ret</ResponseCode>
        <ReplyMessage>"$.result["REPLY-MESSAGE"]"</ReplyMessage>
        <LogoffURL>$LogoutURL</LogoffURL>
    </AuthenticationReply>
</WISPAccessGatewayParam>
```
The supported values of Message Type and Response Code for login message are shown in the following table.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>120</th>
<th>120</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Code</td>
<td>50</td>
<td>100</td>
</tr>
<tr>
<td>Meaning</td>
<td>Login success</td>
<td>Login fail (due to error username/password or *lack of response from the external RADIUS server)</td>
</tr>
</tbody>
</table>

*Lack of response from the external RADIUS server: the log of this situation can be found in system log.

3.3 Logout

An example of XML format used during logout is shown as follows.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam>
  <LogoffReply>
    <MessageType>130</MessageType>
    <ResponseCode>$ret</ResponseCode>
  </LogoffReply>
</WISPAccessGatewayParam>
```

The supported values of Message Type and Response Code for logout message are shown in the following table.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>130</th>
<th>130</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Code</td>
<td>150</td>
<td>255</td>
</tr>
<tr>
<td>Meaning</td>
<td>Logout success</td>
<td>Logout fail (cause can be lack of response from the external RADIUS server or *unknown)</td>
</tr>
</tbody>
</table>

* Undefined causes of failed logout are classified into Response Code 255.

4. WISPr Configuration Pages

For each Service Zone, we can configure the WISPr setting as the following.
The configurable items are shown as the following.

Location ID and Location Name can also be configured by VLAN (in Port Location Mapping profile).
5. Summary

In this document, the authentication flow of WISPr and the supported message types on the controllers have been introduced, with iPass connector as an example.

6. Remarks

Please contact _____________ for additional information.