



Configuring Authentication

CHAPTERS

1. Overview
2. Local Authentication Configuration
3. Radius Authentication Configuration
4. Onekey Online Configuration
5. Guest Resources Configuration
6. Viewing the Authentication Status
7. Configuration Example



This guide applies to:

TL-ER5120 v3, TL-ER6120 v2, TL-ER6020 v2, TL-R600VPN v4, TL-R480T+ v9, TL-R470T+ v6.

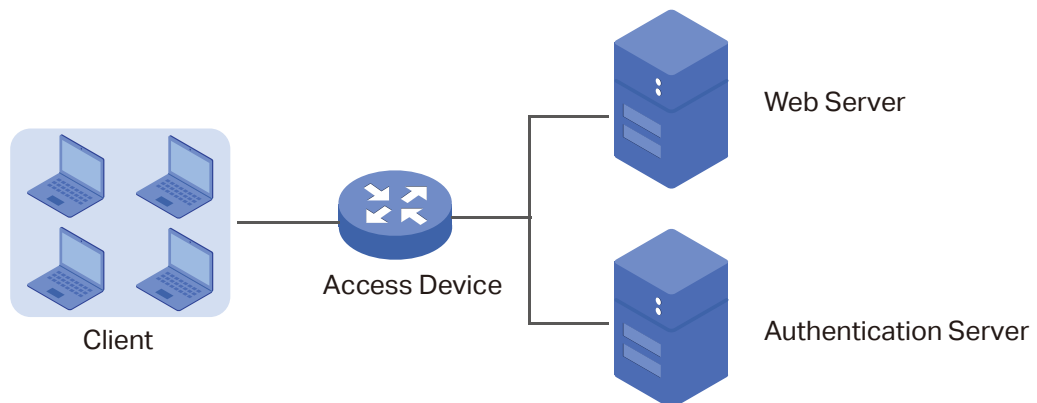
1 Overview

Portal authentication, also known as Web authentication, is usually deployed in a guest-access network (like a hotel or a coffee shop) to control the client's internet access. In portal authentication, all the client's HTTP requests will be redirected to an authentication page first. The client needs to enter the account information on the page to authenticate, then can visit the internet after the authentication succeeded.

1.1 Typical Topology

The typical topology of portal authentication is shown as below:

Figure 1-1 Topology of Portal Authentication



- **Client**

The end device that needs to be authenticated before permitted to access the internet.

- **Access Device**

The device that supports portal authentication. In this configuration guide, it means the router. The Access Device helps to: redirect all HTTP requests to the Web Server before authenticated; interact with the Authentication Server to authenticate the client during the authentication process; permit users to access the internet after the authentication succeeded.

- **Web Server**

The web server responds to client's HTTP requests, and returns an authentication login page.

