

Amigopod

Implementing Accounting-Based Authorization



Copyright

© 2011 Aruba Networks, Inc. Aruba Networks trademarks include Airwave, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.



www.arubanetworks.com
1344 Crossman Avenue
Sunnyvale, California 94089
Phone: 408.227.4500
Fax 408.227.4550

Table of Contents

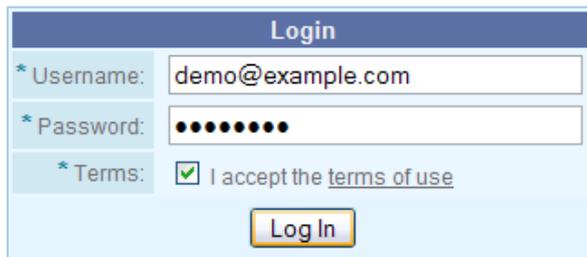
1	Introduction	4
	Audience	4
	Document Overview	4
	Disclaimer	5
2	About Accounting-Based Authorization	6
	Authentication, Authorization and Accounting	6
	Accounting-Based Authorization	7
	Authorization during Access-Request	7
	Authorization during Accounting-Request	8
	NAS Requirements	10
3	Configuring Accounting-Based Authorization	11
	Check Plugin Versions	11
	Create RADIUS User Role	11
	Create RADIUS NAS Client	12
	Create Terms of Use page	12
	Set Terms of Use URL	13
	Create Landing page	13
	Create Login page	16
	Additional Configuration Guidelines	18
4	Verifying Accounting-Based Authorization	19
	Check NAS captive portal settings	19
	Check terms of use page	19
	Check login page	19
	Check landing page	20
	Check traffic limit	20
5	Modifying Accounting-Based Authorization	21
	Adjusting the traffic limit	21
	Count only uploaded or downloaded traffic	21
	Accounting terminology	21
	Counting only downloaded traffic	21

1 Introduction

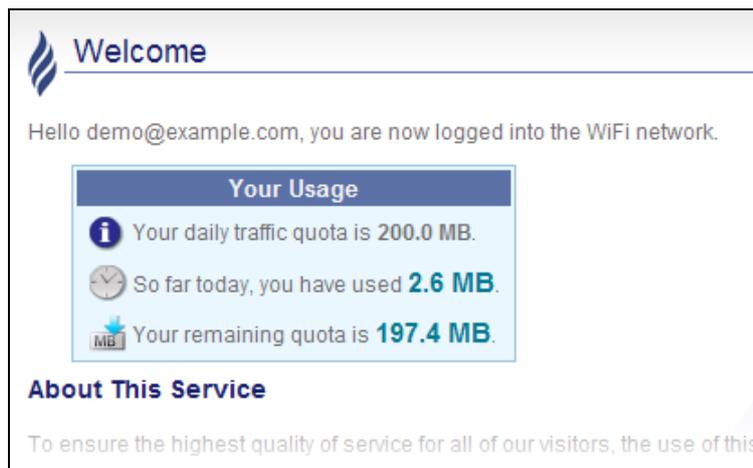
This technical note explains how to use accounting-based authorization to build a complete portal for a network service that offers free usage to guests, where guests are restricted to a certain daily quota of traffic.

The completed portal includes:

- A **login page** where guests can log in with their username and password.



- A **terms of use page** describing the conditions under which the guest service is provided.
- A **landing page** showing the guest's current traffic counters and remaining quota.



- A **user role** configured with the appropriate authorization rules based on accounting traffic.

Audience

This document is intended for network administrators and system integrators deploying an Amigopod-based visitor management solution.

Basic familiarity with the Amigopod Visitor Management Appliance is assumed. For in-depth information about the features and functions of the Amigopod appliance, refer to the Amigopod Deployment Guide.

Document Overview

The first section of the document explains the concept of accounting-based authorization, and how this solution works with the Amigopod Visitor Management Appliance.

The next section contains a detailed configuration guide for creating the portal. Step-by-step instructions are provided for creating each page, and for performing all necessary configuration tasks.

Disclaimer

The topics of network design, security architectures and visitor access are complex subjects, and no single document can hope to cover all of the possible combinations of network equipment, network design, deployment requirements, and device configurations, nor can all the possible security implications for a particular recommendation be covered.

Therefore, while you read this document, it is best to consider it as a guide to developing your own understanding of the network design topics covered, and as a basis for further investigation.

2 About Accounting-Based Authorization

This section provides background information explaining the concepts of authorization and accounting, and how these can interact to provide a restricted network service to guests.

Authentication, Authorization and Accounting

The Amigopod Visitor Management Appliance is built on the industry standard AAA framework, which consists of authentication, authorization and accounting components.

