# Operating Manual

## (Software Release 8.7)

## for Gateways

**Email: support@radiusgateway.com**

**Phone: 877-298-4103 (North America)**
**or +1-419-879-3224 (international)**

# TABLE OF CONTENTS

Chapter 1: Radius Gateway Quick Config ..... 6
Tools Needed ..... 6
Connecting to the Gateway for Configuration ..... 6
Setting up the Internet Connection ..... 7
Static IP Address ..... 8
DHCP Address ..... 8
PPPoE Configuration ..... 9
Typical Guest Network Configuration ..... 10
Guest Network Authentication ..... 11
Chapter 2: Web Interface Administration ..... 14
System Menu ..... 14
Change Password (System → Change Password) ..... 14
Gateway Admin Users (System → Gateway Admin Users) ..... 14
E-Mail Settings (System→E-Mail Settings) ..... 14
Clock (System → Clock) ..... 14
Identity & Location (System → Identity & Location) ..... 14
Resources (System → Resources) ..... 14
Syslog (System → Syslog) ..... 15
Logging Rules (System → Logging Rules) ..... 15
Remote Syslog Settings (System → Remote Syslog Settings) ..... 15
Backup/Restore (System → Backup/Restore) ..... 15
Reboot (System → Reboot) ..... 15
Reset Configuration (System → Reset Configuration) ..... 15
ISP Menu ..... 16
Configuration (ISP → Configuration) ..... 16
DNS (ISP → DNS) ..... 23
DynDNS (ISP → DynDNS) ..... 23

Copyright © 2021 Radius Gateway LLC. All rights reserved.

Guest Network Menu ..... 25
Active Users (Guest Network → Active Users) ..... 26
Devices (Guest Network → Devices) ..... 31
Authentication (Guest Network → Authentication) ..... 33
Connection Limiting (Guest Network → Connection Limiting) ..... 43
DHCP Leases (Guest Network → DHCP Leases) ..... 44
DHCP Server (Guest Network → DHCP Server) ..... 44
IP Addresses (Guest Network → IP Address) ..... 45
P2P File Sharing (Guest Network → P2P File Sharing) ..... 46
Pay Access Plans (Guest Network → Pay Access Plans) ..... 47
RADIUS Client (Guest Network → RADIUS Client) ..... 49
SMTP Redirect (Guest Network → SMTP Redirect) ..... 50
Public IPs (Guest Network → VPN IP Pool) ..... 52
VPN Mappings (Guest Network → VPN Mappings) ..... 54
Walled Garden (Guest Network → Walled Garden) ..... 56
Guest Login Templates ..... 58
HTML ..... 58
Images ..... 59
Login Page Logo (Guest Network → Login Page Logo) ..... 59
Terms of Service (Guest Network → Terms of Service) ..... 60
PMS Menu ..... 61
PMS Interface Configuration (PMS → Configuration) ..... 61
PMS Status (PMS → Status) ..... 62
PMS Log (PMS → Log) ..... 63
RADIUS Server Menu ..... 64
Browse Users (Radius Server → Browse Users) ..... 64
Search Users (RADIUS Server → Search Users) ..... 71
Delete Old Users (RADIUS Server → Delete Old Users) ..... 71
RADIUS User Profiles (RADIUS Server → RADIUS User Profiles) ..... 71

Copyright © 2021 Radius Gateway LLC. All rights reserved.

Tools Menu ..... 73
Ping (Tools → Ping) ..... 73
IP Scan (Tools → IP Scan) ..... 73
Netwatch (Tools → Netwatch) ..... 74
Advanced Menu ..... 75
Back Office Network (Advanced → Back Office Network) ..... 75
DNS Cache (Advanced → DNS Cache) ..... 76
Firewall Filter (Advanced → Firewall Filter) ..... 77
Guest Network VLAN Mode (Advanced → Guest Net VLAN Mode) ..... 78
Add Guest Network VLANs from CSV file ..... 80
Guest 2 Guest (Advanced → Guest 2 Guest) ..... 81
Destination NAT (Advanced → NAT (DST-NAT)) ..... 81
Source NAT (Advanced → NAT (SRC-NAT)) ..... 83
Firewall Netmap (Advanced → NAT (Netmap)) ..... 84
Interface List (Advanced → Interface List) ..... 85
IP Addresses (Advanced → IP Addresses) ..... 85
Management ACL (Access Control List) (Advanced → Management ACL) ..... 86
Management Ports (Advanced → Management Ports) ..... 86
PPTP Clients (Advanced → PPTP Clients) ..... 87
Remote Query IPs (Advanced → Remote Query IPs) ..... 88
SNMP (Advanced → SNMP) ..... 88
Static DNS (Advanced → Static DNS) ..... 89
Static Routes (Advanced → Static Routes) ..... 89
Chapter 3: Troubleshooting ..... 90
Appendix A: Supported RADIUS Attributes ..... 91
Access-Request ..... 91
Access-Accept ..... 91
Accounting-Request ..... 92
Stop and Interim-Update Accounting-Request ..... 92

Copyright © 2021 Radius Gateway LLC. All rights reserved.

Stop Accounting-Request ..... 92
Appendix B: API ..... 93
PMS query/post ..... 93
Internal User Database Management ..... 95
Appendix C: IPv4 Subnet Mask to CIDR Network Number Conversion ..... 98
Appendix D: Guest Network Login Page Screenshots ..... 99
Standard Accept Button ..... 99
Standard Login Page ..... 100
PayPal Login Page ..... 101
Weekly Code ..... 103

Copyright © 2021 Radius Gateway LLC. All rights reserved.

# CHAPTER 1: RADIUS GATEWAY QUICK CONFIG

## *Tools Needed*

The following items will be needed for initial gateway configuration:

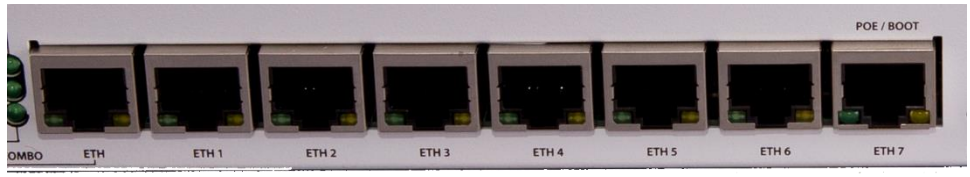
- Desktop or laptop computer with a network card and web browser with JavaScript enabled. The computer must be configured for DHCP network configuration.
- Two (2) Ethernet network cables (CAT5e or CAT6).

## *Connecting to the Gateway for Configuration*

The physical connections to be made for initial configuration are:

- Using one of the network cables, connect the ISP modem or router to the port of the gateway as follows:
    - For the RG-651h, connect ISP to ETH1.
    - For the RG-701h, connect ISP to ETH (to the left of ETH1). If ETH1 is connected to the ISP, then the ISP will not work as expected.
- Using the other network cable, connect the computer to port ETH3 of the gateway.

**RG-651h Gateway**




**RG-701h Gateway**

**NOTE:** All Ethernet ports on the gateway support automatic MDI/MDI-X crossover detection. Thus, there is no need to be concerned about crossover or straight-through network cables when making network connections.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

- To log on to the administration configuration panel, open a web browser and go to location http://10.255.255.254
- The default username is *admin*. The default password is *admin*.

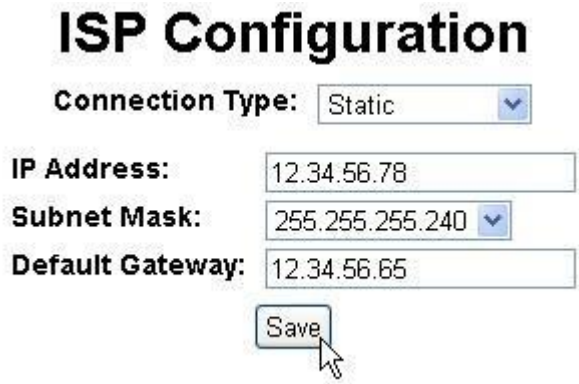
## *Setting up the Internet Connection*

There are several methods available for connecting the gateway to the Internet. These are configured through the **ISP → Configuration** screen.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Static IP Address**

When the selected connection type is “Static” the IP address, subnet mask, and default gateway can be defined. Set the static IP parameters and click the **Save** button.