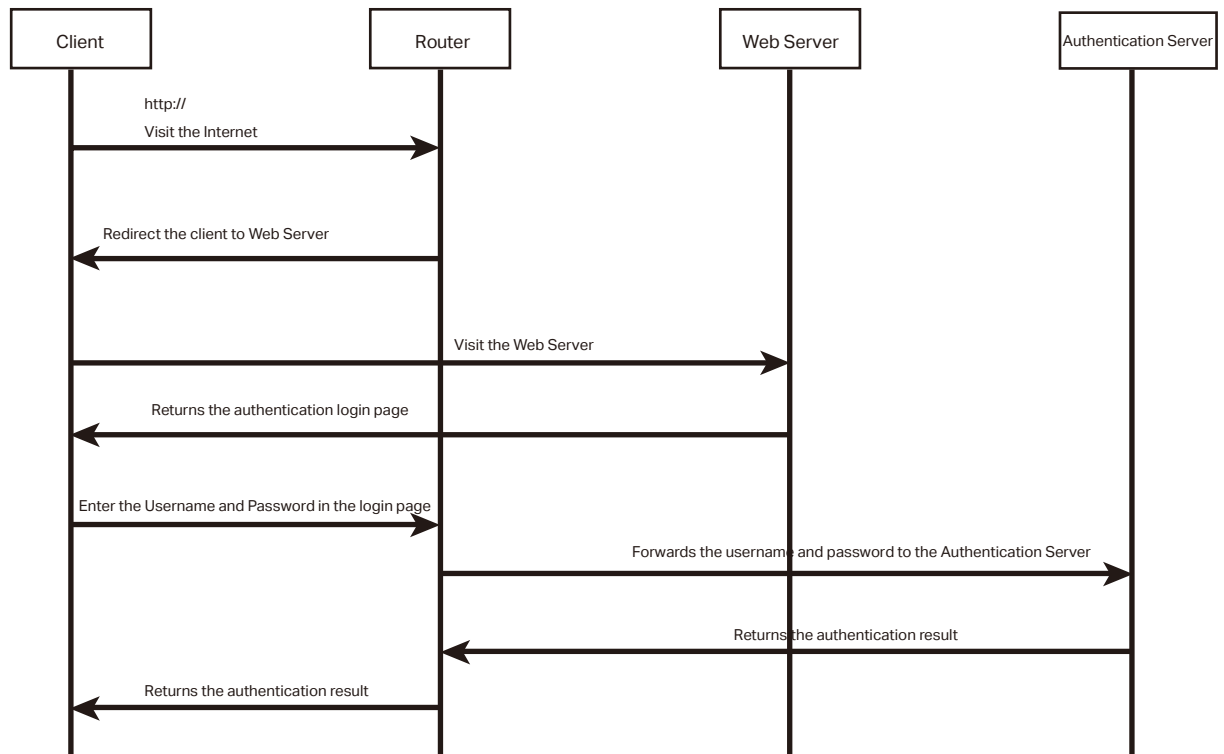
- **Authentication Server**

The authentication server records the information of the user's account, and interacts with the access device to authenticate clients.

1.2 Portal Authentication Process

The portal authentication process is shown as below:

Figure 1-2 Portal Authentication Process



- 1) The client is connected to the router but not authenticated, and starts to visit the internet through HTTP;
- 2) The router redirects the client's HTTP request to the web server;
- 3) The client visits the web server;
- 4) The Web server returns the authentication login page to the client;
- 5) The client enters the username and password on the authentication login page;
- 6) The router forwards the username and password to the authentication server;
- 7) The authentication server returns the authentication result to the router;
- 8) The router replies to the client with the authentication result;
- 9) The client visits the internet after the authentication succeeded.

1.3 Supported Features

To configure portal authentication, you need to configure both the web server and the authentication server. The web server provides the authentication page for login; the authentication server records the account information and authenticates the clients.

1.3.1 Supported Web Server

The router has a built-in web server and also supports external web server. You can configure the authentication page either using the built-in server or the external server.

Custom Page

You can use the built-in web server and customize the authentication page on your router.

External Links

You can specify the external web server and configure the authentication page on the external web server.

1.3.2 Supported Authentication Server

The router provides three types of portal authentication:

Radius Authentication

In Radius authentication, you can specify an external Radius server as the authentication server. The user's account information are recorded in the Radius server.

Local Authentication

If you don't have an additional Radius server, you can choose local authentication. In local authentication, the router uses the built-in authentication server to authenticate. The built-in authentication server can record at most 500 local user accounts, and each account is can be used for at most 1024 clients to authenticate.

Onekey Online

In Onekey Online Authentication, users can access the network without entering any account information.

1.3.3 Guest Resources

Guest Resources is used to provide free resources for users before they pass the portal authentication.

2 Local Authentication Configuration

To configure local authentication, follow the steps:

- 1) Configure the authentication page.
- 2) Configure the local user account.

2.1 Configuring the Authentication Page

The browser will redirect to the authentication page when the client try to access the internet. On the authentication page, the user need to enter the username and password to log in. After the authentication succeeded, the user can access the internet.

Choose the menu **Authentication > Authentication Settings > Web Authentication** to load the following page.

Figure 2-1 Configuring the Authentication Page

Settings

Status: Enable

Idle Timeout: minutes (0 or 5-1440, 0 means always online)

Portal Authentication Port: (8080, 1024-65535)

Authentication Parameters

Authentication Page:

Background Picture: --- (The image size cannot exceed 200KB.)