Diagram 1 shows how the different components of this framework are employed in a guest access scenario.

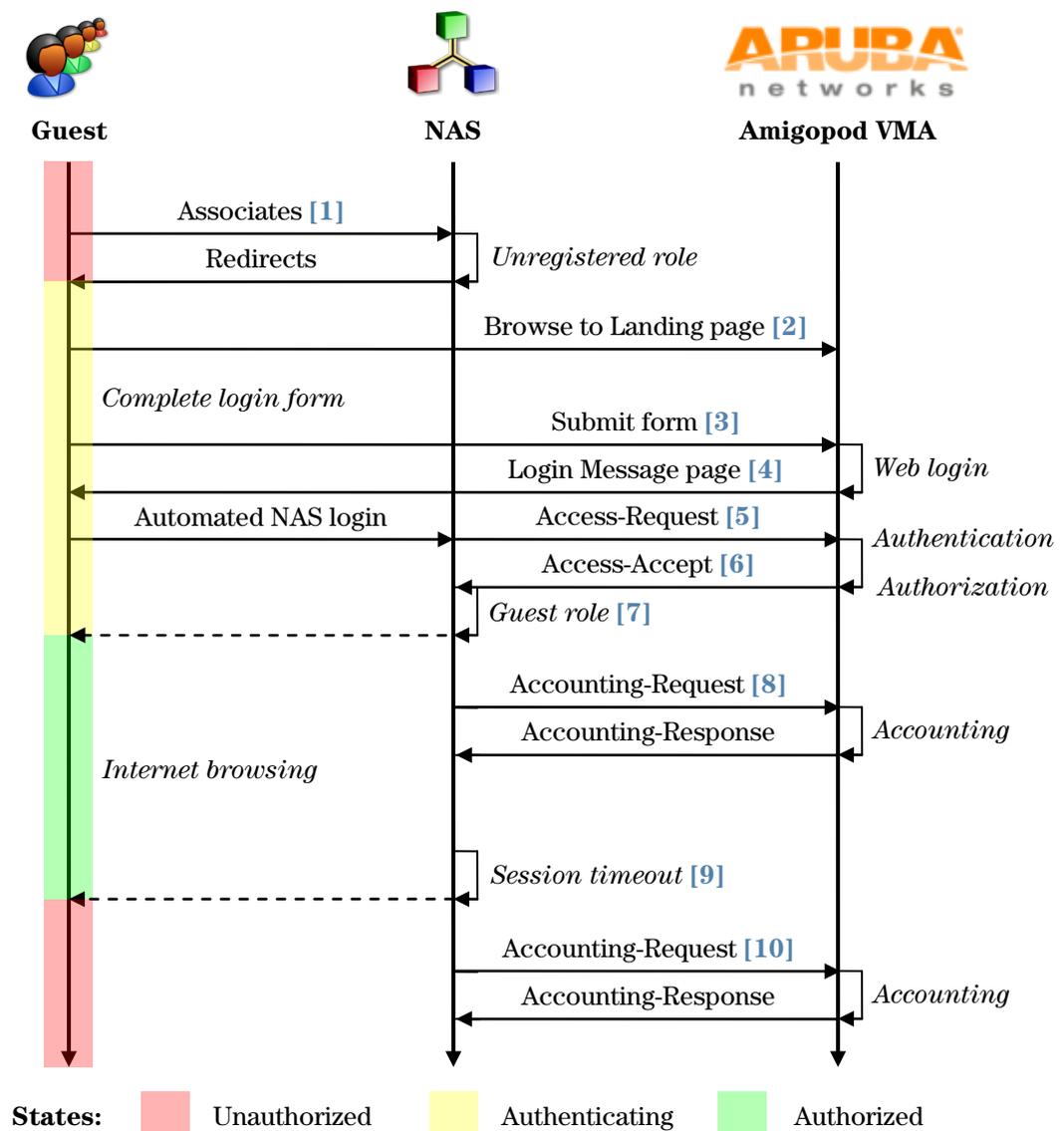


Diagram 1: Sequence diagram for network access using AAA

In the standard AAA framework, network access is provided to a user according to the following process:

- The user connects to the network by associating with a local access point [1].
- A landing page is displayed to the user [2] which allows them to log into the NAS [3], [4] using the login name and password of their guest account.
- The NAS authenticates the user with the RADIUS protocol [5].
- The Amigopod Visitor Management Appliance determines whether the user is authorized, and if so returns vendor-specific attributes [6] that are used to configure the NAS based on the user's role [7].
- If the user's access is granted, the NAS permits the guest to access the network, based on the settings provided by the Amigopod Visitor Management Appliance.
- The NAS reports details about the user's session to the Amigopod Visitor Management Appliance using RADIUS accounting messages [8].
- After the user's session times out [9], the NAS will return the user to an unauthorized state and finalize the details of the user's session with an accounting update [10].