**DHCP Address**

When the selected connection type is “DHCP Client” simply click the **Save** button to put the gateway into DHCP client mode. The default connection type is DHCP Client. When the gateway is plugged into the ISP modem, it will attempt to obtain an IP address via DHCP request.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**PPPoE Configuration**

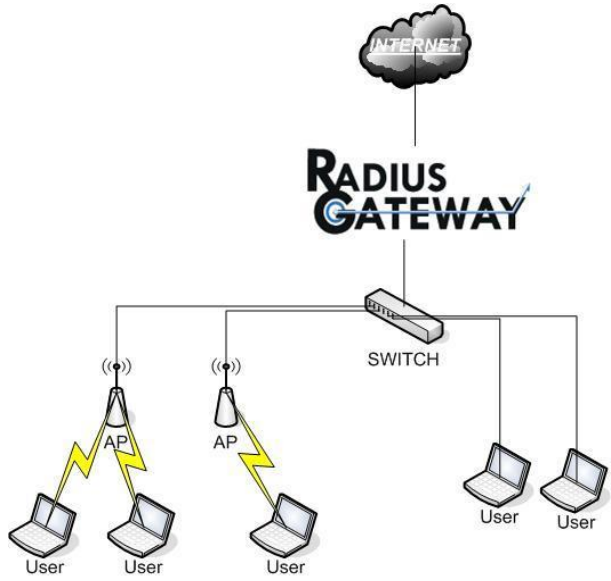
When the selected connection type is “PPPoE Client” enter the username and password assigned by the ISP. Click **Save** to apply the changes. When the gateway is plugged into the modem, it will attempt to connect to the ISP via the PPPoE protocol.

**NOTE:** The ISP modem must be in bridge mode in order for PPPoE requests to be properly sent to the ISP. Typically, the ISP must place the modem into bridge mode and the ISP should be contacted if difficulty is encountered.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

### *Typical Guest Network Configuration*

Typically, the best guest network configuration is a network composed of a single subnet without any other routers on the guest network. The guest network should be composed of a single subnet, because authentication is done on a MAC address and IP address basis.

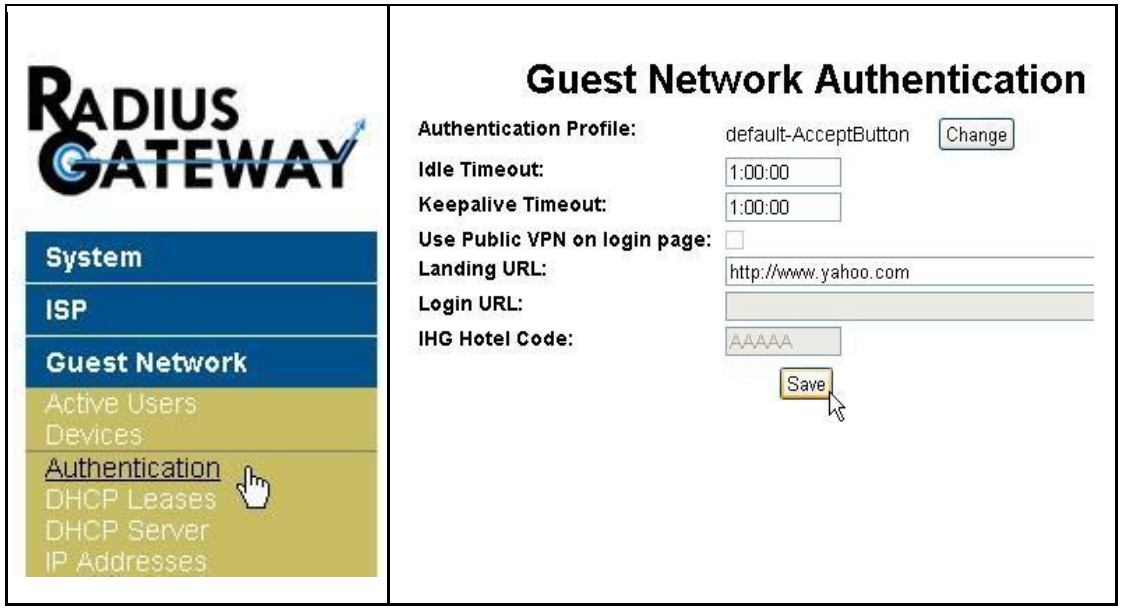



**IMPORTANT NOTE:** If the guest network is not composed of a single subnet, authentication will yield unexpected results.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

### *Guest Network Authentication*

Guest network authentication is configured through the **Guest Network → Authentication** screen. By default, authentication is disabled.




The Guest Network Authentication screen enables the necessary fields depending on which authentication profile is selected. The fields are described below. To save the desired guest network authentication method, click the **Save** button.

- **Authentication Profile:** Determines how users authenticate and gain Internet access.
- **Idle Timeout:** Determines how long the gateway will hold onto a MAC address if it is not transmitting or receiving. When this timeout is reached, the user will be logged out by the gateway automatically.
- **Keepalive Timeout:** Determines how long the gateway will hold onto a MAC address if it is not seen on the network at all (e.g., if a user shuts down his or her computer). When this timeout is reached, the user will be logged out automatically.
- **Use Public VPN on login page:** Some VPN clients require a public IP address to function properly. When VPN mappings are properly enabled and configured, this checkbox controls the display of a field for a user to check if a public IP address is required for VPN access. During initial configuration, this button is disabled.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

- **Landing URL:** If the selected Profile involves a landing URL, this field will be enabled. After a user is logged in, he or she will be redirected to this URL as their landing page. If this field is left blank, the landing URL will be the URL originally requested by the user (typically the user's home page).
- **Login URL:** If the selected Profile involves a login URL, this field will be enabled. The user is redirected to this URL as part of the login process.
- **Hotel Code:** If the selected Profile requires a Holiday Inn or Holiday Inn Express eHost page, this field will be enabled. The hotel code is entered in this field which is used to determine the eHost landing page.

To change the desired authentication method, click the **Change** button from the Guest Network Authentication screen.

The Radius Gateway has several different possibilities for guest authentication. After selecting the desired method, click the **Save** button.

- **DISABLED —** This setting allows guests to connect to the Internet without being authenticated. By default, authentication is disabled. When authentication is disabled, a default bandwidth per user may be set on the **Guest Network→Authentication** screen.
- **PMS** — If PMS modules have been purchased and enabled, the PMS authentication method uses PMS connectivity to verify and/or charge users for network access against the PMS database.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

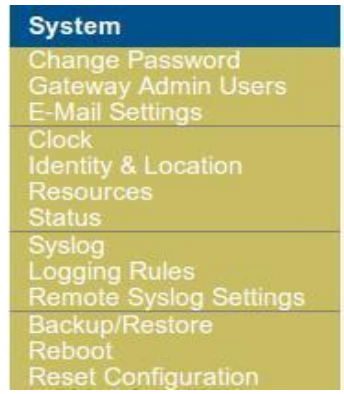
- **PMS Free** — If PMS modules have been purchased and enabled, the PMS Free method uses PMS connectivity to verify users for network access against the PMS database. Unlike the PMS profile, this profile does not require users to create their own accounts. It only verifies room number and last name.
- **PayPal** — If paid user accounts are desired, the PayPal authentication method may be selected.
- **RADIUS-external** — This setting works in conjunction with the RADIUS settings to perform external RADIUS authentication along with displaying an external login page.
- **Weekly Code** — This authentication method sets up a code that rotates weekly on a given day and time. Users must enter the correct access code to gain Internet access.
- **Default-AcceptButton** — This setting performs internal authentication. It presents a basic "terms of service" page. The logo and terms of service items are configurable in the **Guest Network → Login Page Logo** and **Guest Network → Terms of Service** screens respectively. When the guest clicks the **Agree** button, he or she is logged in and redirected to a landing page.
- **Default-Login** — This setting performs internal authentication. It presents a basic terms of service page along with a login form. Usernames and passwords are stored and authenticated locally on the gateway. The logo and terms of service items are configurable in the **Guest Login Templates → Login Page Logo** and **Guest Login Templates → Terms of Service** screens respectively. Usernames and passwords are configurable in the RADIUS Server menu.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

# CHAPTER 2: WEB INTERFACE ADMINISTRATION

## *System Menu*

The system menu controls the system-wide features of the gateway.




**Change Password (System → Change Password)**

This link allows the currently logged-in administrative user to change his or her password.

**Gateway Admin Users (System → Gateway Admin Users)**

This link allows management of available gateway administrative users. By default, the admin user is the only user available, but other admin and limited users may be added through this screen.