Welcome Information: (1-50 characters)

Copyright: (1-50 characters)

Page Preview:

Radius Type:

Expiration Reminder: Enable

Time to Remind: days (1-10)

Remind Type:

Remind Interval: minutes (1-120)

Remind Content: (1-50 characters)

Page Preview:

Follow these steps to configure authentication page:

- 1) In the **Settings** section, enable authentication status, configure the idle timeout and portal authentication port.

Status	Check the box to enable portal authentication.
Idle Timeout	Specify the idle timeout. The client will be disconnected after the specified period (Idle Timeout) of inactivity, and is required to be authenticated again. Value 0 means the client will always keep online until the authentication timeout leased, even if the client remains inactive.
Portal Authentication Port	Enter the service port for portal authentication. The default setting is 8080.

- 2) In the **Authentication Parameters** section, configure the parameters of the authentication page.

Authentication Page	<p>Choose the authentication page type.</p> <p>Custom: You can use the built-in web server to customize the authentication page by specifying the background picture, welcome information and copyright information.</p> <p>External Links: You can specify a external web server to provide the authentication page by entering the URL of the external web server.</p>
Background Picture	Click the Upload button to choose a local image as the background picture of the custom authentication page.
Welcome Information	Specify the welcome information to be displayed on the custom authentication page.
Copyright	Specify the copyright information to be displayed on the custom authentication page.
Page Preview	Click the Login Page Preview button, and you can preview the customized authentication page
Authentication URL	Specify the URL for authentication page if you choose the Authentication Page as "External Links". The browser will redirect to this URL when the client starts the authentication.
Success Redirect URL	Specify the Success Redirect URL if you choose the Authentication Page as "External Links". The browser will redirect to this URL after the authentication succeeded.
Fail redirect URL	Specify the Fail Redirect URL if you choose the Authentication Page as "External Links". The browser will redirect to this URL if the authentication failed.

 **Note:**

If the web server is not deployed in the LAN, you need to create a Guest Resource entry to ensure the client can access the external web server before the authentication succeeded. For the configuration of Guest Resource, go to [Guest Resources Configuration](#).

3) Choose the authentication type, and configure the expiration reminder, then click **Save**.

Authentication Type	Choose the authentication type as Local Authentication.
Expiration Reminder	Check the box to enable expiration reminder. A remind page will appear to remind users when the online time is about to expire.
Time to Remind	Specify the number of days before the expiration date to remind users.
Remind Type	<p>Specify the remind type.</p> <p>Remind Once: Remind the user only once after the authentication succeeded.</p> <p>Remind Periodically: Remind users at specified intervals during the remind period.</p>

Remind Interval	Specify the interval at which the router reminds users if the remind type is specified as "Remind Periodically".
Remind Content	Specify the remind content. The content will be displayed on the Remind page.
Page Preview	Click the button to view the remind page.

2.2 Configuring the Local User Account

In Local authentication, the router uses the built-in authentication server to authenticate users. You need to configure the authentication accounts for the local users.

The router supports two types of local users:

Formal User: If you want to provide the user with network service for a long period of time (in days), you can create Formal User accounts for them.

Free User: If you want to provide the user with network service for a short period of time (in minutes), you can create Free User accounts for them.

2.2.1 Configuring the Local User Account

- **Configuring the Formal User Account**

Choose the menu **Authentication > User Management > User Management** and click **Add** to load the following page.

Figure 2-2 Configuring the Formal User Account

<input type="checkbox"/>	ID	User Type	Username	Authentication Timeout	MAC Address	Description	Status	Operation
--	--	--	--	--	--	--	--	--

User Type: Formal User ▼

Username: (1-100 Characters)

Password: (1-100 Characters)

Expiration Date: 2017-12-31 (YYYY-MM-DD)

Authentication Peroid: 00:00-24:00 (HH:MM-HH:MM)

MAC Binding Type: Static Binding ▼

MAC Address : (XX-XX-XX-XX-XX-XX)

Maximum Users: 1 (1-1024)

Upstream Bandwidth: 0 Kbps (0 or 10-1,000,000. 0 means no limit)

Downstream Bandwidth: 0 Kbps (0 or 10-1,000,000. 0 means no limit)

Name: (1-50 characters, optional)

Telephone: (1-50 characters, optional)

Description: (1-50 characters, optional)

Status: Enable

OK
Cancel

Specify the user type, configure the username and password for the formal user account, and configure the other corresponding parameters. Then click **OK**.