Accounting-Based Authorization

Authorization decisions can be made based on the accounting records available to the RADIUS server.

By using this process, traffic limits can be applied for guests within a particular time period.

The example portal developed in this technical note applies a 200 MB combined limit for guest traffic (upload and download), measured in any 24 hour period starting from midnight. Many other rules are possible using the flexible approach to authorization conditions.

There are two scenarios in which authorization is required:

Authorization during Access-Request

As shown in Diagram 1, when a guest connects to the network and logs in a RADIUS Access-Request is performed.

More detail on the initial authorization is shown in Diagram 2.

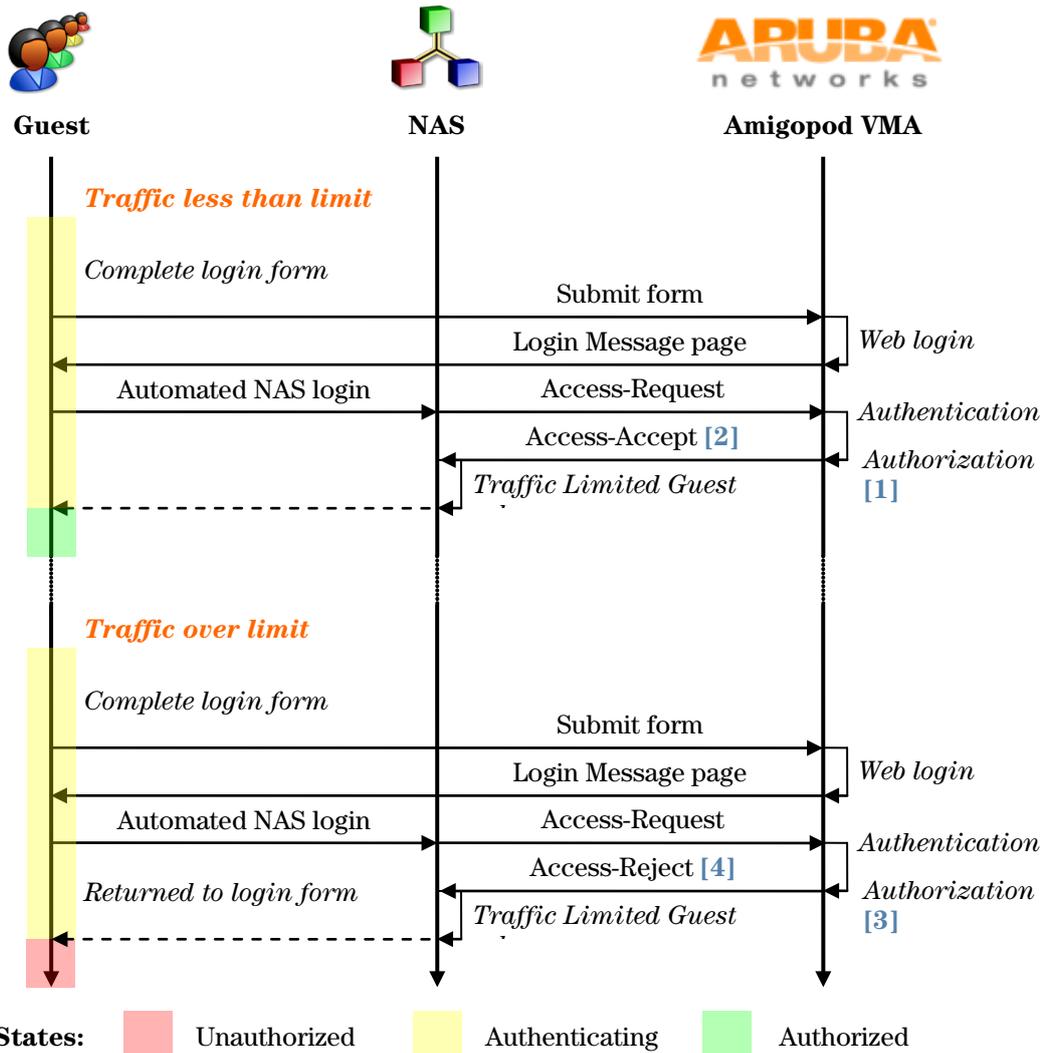


Diagram 2: Sequence diagram for traffic limited authorization

If the guest has not previously logged in today, or if the guest’s total traffic consumption for today is less than the configured limit, then the guest is authorized [1] and an Access-Accept response is sent [2].