**E-Mail Settings (System→E-Mail Settings)**

This link allows the configuration of outgoing SMTP e-mail server settings for the weekly access code e-mail feature. These settings are required for the weekly access code e-mail feature to work properly.

**Clock (System → Clock)**

This link sets the internal clock of the gateway. The time zone and active NTP servers can also be defined.

**Identity & Location (System → Identity & Location)**

This link allows internal identification variables to be set. This is useful to keep track of gateway identity and location information if many gateways are deployed in diverse locations.

**Resources (System → Resources)**

This link shows run-time information of the gateway including up time, CPU load, and

Copyright © 2021 Radius Gateway LLC. All rights reserved.

hard drive space.

**Syslog (System → Syslog)**

This menu displays the currently available internal syslog.

**Logging Rules (System → Logging Rules)**

This link defines where and how syslog messages should be handled. By default, messages stored to disk will have the file name of "log". To store messages on a remote syslog server, configure the IP address and UDP port of the server in the **System → Logging Actions** screen.

**Remote Syslog Settings (System → Remote Syslog Settings)**

This link defines the remote syslog settings.

**Backup/Restore (System → Backup/Restore)**

This link allows for backup and restore functionality. Restore actions can be performed between different gateways of the same model. Restore will fail if the model numbers are different.

**Reboot (System → Reboot)**

This menu item reboots the gateway.

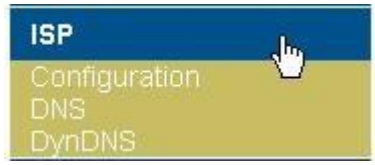
**Reset Configuration (System → Reset Configuration)**

This feature resets the gateway to factory defaults.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

## *ISP Menu*

The ISP menu controls how the gateway connects to the Internet.



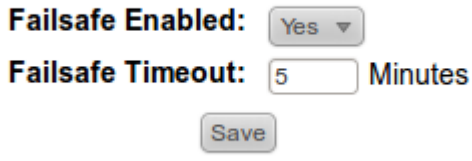

### Configuration (ISP → Configuration)

Several methods are available to connect the gateway to the Internet. These are configured through the **ISP → Configuration** screen.

- Static IP Address
- DHCP Address
- PPPoE
- Failover
- Load Balance

#### ISP Configuration Failsafe

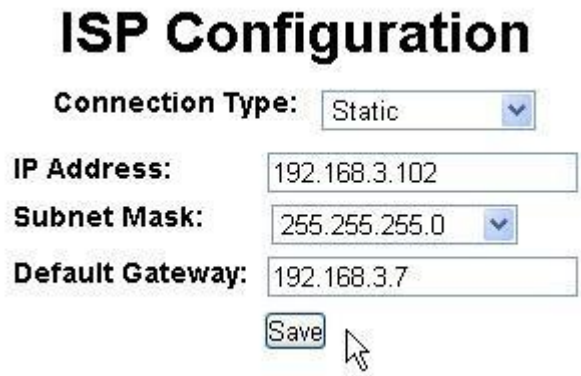
A failsafe feature is also available. This feature is very useful when making remote ISP configuration changes. By default, the failsafe feature is enabled. When failsafe is enabled, the gateway will reboot after the configuration changes are applied. Once ISP changes are applied and the gateway reboots, the administration web page must be logged into within the time specified in the Failsafe Timeout field. If the administration web page is not logged into within the specified amount of time, the gateway will reboot again and restore the previous ISP configuration.




Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Static IP Address**

When the connection type is set to “Static” the IP address, subnet mask and default gateway can be defined. Set the static IP parameters and click the **Save** button.




**NOTE:** The 651h ISP port is ETH1 (for ethernet) or SFP (for fiber connections). The gateway cannot handle both of these ports being connected at the same time.

**NOTE:** The 701h ISP port is ETH (for ethernet) or SFP (for fiber connections). The gateway cannot handle both of these ports being connected at the same time.

**DHCP Address**

When the connection type is set to “DHCP Client” simply click the **Save** button to put the gateway into DHCP client mode. When the gateway is plugged into the modem, it will attempt to obtain an IP address via DHCP request.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**PPPoE**

When the connection type is set to “PPPoE Client” enter the username and password assigned by the ISP. Click **Save** to apply the changes. When the gateway is plugged into the modem, it will attempt to connect to the PPPoE server at the ISP and obtain an IP address.

**NOTE:** The ISP modem must be in bridge mode in order for PPPoE requests to be sent properly to the ISP.

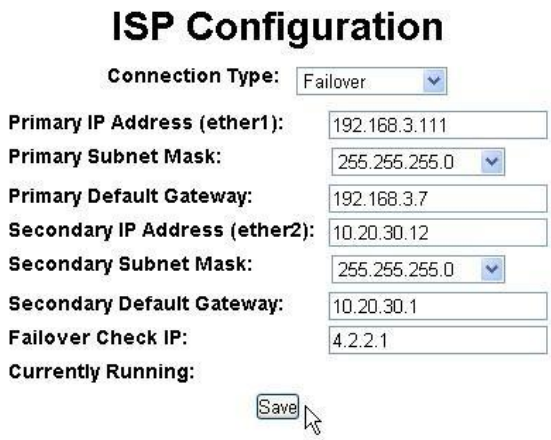
Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Failover**

Failover configuration allows the gateway to fail over from a primary ISP connection to a secondary ISP connection if or when the connection to the primary ISP is lost. Failover configuration mode on the Radius Gateway requires a static IP address configuration on both ISP connections.

**NOTE:** The 651h interfaces are: Primary-ETH1, Secondary-ETH2.

**NOTE:** The 701h interfaces are: Primary-ETH or SFP, Secondary-ETH1 or SFP+.




The method that Radius Gateway uses to determine the state of the primary ISP connection is to ping a specific IP address through the primary ISP port. This IP address is referred to as the "Failover Check IP." The "Failover Check IP" is always checked through the ether1 interface regardless of the currently running connection.

The best IP address to use is one that most users will not be visiting. This is usually an upstream router. If a traceroute is done from the primary ISP connection to a site like google.com, a response would come back similar to the following:

```
Tracing route to google.com [74.125.127.100]
over a maximum of 30 hops:

 1   <1 ms   <1 ms   <1 ms  192.168.3.7
 2    *       *       *     Request timed out.
 3    9 ms    9 ms    9 ms  te-2-1-ur01.valparaiso.in.chicago.comcast.net [68.86.119.29]
```

Copyright © 2021 Radius Gateway LLC. All rights reserved.

```
4   10 ms   21 ms    9 ms  te-8-3-ur02.valparaiso.in.chicago.comcast.net [68.87.230.162]
5    9 ms   11 ms    9 ms  te-8-1-ur02.hammond.in.chicago.comcast.net [68.87.230.157]
6   12 ms   13 ms   12 ms  be-80-ar01.area4.il.chicago.comcast.net [68.87.230.153]
7   12 ms   11 ms   11 ms  pos-1-14-0-0-cr01.chicago.il.ibone.comcast.net [68.86.90.45]
8   12 ms   11 ms   11 ms  xe-10-1-0.edge1.chicago2.level3.net [4.71.248.17]
...
```

In this situation, a good Failover Check IP is 4.71.248.17. This IP address is a core router at a centralized NOC. If this is not desired, the IP address can be set to whatever IP address is desired.

**IMPORTANT NOTE:** When in failover mode, take care only to set up public IP addresses in the **Guest Network → VPN Mappings** with public IP addresses available on the *primary* ISP connection. If IP addresses are mapped to public IP addresses on the secondary connection, they will not map correctly.

**IMPORTANT NOTE:** When in failover mode, verify that the Failover Check IP is **NOT** the same as any defined DNS servers. The secondary connection will not be able to do DNS lookups if the Failover Check IP is the same as a DNS server setting, thus rendering failover useless.

**Load Balance**

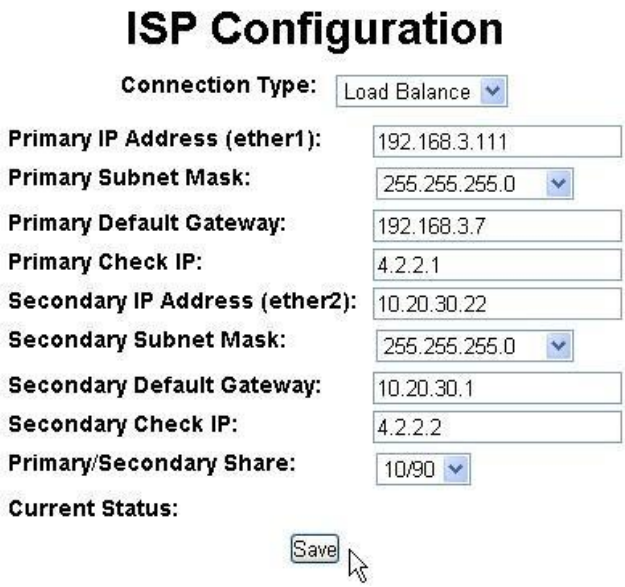
Load Balance configuration allows the gateway to share two Internet connections at a pre-defined ratio. This sharing allows the usage of two Internet connections at different speeds as well. For example, if a T1 is used as a primary connection and a 10mbps cable connection is used as a secondary connection, the ratio may be set to 10/90, thus moving more load balanced traffic through the cable connection than the T1 connection.