User Type	Specify the user type as Formal User.
Username / Password	Specify the username and password of the account. The username cannot be the same as any existing one.
Expiration Date	Specify the expiration date of the account. The formal user can use this account to authenticate before this date.
Authentication Peroid	Specify the period during which the client is allowed to be authenticated.
MAC Binding Type	<p>Specify the MAC Binding type. There are three types of MAC Binding: No binding, Static Binding and Dynamic Binding.</p> <p>No Binding: The client's MAC address will not be bound.</p> <p>Static Binding: Manually enter the MAC address of the client to be bound. Only the bound client is able to use the username and password to authenticate.</p> <p>Dynamic Binding: The MAC address of the first client that passes the authentication will be bound. Afterwards only the bound client is able to use the username and password to authenticate.</p>
MAC Address	Enter the MAC address of the client to be bound if you choos the MAC Binding type as "Static Binding".

Maximum Users	Specify the maximum number of users that are allowed use this account to authenticate. Note: If the MAC Binding Type is either Static Binding or Dynamic Binding, only one client can use this username and password to authenticate,i.e., the bound client, even if the value of Maximum Users is configured to be greater than one.
Upstream Bandwidth / Downstream Bandwidth	Optional. Specify the upstream / downstream bandwidth for the user. 0 means no limit.
Name	Optional. Record the user's name.
Telephone	Optional. Record the user's telephone number.
Description	Optional. Enter a brief description for the user.
Status	Check the box to enable this account.

■ **Configuring the Free User Account**

Choose the menu **Authentication > User Management > User Management** and click **Add** to load the following page.

Figure 2-3 Configuring the Free User Account

<input type="checkbox"/>	ID	User Type	Username	Authentication Timeout	MAC Address	Description	Status	Operation
--	--	--	--	--	--	--	--	--

User Type: Free User ▼

Username: (1-100 Characters)

Password: (1-100 Characters)

Authentication Timeout (minutes): 30 (1-1440)

Authentication Peroid: 00:00-24:00 (HH:MM-HH:MM)

Maximum Users: 1 (1-1024)

Upstream Bandwidth: 0 Kbps (0 or 10-1,000,000. 0 means no limit)

Downstream Bandwidth: 0 Kbps (0 or 10-1,000,000. 0 means no limit)

Description: (1-50 characters, optional)

Status: Enable

OK
Cancel

Specify the user type, configure the username and password for the free user account, and configure the other corresponding parameters. Then click **OK**.

User Type	Specify the user type as Free User.
------------------	-------------------------------------

Username / Password	Specify the username and password of the user account. The username cannot be the same as any existing one.
Authentication Timeout	Specify the free duration of the account. The default value is 30 minutes.
Maximum Users	Specify the maximum number of users that are allowed to use this username and password to authenticate.
Upstream Bandwidth / Downstream Bandwidth	Optional. Specify the upstream/downstream bandwidth for the user. 0 means no limit.
Status	Check the box to enable this account.

2.2.2 (Optional) Configuring the Backup of Local Users

Choose the menu **Authentication > User Management > Configuration Backup** to load the following page.

Figure 2-4 Configuring the Formal User

The screenshot shows a web interface with two main sections: 'Backup' and 'Restore'. The 'Backup' section contains a single button labeled 'Backup'. The 'Restore' section contains a 'File:' label, an empty text input field, a 'Browse' button, and a 'Restore' button.

- To backup local users' accounts

Click **Backup** button to backup all the local users accounts as a CSV file in ANSI coding format.

- To restore local users' accounts

You can import the accounts to the router if you have backups. Click **Browse** to select the file path (the backup must be a CSV file), then click **Restore** to restore the accounts.