To limit the guest’s traffic, if the guest’s total traffic from previous sessions today exceeds the configured limit (200 MB) then this is determined during the authorization process [3] and an Access-Reject response will be sent [4].

Because the Amigopod Visitor Management Appliance uses role-based access control for visitor accounts, the authorization rules above should be defined as part of the role that the visitor accounts are using; in this example, the role is the “Traffic Limited Guest role”.

Authorization during Accounting-Request

Because of the authorization rules applied at login time, if the guest is able to successfully log in then it is known at that time that the guest’s current traffic usage is below the allowed quota.

Once a guest is authorized, then, how are they prevented from consuming more than their allowed traffic quota?

There are two ways to achieve this, depending on the type of NAS equipment in use:

- Vendor-specific attributes — Certain NAS vendors provide the capability to limit the amount of traffic in a particular session. For example:
 - The **ChilliSpot-Max-Total-Octets** attribute may be used with a coova-chilli NAC device.
 - The **Colubris-AVPair** attribute may be used with a HP/Colubris controller; set a suitable value for this attribute such as **max-total-octets=200000000**.

This scenario is not described further in this document, although it is possible to implement this approach with the programmable attributes in the Amigopod’s RADIUS User Roles.

- Interim accounting with dynamic authorization — In the general case, if the NAS does not provide the ability to disconnect the session automatically, the session must be monitored by the RADIUS server using RADIUS Interim Accounting updates sent by the NAS.

Once the traffic limit has been reached, the session must be terminated as it is no longer authorized. To do this, the dynamic authorization extensions to RADIUS defined in RFC 3576 are used. The remainder of this technical note describes how to implement this scenario.

Refer to Diagram 3 to understand how dynamic authorization is used to disconnect a guest session once the traffic limit has been reached.

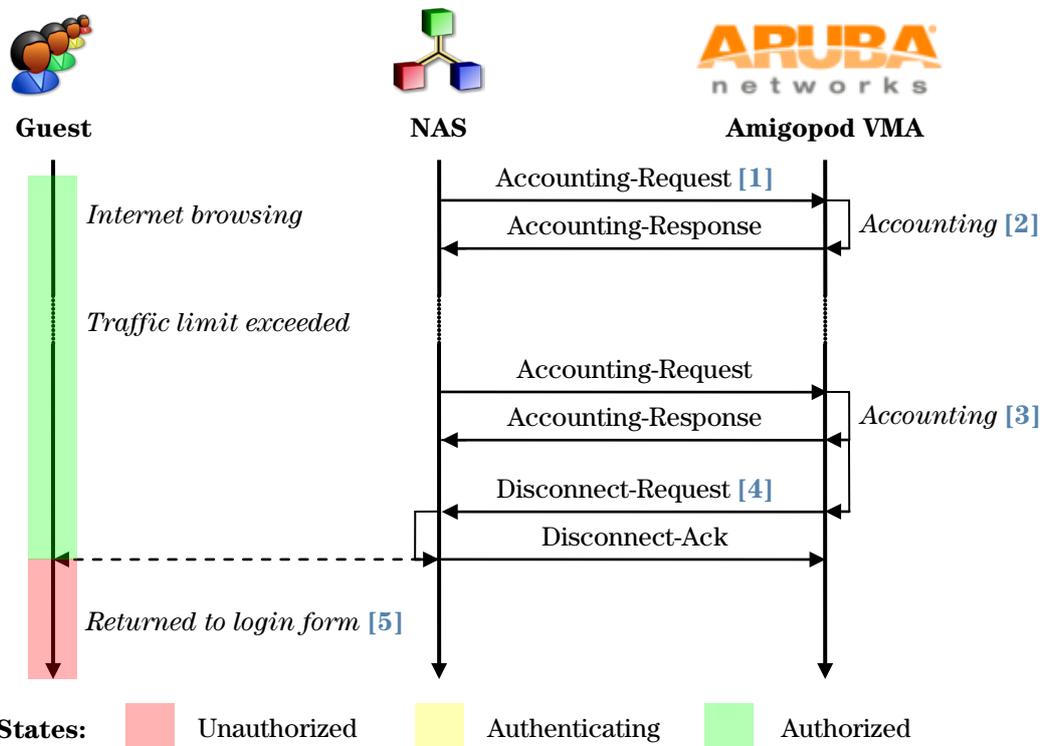


Diagram 3: Sequence diagram for interim accounting authorization

During the course of the session, the NAS sends interim accounting updates, including the current traffic counters for the session, to the RADIUS server using an Accounting-Request

message [1]. The session information is updated on the RADIUS server [2], and can be seen using the Active Sessions view.