Load Balance configuration mode on the Radius Gateway requires a static IP address configuration on both ISP connections. The primary ISP connection is to be configured for ether1 and the secondary ISP is to be configured for ether2. Ports ether3 and above serve the guest network. Load Balance configuration requires primary and secondary connections because each connection is monitored separately for online status. If the primary connection is unavailable, the secondary connection takes over and vice versa. The method that Radius Gateway uses to determine the state of the primary and secondary ISP connections is the same as described above in the Failover section.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**NOTE:** The 651h interfaces are: Primary-ETH1, Secondary-ETH2

**NOTE:** The 701h interfaces are: Primary-ETH or SFP, Secondary-ETH1 or SFP+.




**IMPORTANT NOTE:** When in Load Balance mode and doing guest network VPN mappings, take care to set up only public IP addresses available on the *primary ISP* connection. If IP addresses are mapped to public IP addresses on the secondary connection, they will not map correctly.

**IMPORTANT NOTE:** Load balancing is only done on outgoing HTTP, POP3, and SMTP connections. This is due to the requirements of some protocols that require all connections come from the same source IP address.

**IMPORTANT NOTE:** When in load balance mode, verify that the Primary and Secondary Check IPs are **NOT** the same as any defined DNS servers. If either connection is disconnected, there will be problems performing DNS lookups, potentially breaking the built-in failover functions and end-user connectivity.

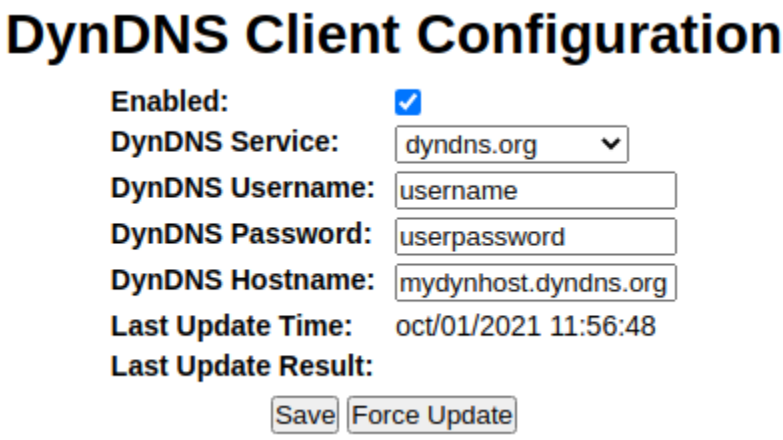
Copyright © 2021 Radius Gateway LLC. All rights reserved.

**DNS (ISP → DNS)**

This screen controls the primary and secondary DNS server settings for the Internet connection. DNS servers are only configurable when the ISP configuration is Static IP or Failover.

**DynDNS (ISP → DynDNS)**

When a gateway is on a DHCP address or PPPoE connection, remote management can be difficult due to changing IP addresses. Radius Gateway integrates with several widely used dynamic DNS providers including dyndns.org, changeip.com, dnsdynamic.com, he.net, and noip.com. These providers dynamically update a DNS entry if and when your gateway IP's public address changes.




To configure DynDNS:

1. If needed, select your preferred Dynamic DNS service from the above list.
2. When the Dynamic DNS account and host are completely set up with service, enable the DynDNS checkbox on the Radius Gateway.
3. On the Radius Gateway, enter your username, password, and host information.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

4. Click **Save**.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**NOTE:** DynDNS updates occur once every 15 minutes. Updates may take up to 15 minutes before they are reflected on the DynDNS account. During regular updates, the gateway first checks to see if an update is necessary. If so, it will update the DynDNS hostname. If an update is not necessary, it will simply do nothing. Also, once every 24 hours, a forced DynDNS update is performed. The forced update updates the DynDNS account regardless of whether or not the IP address has changed. This keeps the DynDNS account active while not over-updating, which may cause a lockout of the DynDNS account.

**IMPORTANT NOTE:** If a forced update is desired, click the **Force Update** button. Care must be taken to not perform a forced update too often, as it may result in the dyndns.org account being locked out.

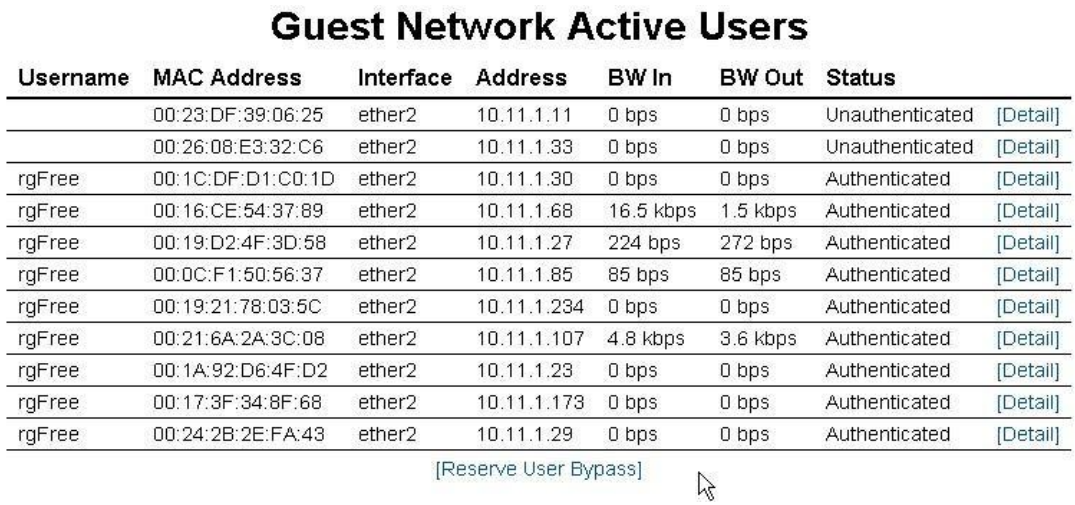
### *Guest Network Menu*

The Guest Network menu controls how the guest network is configured.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Active Users (Guest Network → Active Users)**

This link shows and allows control of guest network users currently on the guest network ports. It displays the authenticated and unauthenticated users currently on the guest network.



**Guest Network Active Users**

| Username | MAC Address | Interface | Address | BW In | BW Out | Status | |
|---|---|---|---|---|---|---|---|
| | 00:23:DF:39:06:25 | ether2 | 10.11.1.11 | 0 bps | 0 bps | Unauthenticated | [Detail] |
| | 00:26:08:E3:32:C6 | ether2 | 10.11.1.33 | 0 bps | 0 bps | Unauthenticated | [Detail] |
| rgFree | 00:1C:DF:D1:C0:1D | ether2 | 10.11.1.30 | 0 bps | 0 bps | Authenticated | [Detail] |
| rgFree | 00:16:CE:54:37:89 | ether2 | 10.11.1.68 | 16.5 kbps | 1.5 kbps | Authenticated | [Detail] |
| rgFree | 00:19:D2:4F:3D:58 | ether2 | 10.11.1.27 | 224 bps | 272 bps | Authenticated | [Detail] |
| rgFree | 00:0C:F1:50:56:37 | ether2 | 10.11.1.85 | 85 bps | 85 bps | Authenticated | [Detail] |
| rgFree | 00:19:21:78:03:5C | ether2 | 10.11.1.234 | 0 bps | 0 bps | Authenticated | [Detail] |
| rgFree | 00:21:6A:2A:3C:08 | ether2 | 10.11.1.107 | 4.8 kbps | 3.6 kbps | Authenticated | [Detail] |
| rgFree | 00:1A:92:D6:4F:D2 | ether2 | 10.11.1.23 | 0 bps | 0 bps | Authenticated | [Detail] |
| rgFree | 00:17:3F:34:8F:68 | ether2 | 10.11.1.173 | 0 bps | 0 bps | Authenticated | [Detail] |
| rgFree | 00:24:2B:2E:FA:43 | ether2 | 10.11.1.29 | 0 bps | 0 bps | Authenticated | [Detail] |

[Reserve User Bypass]

There are several fields displayed in the initial window:

- **Username —** The name field displays the username. If the user has not used the normal authentication means to log on, this field will remain blank.
- **MAC Address** — MAC Address of the user or equipment.
- **Interface** — Interface on which the user is accessing the network.
- **Address —** IP address assigned on the user's computer.
- **BW In / BW Out** — Bandwidth currently being used by the user. This is automatically updated every 10 seconds.
- **Status** — Current status of the user.