You can also manually add multiple local user accounts at a time:

- 1) Create an Excel file and add the local user accounts to it, then save the Excel file as a CSV file with ANSI coding format. You can click **Backup** to obtain a CSV file to view the correct format.
- 2) Click **Browse** to select the file path, then click **Restore** to restore the file.

 **Note:**

Using Excel to open the CSV file may cause some numerical format changes, and the number may be displayed incorrectly. If you use Excel to edit the CSV file, please set the cell format as text.

3 Radius Authentication Configuration

To configure Radius Authentication, follow the steps:

- 1) Configure the authentication page.
- 2) Specify the external Radius server and configure the corresponding parameters.

3.1 Configuring Radius Authentication

Choose the menu **Authentication > Authentication Settings > Web Authentication** to load the following page.

Figure 3-1 Configuring the Radius Authentication

Settings

Status: Enable

Idle Timeout: minutes (0 or 5-1440, 0 means always online)

Portal Authentication Port: (8080, 1024-65535)

Authentication Parameters

Authentication Page: ▼

Background Picture: --- (The image size cannot exceed 200KB.)

Welcome Information: (1-50 characters)

Copyright: (1-50 characters)

Page Preview:

Authentication Type: ▼

Primary Radius Server: (Required)

Secondary Radius Server: (Optional)

Authentication Port: (1024-65535)

Authorized Share Key: (1-48 characters)

Retry Times: (1-10)

Timeout Interval: (1-60 seconds)

Authentication Method: ▼

Follow these steps to configure Radius Authentication:

- 1) In the **Settings** section, enable the authentication status, configure the idle timeout and portal authentication port.

Status	Check the box to enable portal authentication.
---------------	--

Idle Timeout	Specify the idle timeout. The client will be disconnected after the specified period (Idle Timeout) of inactivity, and is required to be authenticated again. Value 0 means the client will always keep online until the authentication timeout leased, even if the client remains inactive.
Portal Authentication Port	Enter the service port for portal authentication. The default setting is 8080.

- 2) In the **Authentication Parameters** section, configure the parameters of the authentication page.

Authentication Page	Choose the authentication page type. Custom: You can use the built-in web server to customize the authentication page by specifying the background picture, welcome information and copyright information. External Links: You can use external pages by specifying the external links as the authentication page.
Background Picture	Click the Upload button to choose a local image as the background picture of the custom authentication page.
Welcome Information	Specify the welcome information to be displayed on the custom authentication page.
Copyright	Specify the copyright information to be displayed on the custom authentication page.
Page Preview	Click the Login Page Preview button, and you can preview the customized authentication page
Authentication URL	Specify the URL for authentication page if you choose the Authentication Page as "External Links". The browser will redirect to this URL when the client starts the authentication.
Success Redirect URL	Specify the Success Redirect URL if you choose the Authentication Page as "External Links". The browser will redirect to this URL after the authentication succeeded.
Fail redirect URL	Specify the Fail Redirect URL if you choose the Authentication Page as "External Links". The browser will redirect to this URL if the authentication failed.

 **Note:**

If the web server is not deployed in the LAN, you need to create a Guest Resource entry to ensure the client can access the external web server before the authentication succeeded. For the configuration of Guest Resource, go to [Guest Resources Configuration](#).

- 3) Specify the external Radius server and configure the corresponding parameters, then click **Save**.

Authentication Type	Choose the authentication type as Radius Authentication.
---------------------	--

Primary Radius Server	Enter the IP address of the primary Radius server.
Secondary Radius Server	Optional. Enter the IP address of the secondary Radius server. If the primary server is down, the secondary server will be effective.
Authentication Port	Enter the service port for Radius authentication. By default, it is 1812.
Authorized Share Key	Specify the authorized share key. This key should be the same configured in the Radius server.
Retry Times	Specify the number of times the router will retry sending authentication requests after the authentication failed.
Timeout Interval	Specify the timeout interval that the client can wait before the radius server replies.
Authentication Method	Specify the authentication protocol as PAP or CHAP.

4 Onekey Online Configuration

In Onekey Online authentication, users only need to click the “Onekey online” button on the authentication page, then can access the internet. The username and password are not required.