If the guest reaches the allowed traffic limit, then on the next accounting update [3] the authorization will be rechecked. Because the session is no longer authorized to continue, the Amigopod Visitor Management Appliance will initiate an RFC 3576 Disconnect-Request [4] to the NAS, which will disconnect the visitor's session and respond with an acknowledgment.

Further attempts by the guest to access the network will trigger the NAS captive portal functionality to redirect the guest to the login form [5].

As shown in Diagram 2, the guest is now over the traffic limit and will be denied access to the network (Access-Reject) with each subsequent login attempt. This will continue until the authorization rules permit the guest to login again.

NAS Requirements

Full support for an accounting-based authorization model requires NAS equipment that supports at least **one** of the two approaches described below:

1. Support for limiting individual sessions by traffic counters.
2. Support for **both** RADIUS Interim Accounting (RFC 2869) **and** the Dynamic Authorization Extensions to RADIUS (RFC 3576) – specifically, support for the Disconnect-Request packet.

Without NAS support for either point 1 or point 2 above, accounting-based authorization cannot be implemented properly in the guest portal.

3 Configuring Accounting-Based Authorization

Check Plugin Versions

Accounting-based authorization requires the Amigopod RADIUS Services plugin, version 2.1.30 or later.

To verify you have the correct plugin versions installed, navigate to **Administrator>Plugin Manager>Manage Plugins** and check the version number in the list.

Use the **Update Plugins** link to download and install updated plugins.

Create RADIUS User Role

Navigate to **RADIUS>User Roles** and then click the **Create a new role** link.

1. Enter a suitable role name, such as **Traffic Limited Guest**, and a description for the role.
2. Add an attribute to the role. Select the **Tmp-String-1** attribute, type a description of the attribute in the Value field (“Authorization – 200 MB traffic limit”), and select **Enter condition expression...** from the **Condition** drop-down list. Use the following expression:

```
return GetUserTraffic('00:00', 'now') > 200e6 &&
AccessReject();
```

This expression limits users to a 200 MB traffic limit, measured from midnight on a daily basis, and including both uploaded and downloaded traffic towards this quota. All user sessions with the same username are counted as part of the traffic limit.

Slight variations on this expression can be used to adjust the actual traffic limit, and whether the upload and/or download statistics are counted. For details, search for the term `GetUserTraffic` in the Amigopod Deployment Guide.

3. Add another attribute. Select the **Reply-Message** attribute, and enter the following expression for the value:

```
<?= $role["name"]
```

This value expression returns the role name in the **Reply-Message** attribute; if desired, you can enter a different value to be returned.

4. Create any other attributes as required for your network access equipment.
5. Click **Save Changes** to create the new role.

Your newly created role should appear as shown in the screenshot below:

RADIUS Role Editor

Role ID: **4**

* Role Name:
Enter a name for this role.

Description:
Enter comments or descriptive text about the role.

RADIUS Attributes

Attributes:

Attribute	Value	Condition
Tmp-String-1	Authorization - 200 MB traffic limit	Expression: return GetUserTraffic('00:00', 'now') > 200e6 && AccessReject();
Reply-Message	<?= \$role["name"]	Always

Modify the list of RADIUS attributes that are attached to this role.

Create RADIUS NAS Client

Navigate to **RADIUS>NAS List** and then click the **Create** tab.

Enter suitable values for the **name** and **IP address** fields, and select a NAS Type that is marked as RFC 3576 capable.

NOTE

If the network access server does not provide RFC 3576 support, the Amigopod RADIUS server will not be able to disconnect sessions that are currently in progress. Ensure that your NAS equipment has this capability, and that it is enabled for use with the Amigopod Visitor Management Appliance.

Complete the form by providing a shared secret, and enter an optional description. Click **Create NAS Device**.

Your NAS list should appear as shown in the screenshot below:

Name	Hostname	Type	Comments
WLAN Controller	192.168.2.5	cisco_3576	Provides captive portal and ...

1 network access server

20 rows per page

Create Terms of Use page

Navigate to **RADIUS>Web Logins** and then click the **Create a new web login page** link.

1. Enter a suitable name for the page, such as **Terms of Use**, provide a page name **terms_of_use** (this will appear in the URL for the page), and optionally supply a description.
2. Select the **Cisco Systems** vendor settings. Note that this page will not actually be used to perform a web login, so the vendor settings are redundant, however they must be entered to create the page.