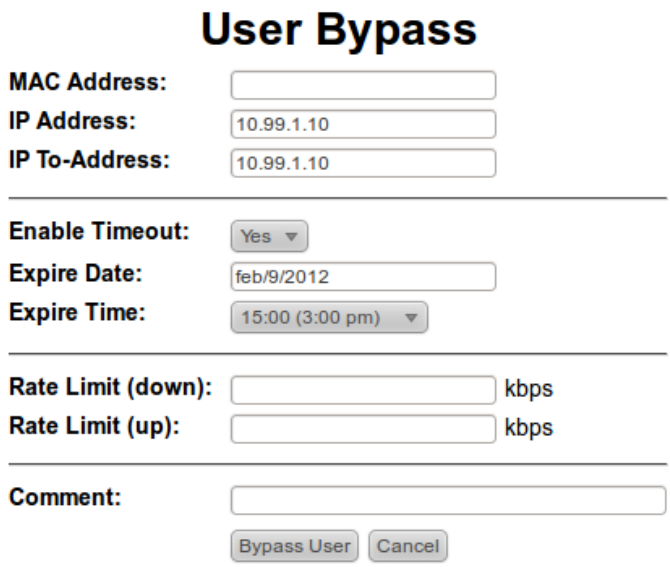
**NOTE:** If authentication is disabled, this list will be empty.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Bypass a user that is not currently on the guest network**

If a user is not visible on the Active Users screen, the **Reserve User Bypass** link at the bottom of the Active Users screen may be clicked to reserve a user bypass manually in advance. The MAC address of the computer is required and will not be filled in automatically by the gateway. This feature is useful to schedule users ahead of time before being seen on the guest network.

An example would be a conference room at a hotel. If a conference attendee has special equipment or bandwidth requirements, this screen may be used to provision resources ahead of time. When the attendee starts up his or her equipment, it will already be bypassed with the needed rate limits.




The new user is assumed to be using DHCP network configuration. On the user bypass screen, the gateway will automatically choose an IP address that the user will receive when they connect to the network. Once defined, the gateway reserves this IP address for the user. The User Bypass screen fields are described in more detail below in the section titled "Bypass a user that is currently on the guest network."

Copyright © 2021 Radius Gateway LLC. All rights reserved.

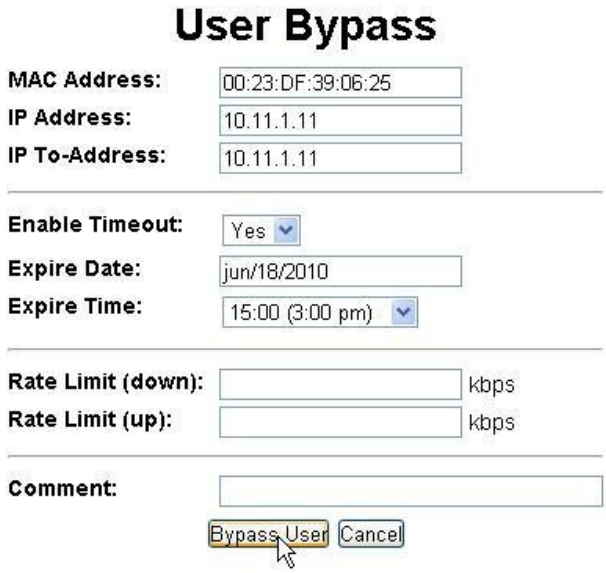
**Detail View**

To view the detail of a user currently visible on the guest network, click the **Detail** link on the desired row. From this screen, it is possible to bypass users or equipment as well as to block users.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Bypass a user that is currently on the guest network**

To manually bypass a user, click the **Bypass as User** button from the user detail screen. This will open the User Bypass screen.




This screen contains fields to enable timeout and rate limiting of the user.

The "IP address" field is the IP address configured on the user's computer. If this address is not within the scope of the guest network, it is internally translated to an IP that is within the scope of the guest network via the "IP To-Address" field. These fields are filled in automatically by the gateway but may be changed if needed.

By default, the timeout is set to 24 hours from the current gateway time. If the timeout is not enabled, the user will be permanently bypassed and will need to be manually deleted. If the timeout is set, the user will be automatically deleted at the set time.

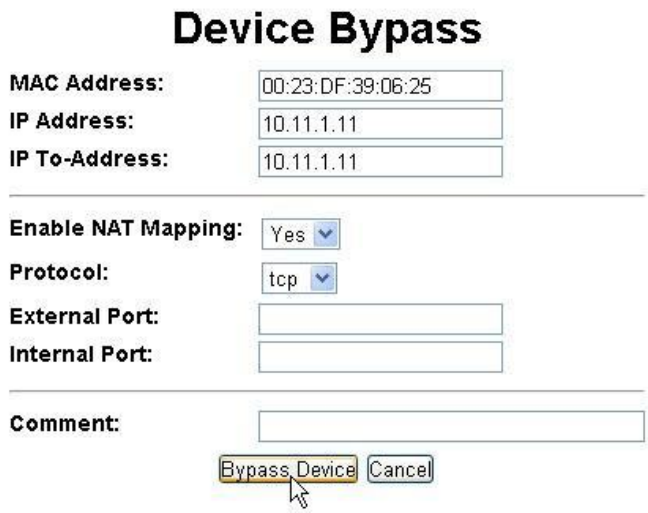
The rate limit fields are blank by default. If these fields are left blank, the rate limit will not be set. It is highly recommended that the rate limits be set under normal circumstances to prevent a single user from hogging the entire bandwidth of the Internet connection.

To save the user bypass, click the **Bypass User** button.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Device Bypass**

Equipment can also be bypassed in a similar manner. To bypass equipment with an automatic external to internal NAT port mapping, click the **Bypass as Device** button from the user detail screen. This will open the Device Bypass screen.




This screen bypasses a MAC/IP address as a device.

It is also possible to define an external port map to the device from this screen. If this is desired, set the "Enable NAT Mapping" field to "Yes" and set the external port and internal port in the form.

**IMPORTANT DEVICE CONFIGURATION:** It is VERY important to set the default gateway IP address on internal guest network devices be configured to an address that is assigned to the guest network interface of the gateway (**Guest Network → IP Addresses**). Devices will not be manageable remotely if devices do not have a default gateway properly configured.

**NOTE:** It is highly recommended that the equipment residing on the guest network belong to a different subnet than the guests themselves. Make sure to configure this subnet in the **Guest Network → IP Address** window if desired.

**NOTE:** This dialog only maps a single port from external to internal. To map multiple ports, **Advanced → NAT (DST-NAT)** may be used.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Devices (Guest Network → Devices)**

This screen displays and configures guest network devices.