4.1 Configuring the Authentication Page

Choose the menu **Authentication > Authentication Settings > Web Authentication** to load the following page.

Figure 4-1 Configuring the Web Authentication

Settings

Status: Enable

Idle Timeout: minutes (0 or 5-1440, 0 means always online)

Portal Authentication Port: (8080, 1024-65535)

Authentication Parameters

Authentication Page: ▼

Background Picture: --- (The image size cannot exceed 200KB.)

Welcome Information: (1-50 characters)

Copyright: (1-50 characters)

Page Preview:

Radius Type: ▼

Free Authentication Timeout: minutes (1-1440)

Follow these steps to configure Onekey Online Authentication:

- 1) In the **Settings** section, enable the authentication status, configure the idle timeout and portal authentication port.

Status	Check the box to enable portal authentication.
Idle Timeout	Specify the idle timeout. The client will be disconnected after the specified period (Idle Timeout) of inactivity, and is required to be authenticated again. Value 0 means the client will always keep online until the authentication timeout leased, even if the client remains inactive.

Portal Authentication Port	Enter the service port for portal authentication. The default setting is 8080.
----------------------------	--

- 2) In the **Authentication Parameters** section, configure the parameters of the authentication page and choose the authentication type, then click **Save**.

Authentication Page	Choose the type of authentication page as Custom Page. Note: External Links is not available for Onekey Online.
---------------------	--

Background Picture	Click the Upload button to choose a local image as the background picture of the custom authentication page.
--------------------	---

Welcome Information	Specify the welcome information to be displayed on the custom authentication page.
---------------------	--

Copyright	Specify the copyright information to be displayed on the custom authentication page.
-----------	--

Page Preview	Click the Login Page Preview button, and you can preview the customized authentication page
--------------	--

Authentication Type	Choose the authentication type as Onekey Online.
---------------------	--

Free Authentication Timeout	Specify the free duration for Onekey Online. When the free duration expired, users can click "Onekey Online" button on the authentication page to continue to visit the internet.
-----------------------------	---

5 Guest Resources Configuration

Guest resources are limited network resources provided for users before they pass the portal authentication.

You can configure the guest resources in two ways:

- **Five Tuple Type**

Specify the client and the network resources the client can visit based on the settings of IP address, MAC address, VLAN ID, service port and protocol. It is recommended to select Five Tuple Type when the IP address and service port of the free network resource are already known.

- **URL Type**

Specify the client and the network resources the client can visit based on the settings of the URL, IP address, MAC address and service port. It is recommended to select URL Type when the URL of the free network resource is already known.

 **Note:**

By default, the Guest Resource table is empty, which means all the clients cannot visit any network resource before they pass the portal authentication.

5.1 Configuring the Five Tuple Type

Choose the menu **Authentication > Authentication Settings > Guest Resources** and click **Add** to load the following page.

Figure 5-1 Configuring the Five Tuple Type

<input type="checkbox"/>	ID	Name	Type	Source IP Range	Destination IP Range	Source Port	Destination Port	Status	Operation
--	--	--	--	--	--	--	--	--	--

Name: (1-50 characters)

Type: Five Tuple Type ▼

Source IP Range: / (Optional)

Destination IP Range: / (Optional)

Source MAC Address: (XX-XX-XX-XX-XX-XX, optional)

Source Port Range: – (1-65535, optional)

Destination Port Range: – (1-65535, optional)

Protocol: TCP ▼

Description: (1-50 characters)

Status: Enable

Specify the client and the network resources the client can visit by configuring the IP address, MAC address and service port, then click **OK**.

Name	Enter the name of the guest resource entry.
Type	Choose the guest resource type as Five Tuple Type.
Source IP Range	Specify the IP range of the client(s) by entering the network address and subnet mask bits. Only the specified clients can visit the guest resources.
Destination IP Range	Specify the IP range of the server(s) that provides the guest resources by entering the network address and subnet mask bits.
Source MAC Address	Enter the MAC address of the client.
Source Port Range	Enter the source service port range.
Destination Port Range	Enter the destination service port range.
Description	Enter a brief description for the Guest Resources entry to make it easier to search and manage.
Protocol	Specify the protocol as TCP or UDP for the Guest Resources.
Status	Check the box to enable the guest resource entry.