3. Select the **[x] Provide a custom login form** checkbox.
4. Under the **Login Page** heading, select an appropriate skin to control the look and feel of the page.
5. Enter a page title, such as **Terms of Use**, in the **Title** field.
6. Provide the HTML for the terms of use in the **Header HTML** text area.

NOTE

Refer to the “Basic HTML syntax” section of the Amigopod Deployment Guide for information about the syntax of HTML. Most document text can be easily converted to basic HTML with the addition of paragraph tags (<p>) and basic formatting is also easily applied.

7. Delete the contents of the **Footer HTML and Login Message** fields, as these are not required.
8. Click **Save Changes** to create the terms and conditions page.

Set Terms of Use URL

After creating a page that describes the terms of use, you may link it into the application by setting the Guest Manager configuration appropriately.

1. Navigate to **Customization>Guest Manager Settings**.
2. In the **Terms Of Use URL** field, enter the value **terms_of_use.php**.
3. If you have used a page name other than `terms_of_use` for the **Terms of Use** page, update this value accordingly – remember to add the suffix “.php”.
4. Click **Save Configuration** to have your changes take effect.

Create Landing page

Navigate to **RADIUS > Web Logins** and then click the **Create a new web login page** link.

1. Enter a suitable name for the page, such as **Landing Page**, provide a page name such as **traffic_stats** (this will appear in the URL for the page), and optionally supply a description.
2. Select the **Cisco Systems** vendor settings. Note that this page will not actually be used to perform a web login, so the vendor settings are redundant, however they must be entered to create the page.
3. Select the **[x] Provide a custom login form** checkbox.
4. Under the **Login Page** heading, select an appropriate skin to control the look and feel of the page.
5. Enter a page title, such as **Welcome**, in the **Title** field.
6. Enter the following template code in the **Header HTML** text area. This code is used to look up the guest’s current session information and calculate their remaining traffic quota.

```

{* NOTE: The allowed traffic limit is defined below: *}
{assign var=traffic_limit value=200e6}

{* Do not edit below this line *}
{nwa_radius_query_method=GetIpAddressCurrentSession
 _assign=current_session}

{if $current_session.username}
 {nwa_radius_query_method=GetUserTraffic
 username=$current_session.username from_time="00:00"
 to_time="now" _assign=traffic_used}
{else}
 {assign var=traffic_used value=0}
{/if}

{assign var=traffic_remaining value=`$traffic_limit-
 $traffic_used`}

```

If you are using a traffic limit other than 200 MB, you should adjust the value in **{assign var=traffic_limit value=200e6}**. Here, **200e6** is a value indicating 200,000,000 bytes. For example, to set up a 500 MB quota, you could use the value **500e6** instead.

7. Enter the following template code in the Footer HTML text area. This code is used to display information about the guest's current usage, a message about the service, and a link to the guest's home page.

```

{* This is the actual message displayed *}

{if $current_session.username}
<p>
  Hello <b>{$current_session.username}</b>, you are now
  logged into the WiFi network.
</p>
{else}
<p>
  You are now logged into the WiFi network.
</p>
{/if}

{*
<h3>
  Your Usage
</h3>
*}
<table {$table class content}>
<tr><th class="nwaTop">Your Usage</th></tr>
<tr><td class="nwaBody">

{nwa icontext icon="images/icon-info22.png" valign="middle"
 novspace="1"}
  Your daily traffic quota is
  <b>{$traffic_limit|NwaByteFormatBase10:0}</b>.
{/nwa icontext}

</td></tr><tr><td class="nwaBody">

```

```

{nwa_icontext icon="images/icon-clock22.png" valign="middle"
novspace="1"}
    So far today, you have used
    <span class="nwaImportant">
    {$traffic_used|NwaByteFormatBase10:0}</span>.
{/nwa_icontext}

</td></tr><tr><td class="nwaBody">

{nwa_icontext icon="images/icon-report-bytes-out22.png"
valign="middle" novspace="1"}
    Your remaining quota is
    <span class="nwaImportant">
    {$traffic_remaining|NwaByteFormatBase10:0}</span>.
{/nwa_icontext}

</td></tr></table>

<h3>
    About This Service
</h3>
<p>
    To ensure the highest quality of service for all
    of our visitors, the use of this WiFi service is
    subject to a <b>quota</b>.
</p>
<p>
    This means that you can only download a limited
    amount of information before you will be
    disconnected.
</p>
<p>
    Traffic quotas are reset at <b>midnight</b>
    every day.
</p>
<p>
    To ensure you do not go over your quota, follow
    these tips:
</p>
<ul>
    <li>Do not use file-sharing or peer-to-peer services like
    BitTorrent</li>
    <li>Avoid downloading large files</li>
    <li>Limit your use of video sharing sites like YouTube</li>
</ul>

<h3>
    Terms of Use
</h3>
<p>
    By logging in to the network, you agree to the
    <a href="terms_of_use.php" target="_blank">terms of use</a>.
</p>

{* link to home page *}

```

```

<style type="text/css">
```

traffic (as recommended by the Amigopod Security Manager), then update the Default URL accordingly:

```
https://{Smarty.server.HTTP_HOST}/traffic_stats.php
```

If you have used a page name other than **traffic_stats** for the landing page, then update the Default URL accordingly.