## Guest Network Devices

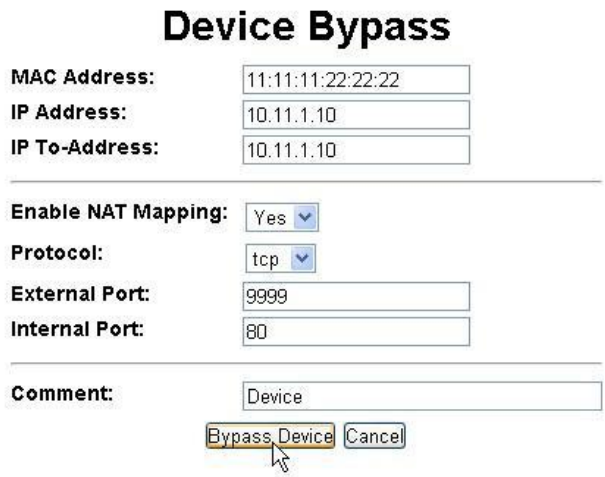
| MAC Address | Interface | Address | Status | Comment | |
|---|---|---|---|---|---|
| 00:20:A6:C9:20:48 | ether2 | 10.17.5.235 | up | AP 235 | [Detail] |
| 00:20:A6:C9:20:37 | ether2 | 10.17.5.236 | up | AP 236 | [Detail] |
| 00:20:A6:C3:98:62 | ether2 | 10.17.5.237 | up | AP 237 | [Detail] |
| 00:20:A6:C3:E7:07 | ether2 | 10.17.5.238 | up | AP 238 | [Detail] |
| 00:20:A6:C9:20:CF | | 10.17.5.239 | down | AP 239 | [Detail] |
| 00:20:A6:C3:D6:37 | ether2 | 10.17.5.240 | up | AP 240 | [Detail] |
| 00:20:A6:C8:54:4D | ether2 | 10.17.5.241 | up | AP 241 | [Detail] |
| 00:20:A6:C8:55:5B | ether2 | 10.17.5.242 | up | AP 242 | [Detail] |
| 00:20:A6:C3:E5:F7 | ether2 | 10.17.5.243 | up | AP 243 | [Detail] |
| 00:20:A6:C8:E1:5A | ether2 | 10.17.5.244 | up | AP 244 | [Detail] |
| 00:20:A6:C8:51:A6 | ether2 | 10.17.5.245 | up | AP 245 | [Detail] |
| 00:20:A6:C9:20:BE | ether2 | 10.17.5.246 | up | AP 246 | [Detail] |
| 00:20:A6:C9:1F:05 | ether2 | 10.17.5.247 | up | AP 247 | [Detail] |
| 00:20:A6:C8:6C:5E | ether2 | 10.17.5.248 | up | AP 248 | [Detail] |
| 00:20:A6:C8:6C:6F | ether2 | 10.17.5.249 | up | AP 249 | [Detail] |
| 00:20:A6:C9:21:35 | ether2 | 10.17.5.250 | up | AP 250 | [Detail] |
| 00:20:A6:C8:E1:AD | ether2 | 10.17.5.251 | up | AP 251 | [Detail] |
| 00:20:A6:C8:56:47 | ether2 | 10.17.5.252 | up | AP 252 | [Detail] |
| 00:20:A6:C8:55:4A | ether2 | 10.17.5.253 | up | AP 253 | [Detail] |
| 00:20:A6:C5:68:8E | ether2 | 10.17.5.254 | up | AP 254 | [Detail] |

[Reserve Device Bypass]

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Reserve Device Bypass**

To add a new device that is not visible from the Active Users screen, click the **Reserve Device Bypass** link at the bottom of the Devices screen. The settings are the same as when equipment is added in the **Guest Network → Active Users** screen. For more detail on these settings, please see the "Device Bypass" section in the Active Users (**Guest Network → Active Users**) section of this document.




Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Authentication (Guest Network → Authentication)**

This screen defines how users on the guest network are authenticated. The Radius Gateway device has many different profiles available for guest authentication.

- **DISABLED —** This setting allows guests to connect to the Internet without being authenticated. By default, authentication is disabled. When authentication is disabled, a default bandwidth per user may be set on the **Guest Network→Authentication** screen.
- **PMS** — If PMS modules have been purchased and enabled, the PMS authentication method uses PMS connectivity to verify and/or charge users for network access against the PMS System.
- **PMS Free** — If PMS modules have been purchased and enabled, the PMS Free method uses PMS connectivity to verify users for network access against the PMS System. Unlike the PMS profile, this profile does not require users to create their own accounts. It only verifies room number and last name.
- **PayPal** — If paid user accounts are desired, the PayPal authentication method may be selected.
- **RADIUS-external —** This setting works in conjunction with the RADIUS settings to perform external RADIUS authentication along with displaying an external login page.
- **Weekly Code** — This authentication method sets up a code that rotates weekly on a given day and time. Users must enter the correct access code to gain Internet access.
- **Default-AcceptButton** — This setting performs internal authentication. It presents a basic "terms of service" page. The logo and terms of service items are configurable in the **Guest Network → Login Page Logo** and **Guest Network → Terms of Service** screens respectively. When the guest clicks the **Agree** button, he or she is logged in and redirected to a landing page.
- **Default-Login** — This setting performs internal authentication. It presents a basic terms of service page along with a login form. Usernames and passwords are stored and authenticated locally on the gateway. The logo and terms of service items are configurable in the **Guest Network → Login Page Logo** and **Guest Network → Terms of Service** screens respectively. Usernames and passwords are configurable in the RADIUS Server menu.

**IMPORTANT NOTE:** The guest network should be composed of a single subnet, because authentication is performed on a MAC address basis. If the guest network is not composed of a single subnet, authentication will yield unexpected results. See the network diagram in Chapter 1 for more information.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

The Guest Network Authentication screen displays and enables the necessary fields depending on which authentication profile is selected. The login method configurations are described in the following sections.

**Set Authentication Mode**

To change the authentication mode, click the **Change** button in the Guest Network Authentication screen. Some authentication methods are also capable of a preview. When applicable, to view a preview of the chosen authentication profile, click the **Preview** button.

**Common Authentication Configuration Fields**

Most guest authentication methods have common fields that are definable. These include:

- **Idle Timeout:** Determines how long the gateway will hold onto a MAC address if it is not transmitting or receiving. When this timeout is reached, the user will be logged out by the gateway automatically.
- **Keepalive Timeout:** Determines how long the gateway will hold onto a MAC address if it is not seen on the network at all (e.g., a user shuts down his or her computer). When this timeout is reached, the user will be logged out.
- **Use Public VPN on login page:** If public VPN mappings are defined and the selected authentication method is able to display a checkbox automatically on the login page for a user to choose a VPN IP, this field will be displayed. Currently, this check box is supported in Holiday Inn, Holiday Inn Express, Weekly Code, and Default-AcceptButton login methods. More information about guest network VPN IP mappings may be found in the **Guest Network→VPN IP Pool** and **Guest Network→VPN Mappings** sections of this document.
- **Landing URL:** If the selected Profile involves a landing URL, this field will be visible. After a user is logged in, he or she will be redirected to this URL as their landing page. If this field is left blank, the landing URL will be the URL originally requested by the user (typically the user's home page).

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Authentication Disabled**

When authentication is disabled, a bandwidth cap may be enforced for each user on the guest network. To enable bandwidth cap, click the "Enable bandwidth cap per user" check box and enter the desired bandwidth limitations. Then, click the **Save** button.

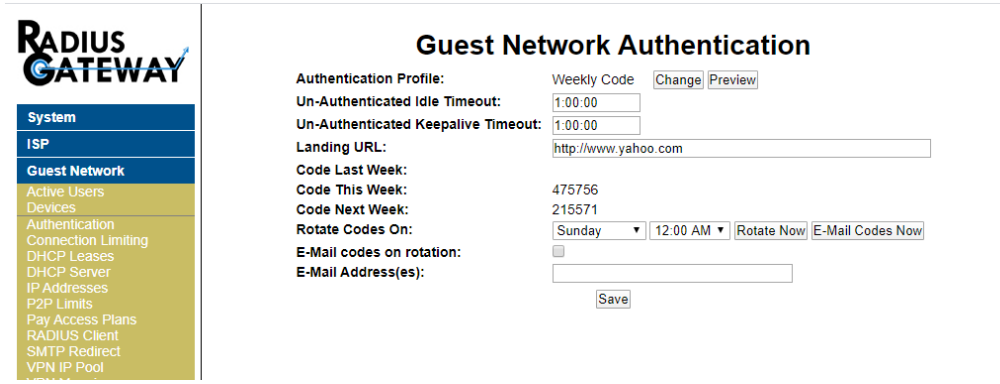
**Weekly Access Code**

The Weekly Access code login method allows for a standard weekly access code. The configuration page shows last week's code, the current code, and next week's code. The following fields are available and configurable for these authentication profiles:

- **Rotate Codes On:** This field determines on what day and what hour to rotate the weekly codes. The "Rotate Now" button may also be clicked to rotate the codes manually if desired.
- **E-Mail codes on rotation:** If this box is checked, the gateway will attempt to e-mail the recipients defined in the E-Mail Address(es) field when codes rotate.
- **E-Mail Address(es):** This field defines which e-mail addresses will receive the new codes after they are rotated (either automatically at the specified time or manually when the **Rotate Now** button is clicked).

**IMPORTANT NOTE:** When choosing to e-mail new codes, the outgoing SMTP server settings MUST BE defined in the **System→E-Mail Settings** screen.