 **Note:**

In a Guest Resource entry, if some parameter is left empty, it means the router will not restrict that parameter. For example, if the source IP range is left empty, it means all the clients can visit the specified guest resources.

5.2 Configuring the URL Type

Choose the menu **Authentication > Authentication Settings > Guest Resources** and click **Add** to load the following page.

Figure 5-1 Configuring the URL

<input type="checkbox"/>	ID	Name	Type	Source IP Range	Destination IP Range	Source Port	Destination Port	Status	Operation
--	--	--	--	--	--	--	--	--	--

Name: (1-50 characters)

Type: URL Type ▼

URL Address: (1-128 characters)

Source IP Range: / (Optional)

Source MAC Address: (XX-XX-XX-XX-XX-XX, optional)

Source Port Range: - (1-65535, optional)

Description: (1-50 characters)

Status: Enable

Specify the client and the network resources the client can visit by configuring the URL of the network resource and the parameters of the clients, then click **OK**.

Name	Enter the name of the guest resource entry.
Type	Choose the guest resource type as URL Type.
URL Address	Enter the URL address or IP address of the network resource that can be visited for free.
Source IP Range	Configure the IP range of the client(s) by entering the network address and subnet mask bits.
Source MAC Address	Enter the MAC address of the client.
Source Port Range	Enter the source service port range.

Description	Enter a brief description for the Guest Resources entry to make it easier to search and manage.
--------------------	---

Status	Check the box to enable the guest resource entry.
---------------	---




 **Note:**

In a Guest Resource entry, if some parameter is left empty, it means the router will not restrict that parameter. For example, if the source IP range is left empty, it means all the clients can visit the specified guest resources.

6 Viewing the Authentication Status

Choose the menu **Authentication > Authentication Status > Authentication Status** to load the following page.

Figure 6-1 Viewing the Authentication Status

Authenticated User List						
Entry Count: 1		 Refresh  Offline				
<input type="checkbox"/>	ID	Type	Starting Time	IP Address	MAC Address	Operation
<input type="checkbox"/>	1	Local Authentication	2017-1-1 1:10:54	192.168.0.197	74-D4-35-9F-DB-1C	

Here you can view the clients that pass the portal authentication.

Type	Displays the authentication type of the client.
Starting Time	Displays the starting time of the authentication.
IP Address	Displays the client's IP address.
MAC Address	Displays the client's MAC address.