6. Select the **[x] Force default destination for all clients** checkbox. This is to ensure that guests are always redirected to the landing page to view their current traffic statistics after logging in.
7. Under the **Login Page** heading, select an appropriate skin to control the look and feel of the page.
8. Enter a page title, such as **Login**, in the **Title** field.
9. To display an error message if a login attempt is unsuccessful (due to a failed authorization), some logic may be added to the **Header HTML** text area.

```
<p>
  Please login to the network using your Amigopod
  username and password.
</p>
{if $err_flag}
{nwaicontext type=error}
Login attempt failed. Your username or password may be
invalid, or you may have exceeded your daily download limit.
{/nwaicontext}
{/if}
```

The above example is suitable for Cisco wireless equipment, which will supply an **err_flag** parameter on redirect to the login page indicating if the RADIUS authentication attempt failed. Equipment from other vendors may use a different field name; the parameter can often be determined by carefully examining the redirection URL generated by the NAS equipment. Contact Amigopod support if you require additional assistance.

10. The other text displayed on the login page may be customized using the **Header HTML** and **Footer HTML** text areas.

For example, to display information about the terms of use, you might use the following Footer HTML:

```
<h3>Terms of Use</h3>
<p>
  By logging in to the network, you agree to the
  <a href="terms of use.php" target=" blank">
  Terms of Use</a>.
</p>
```

11. The text of the login message page may be customized using the **Login Message** text area.
12. Set a suitable login delay such as **2** seconds.
13. Click **Save Changes** to create the terms and conditions page.

Additional Configuration Guidelines

To complete the deployment, ensure that each of the following points has been taken into consideration:

- The NAS captive portal should redirect guests to the login page, which will be located at a URL such as: <http://amigopod/login.php>.
- If you are using HTTPS for guest traffic (as recommended by the Amigopod Security Manager), then update the URL accordingly, e.g. <https://amigopod/login.php>.
- If you have used a page name other than **login** for the login page, then update the URL accordingly, e.g. https://amigopod/acme_login.php.
- The NAS should be configured to authenticate guests with the Amigopod RADIUS server.
- The NAS should be configured to send session accounting traffic to the Amigopod RADIUS server.
- The NAS should be configured to accept dynamic authorization (RFC 3576) requests from the Amigopod RADIUS server.
- Use the same shared secret for authentication, accounting and dynamic authorization; on the Amigopod RADIUS server, the shared secret configured for the NAS is used for all three functions.
- Interim accounting on the NAS should be enabled where possible; the `Acct-Interim-Interval` RADIUS attribute may be required to enable interim accounting and set the interval, or the interim accounting interval may be configured separately on the NAS. Consult the NAS vendor's documentation for additional details.

Refer to the Amigopod integration guide corresponding to your vendor's equipment for additional information about configuring other basic networking aspects of the deployment.

Also note that this technical note does not cover guest account provisioning. For details on sponsored account creation, guest self-registration or guest purchased access, refer to the appropriate section in the Amigopod Deployment Guide.

4 Verifying Accounting-Based Authorization

Check NAS captive portal settings

Connect to the guest network, and open a web browser.

Ensure that the NAS captive portal takes effect, and redirects your web browser to the login page.

Troubleshooting tips: If these steps are unsuccessful, check your NAS equipment configuration (wired or wireless).

- Is the client able to reach the NAS controller?
- Is the client able to reach the Amigopod Visitor Management Appliance?
- Has the correct external login page URL been provided?

Check terms of use page

Click the “terms of use” link on the login page.

Verify that the terms of use are displayed in a separate browser window.

Troubleshooting tips: If the terms of use page is not displayed, or displays incorrectly, check the following items:

- Has the correct link to the terms of use page been configured under **Customization > Guest Manager settings**, and in the login and/or landing page Header/Footer HTML text areas?
- Does the Terms of Use web login page have valid HTML syntax for the text to be displayed?

Check login page

Attempt to log into the network using an invalid username or password. Verify that the login page displays an error message stating “Invalid username or password”.