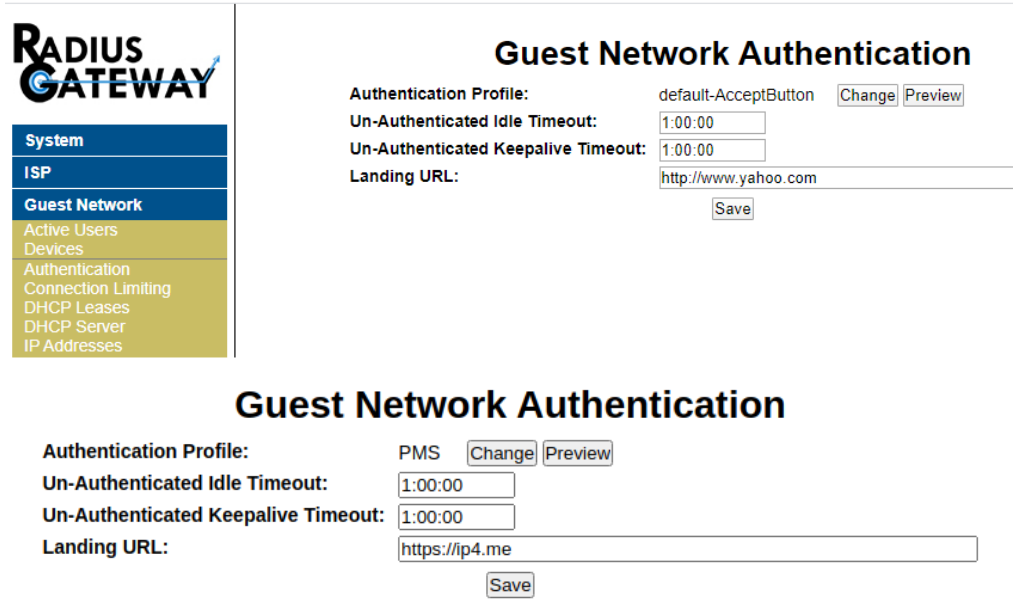
Copyright © 2021 Radius Gateway LLC. All rights reserved.




**PMS**

The PMS authentication profile is available on gateways with the add-on PMS module purchased and installed. This authentication method presents a login screen to end users. If the end user doesn't have an account, he or she may purchase or acquire an account by signing up and verifying room reservations against a PMS system. Available fields for configuration are Idle Timeout, Keepalive Timeout, and Landing URL.

- Supported PMS interfaces include: Agilysys, Amadeus, Infor, Lodging Link, Opera, and Visual Matrix.




Copyright © 2021 Radius Gateway LLC. All rights reserved.

**PMS Free**

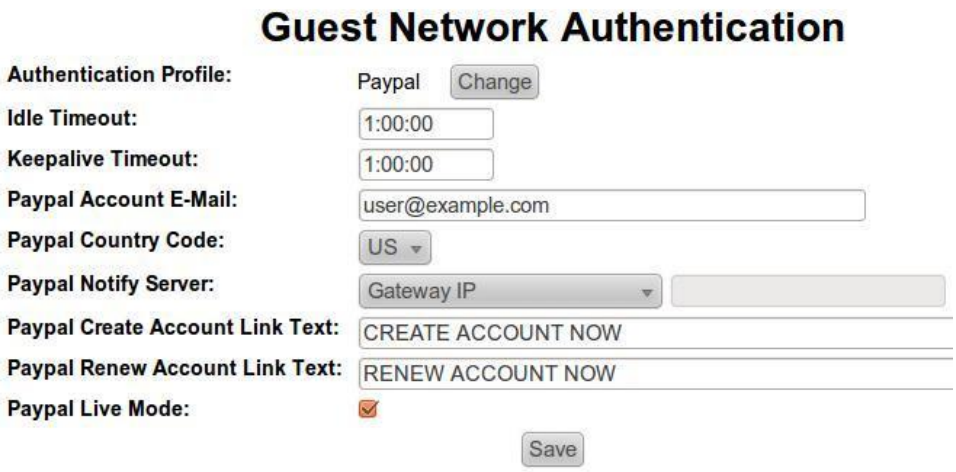
PMS Free authentication is the same as PMS. The only difference is that PMS room verification is all that is required. Users are not required to create or purchase accounts.

**PayPal**

The PayPal Authentication profile allows a user to setup an account and purchase service via a PayPal account. The PayPal configuration fields include:

- **Account E-Mail:** This is the e-mail address on the PayPal account.
- **Country Code:** This is the country code for the PayPal interface. PayPal displays address formats for the selected country code. Available country codes are US, AU, CA, GB, IE, and NZ. The working currency code is defined in **Guest Network→Pay Access Plans**.
- **PayPal Notify Server:** When a transaction is successfully completed, PayPal may be configured to notify a specific server of the successful transaction. PayPal may send a request back to the gateway that causes the gateway to create or renew the requested account. Available options are:
  - None (user MUST click the return link in order to complete their order)
  - Gateway IP (PayPal sends notification to the gateway public IP address)
  - Gateway DynDNS Hostname (PayPal sends notification to the gateway's DynDNS hostname)
  - Other IP or host (PayPal sends notification to a customized IP address; used in the case of a double-NAT configuration)
  - Other URL (PayPal sends notification to a fully customized URL)
- **Create Account Link Text:** On the PayPal receipt page, this is the text for the link the user may click to return to the login page after a successful account creation.
- **Renew Account Link Text:** On the PayPal receipt page, this is the text for the link the user may click to return to the login page after a successful account renewal.
- **Live Mode:** PayPal may be configured for development/test mode. In test mode, a PayPal Sandbox account is required. More information about the PayPal API and Sandbox may be found on the PayPal web site http://www.paypal.com.

Copyright © 2021 Radius Gateway LLC. All rights reserved.




**default-AcceptButton & default-Login**

The default AcceptButton profile presents the guest user with a login screen consisting of a terms of service box and an Accept button. To gain Internet access, a user must click the **I Agree** button.

The default Login profile presents the guest user with a login screen consisting of a terms of service box and fields for username and password. Usernames and passwords may be defined in the **RADIUS Server→Browse Users** screen.

For both of these profiles, the Terms of Service is configurable on the **Guest Network→Terms of Service** screen. Similarly, the login page logo is customizable on the **Guest Network→Login Page Logo** screen.

**RADIUS-external**

The RADIUS-external authentication profile directs a user on the guest network to an external login page. The remote login page and RADIUS authentication method takes the following steps for the end user:

- Radius Gateway redirects end user to remote server to display the login page(s).
- Remote web server serves page(s) required for sign up or login.
- On user login, remote server redirects user to local Radius Gateway login page with the proper parameters set. This triggers the Radius Gateway to perform RADIUS authentication with the configured RADIUS server(s).

Copyright © 2021 Radius Gateway LLC. All rights reserved.

The following steps may be taken to enable a basic external login page with RADIUS authentication.

**STEP 1: Code web page.**
Sample code for a login page that resides on an external web server is presented on the following pages for PHP and ASP. The login page on the remote server will receive the following form parameters via an http GET request. See the HTML login page customization section for descriptions of the variables:

- dst
- hostname
- identity
- login-by
- server-address
- interface-name
- ip
- mac
- popup
- error

**IMPORTANT:** Make sure that the login form posts these parameters and their values back to the gateway (except for the error parameter) when the user is performing the actual login.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**PHP Example**

```
<html>
 <head>
  <title>Login Page</title>
 </head>
 <body>
  <h1>Please Log on</h1>
  <form method='post' action='http://<?=$_REQUEST['hostname']?>/login'>
   <table>
    <tr>
     <td>
      <b>Username:</b>
     </td>
     <td>
      <input type="text" name="username">
     </td>
    </tr>
    <tr>
     <td>
      <b>Password:</b>
     </td>
     <td>
      <input type="password" name="password"><br>
     </td>
    </tr>
   </table>

   <input type="submit" value="Login">
   <input type="hidden" name="dst" value="<?=$_REQUEST['dst']?>">
   <input type="hidden" name="hostname" value="<?=$_REQUEST['hostname']?>">
   <input type="hidden" name="identity" value="<?=$_REQUEST['identity']?>">
   <input type="hidden" name="login-by" value="<?=$_REQUEST['login-by']?>">
   <input type="hidden" name="server-address" value="<?=$_REQUEST['server-address']?>">
   <input type="hidden" name="server-name" value="<?=$_REQUEST['server-name']?>">
   <input type="hidden" name="interface-name" value="<?=$_REQUEST['interface-name']?>">
   <input type="hidden" name="ip" value="<?=$_REQUEST['ip']?>">
   <input type="hidden" name="mac" value="<?=$_REQUEST['mac']?>">
   <input type="hidden" name="popup" value="<?=$_REQUEST['popup']?>">

  </form>
  <?
  if ($_REQUEST['error'] != "")
  {
   echo "Error: ".$_REQUEST['error'];
  }
  ?>
 </body>
</html>
```

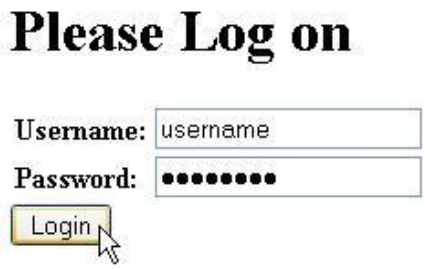
Copyright © 2021 Radius Gateway LLC. All rights reserved.