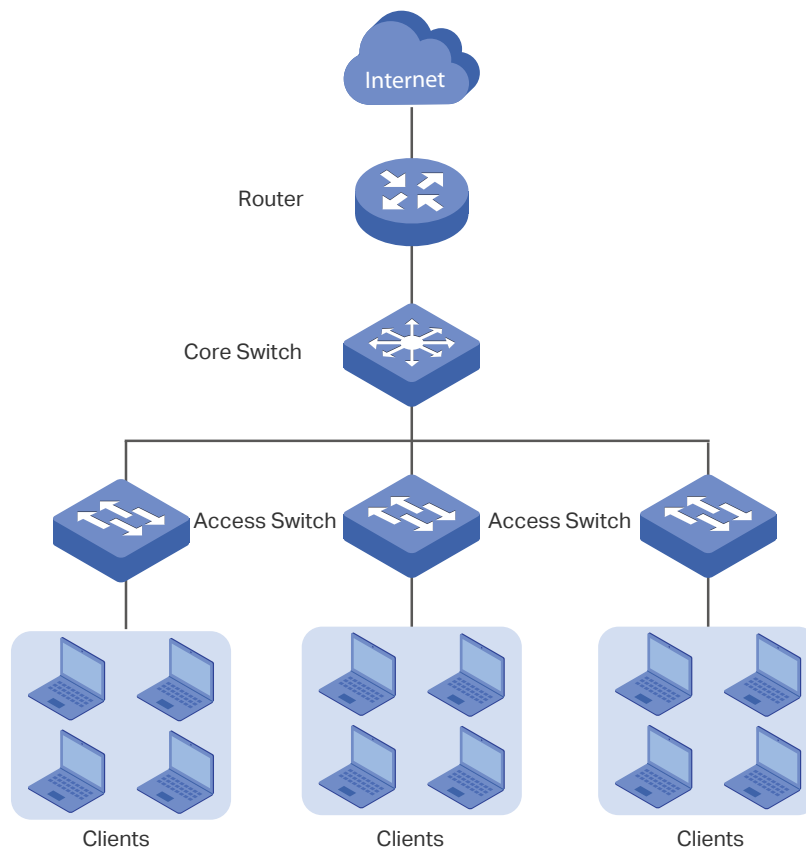
7 Configuration Example

Here we take the application of Local Authentication as an example.

7.1 Network Requirements

A hotel needs to offer internet service to the guests and push hotel advertisement. For network security, only the authorized guests can access the internet.

Figure 7-1 Network Topology



7.2 Configuration Scheme

For the hotel does not have an external Web server or Authentication server, it is recommended to choose Local Authentication to meet this requirement.

- To control the guests' internet access, you can create local user accounts for the guests. The guests need to use the accounts assigned to them to get authenticated, then can visit the internet. The other people cannot visit the internet through the hotel's network without authentication accounts.

- To push hotel advertisement, you can simply customize the authentication page by set the background picture and the welcome information.

7.3 Configuration Procedures

- 1) Enable Portal Authentication, choose the authentication type as Local Authentication, and customize the authentication page.
- 2) Create the authentication accounts for the guests.

7.3.1 Configuring the Authentication Page

Choose the menu **Authentication > Authentication Settings > Web Authentication** to load the following page.

- 1) Enable portal authentication, and keep the Idle Timeout and Portal Authentication Port as default settings.

Figure 7-2 Enable Portal Authentication

Settings

Status: Enable

Idle Timeout: 30 minutes (0 or 5-1440, 0 means always online)

Portal Authentication Port: 8080 (8080, 1024-65535)

- 2) Choose the Authentication Page as **Custom page**, pick a picture of the hotel as the background picture on the authentication page, and specify the welcome information and copyright.

Figure 7-3 Customize the authentication page

Authentication Parameters

Authentication Page: Custom Page

Background Picture: Upload --- (The image size cannot exceed 200KB.)

Welcome Information: Welcome to xxx hotel! (1-50 characters)

Copyright: Copyright©2017 (1-50 characters)

Page Preview: Login Page Preview

- 3) Choose the Authentication Type as **Local Authentication**, and configure the parameters of expiration reminder. Then click **Save**.

Figure 7-4 Configure the authentication type and expiration reminder

Authentication Type: (dropdown)

Expiration Reminder: Enable

Time to Remind: days (1-10)

Remind Type: (dropdown)

Remind Content: (1-50 characters)

Page Preview:

7.3.2 Configuring Authentication Accounts for the Guests

Choose the menu **Authentication > User Management > User Management** to load the following page.

Here we take the configuration of Formal User account as an example. We create an account for the guests of room 101. The username is Room101 and the password is 123456, and at most three guests can use this account to authenticate. Then click **OK**.

Figure 7-5 Configure the Account for the guests

<input type="checkbox"/>	ID	User Type	Username	Authentication Timeout	MAC Address	Description	Status	Operation
--	--	--	--	--	--	--	--	--

User Type: (dropdown)

Username: (1-100 Characters)

Password: (1-100 Characters)

Expiration Date: (YYYY-MM-DD)

Authentication Period: (HH:MM-HH:MM)

MAC Binding Type: (dropdown)

Maximum Users: (1-1024)

Upstream Bandwidth: Kbps (0 or 10-1,000,000. 0 means no limit)

Downstream Bandwidth: Kbps (0 or 10-1,000,000. 0 means no limit)

Name: (1-50 characters, optional)

Telephone: (1-50 characters, optional)

Description: (1-50 characters, optional)

Status: Enable

After all the configuration finished, the guest can use the account to authenticate and access the internet after the authentication succeeded.