Attempt to log into the network without selecting the “I accept the terms of use” checkbox. Verify that the login page displays an error message stating “In order to log in, you must accept the terms and conditions”.

Log in to the network using a valid username and password. Verify that the login message is displayed briefly, followed by the landing page.

Troubleshooting tips: If the login is not successful check the following items:

- Have you provided the correct vendor settings for the login page?
- Is the NAS equipment actually receiving the login attempt from the client and performing a RADIUS login attempt? This can be checked by looking for a RADIUS authentication attempt from the NAS, at **RADIUS > Server Control** or under **Administrator > System Logs**.

- Is the correct shared secret configured on both the NAS and the Amigopod RADIUS Server?
- Is the guest account authorized? Check that the account is enabled, has the correct role, and that the authorization is not failing. Authorization failures are indicated with a log message in **Administrator>System Logs**.

Check landing page

At the landing page, verify that your username is displayed, along with your current usage information and the remaining quota.

Verify that clicking the **Go to my home page** link redirects you to your home page. This indicates that the login has been successful and you are now authorized to use the network.

Using the Amigopod WebUI, navigate to **Guests>Active Sessions** and verify that there is a session listed for your username.

Perform some Internet browsing while you wait for the interim accounting interval to elapse (RFC 2869 recommends a minimum interval of 600 seconds, or 10 minutes, however it may be configured to a smaller value to gain tighter control over traffic limits and provide a more up-to-date view of session statistics on the landing page). Verify that the interim accounting update is reflected in both the Active Sessions list, and on the guest's landing page.

Log out of the network, and then log back in. Verify that the traffic statistics displayed include the previous session's traffic.

Check traffic limit

While connected to the guest network, generate enough traffic to exceed the traffic limit.

Verify that the session is disconnected via an RFC 3576 Disconnect-Request. An authorization failure message should be logged in the application log (check in **Administrator>System Logs**), as well as a message related to the session disconnection.

Troubleshooting tips: If the session is not disconnected, check the following items:

- Is the correct authorization condition configured in the RADIUS user role?
- Is the NAS device receiving an RFC 3576 request?
- Is the correct shared secret configured on both the NAS and the Amigopod RADIUS Server?

5 Modifying Accounting-Based Authorization

Adjusting the traffic limit

The traffic limit is configured in two places:

1. In the **RADIUS User Role** as part of an authorization expression – the value is used to compare against the guest’s current traffic measurement and determine if the access request should be permitted.
2. In the **RADIUS Web Login** as part of the landing page – the value is used to determine the guest’s remaining quota after subtracting the guest’s current traffic measurement.

To increase or decrease the traffic quota, change the traffic limit defined in both of the places listed above.

Count only uploaded or downloaded traffic

The default configuration in this technical note counts both uploaded and downloaded traffic towards the quota.

It is possible for the quota to be measured in one direction only, i.e. either guest uploads or downloads.

Accounting terminology

RADIUS Accounting uses a definition of “input” and “output” octets that corresponds to upload and download.

NOTE

The following discussion assumes that the NAS equipment follows the normal convention that “upload” and “download” are relative to the NAS. In this convention, traffic **received from** a client (i.e. uploaded by the client) is **input** traffic, and traffic **sent to** a client (i.e. downloaded by the client) is **output** traffic. Certain vendors use the opposite convention, in which case you must reverse the definition of “input” and “output”.

If in doubt, perform a large download from a client connected to the NAS in question, and check the accounting statistics – if the “Session Download” is the larger number, then the normal convention applies, and “input” is “upload”. Otherwise, if the “Session Upload” is the larger number, then the reverse convention applies, and “input” is “download”.

Session Traffic	Normal Convention	Reversed Convention
Guest Upload	Input	Output
Guest Download	Output	Input

Counting only downloaded traffic

Two modifications are required to change the quota measurement.

First, use the following condition expression in the RADIUS User Role to count only “output” traffic (in the normal convention, traffic downloaded by a client):

```
return GetUserTraffic('00:00', 'now', 'out') > 200e6 &&  
AccessReject();
```

The additional parameter 'out' indicates that “output” traffic should be calculated. Alternatively, you may specify 'in' instead to count only “input” traffic, or any other value (the default) to count both “input” and “output” traffic.

Secondly, update the following template code in the Header HTML of the landing page. This is required to calculate the actual traffic today for the current user:

```
{nwa_radius_query _method=GetUserTraffic  
username=$current_session.username from_time="00:00" to_time="now"  
in_out="out" _assign=traffic_used}
```

As above, the in_out parameter may be set to “in”, “out” or “in_out” to include both directions.