**ASP Example**

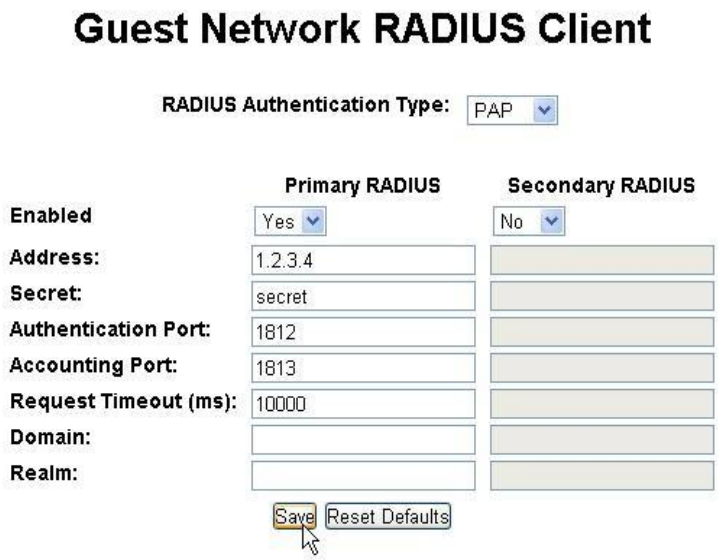
```
<html>
 <head>
  <title>Login Page</title>
 </head>

 <body>
  <h1>Please Log on</h1>

  <form method='post' action="http://<%=Request.QueryString("hostname")%>/login">
   <table>
    <tr>
     <td>
      <b>Username:</b>
     </td>
     <td>
      <input type="text" name="username">
     </td>
    </tr>
    <tr>
     <td>
      <b>Password:</b>
     </td>
     <td>
      <input type="password" name="password"><br>
     </td>
    </tr>
   </table>

   <input type="submit" value="Login">
   <input type="hidden" name="dst" value="<%=Request.QueryString("dst")%>">
   <input type="hidden" name="hostname" value="<%=Request.QueryString("hostname")%>">
   <input type="hidden" name="identity" value="<%=Request.QueryString("identity")%>">
   <input type="hidden" name="login-by" value="<%=Request.QueryString("login-by")%>">
   <input type="hidden" name="server-address" value="<%=Request.QueryString("server-address")%>">
   <input type="hidden" name="server-name" value="<%=Request.QueryString("server-name")%>">
   <input type="hidden" name="interface-name" value="<%=Request.QueryString("interface-name")%>">
   <input type="hidden" name="ip" value="<%=Request.QueryString("ip")%>">
   <input type="hidden" name="mac" value="<%=Request.QueryString("mac")%>">
   <input type="hidden" name="popup" value="true">
  </form>

  <%
  if Request.QueryString("error") <> "" then
   %>
   Error: <%=Request.QueryString("error")%>
   <%
  end if
  %>
 </body>
</html>
```

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Guest Login Page View**




**STEP 2: Define RADIUS client parameters.**
See the RADIUS (**Guest Network → RADIUS Client**) section.



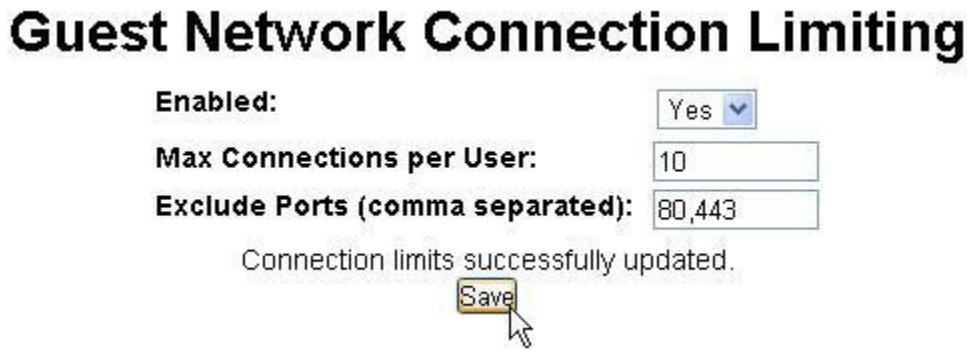

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**STEP 3: Set authentication method to RADIUS-external.**
Set up the login URL to point to the remote server.

**Connection Limiting (Guest Network → Connection Limiting)**

This screen defines limiting of guest TCP connections. If enabled, each IP address on the guest network will only be allowed to open the specified number of TCP connections. This setting may be useful to limit the abuse of P2P file sharing programs to some extent.

The configuration in the image below will limit each user to 10 TCP connections outside of web browsing on ports 80 (http) and 443 (https). Since P2P downloads commonly use more than 50 TCP connections on different TCP ports, this will limit the P2P downloads to only 10 connections.

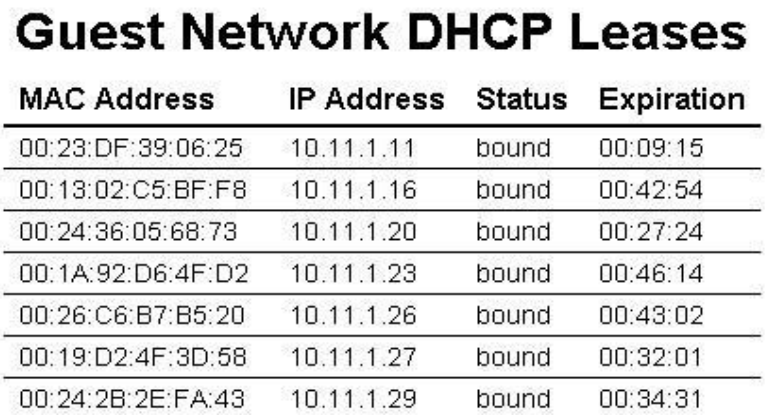



- **Enabled** — Enable or disable Guest Network connection limiting feature.
- **Max Connections per User** — Maximum number of TCP connections allowed to each user on the guest network.
- **Exclude Ports** — Comma-separated list of outgoing TCP ports to exclude from connection limiting.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**IMPORTANT:** Setting the max connections per user to less than 10 may cause serious connectivity problems with guest network users, as well as loss of gateway management from the guest network subnet. If it is desired to set this field to less than 10, make sure to set the Exclude Ports field to exclude ports 80 and 443.

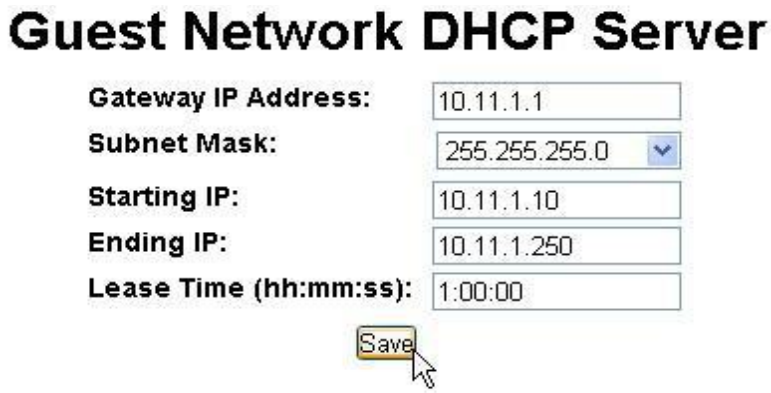
**DHCP Leases (Guest Network → DHCP Leases)**
This screen displays the current guest network DHCP leases.



Guest Network DHCP Leases

| MAC Address | IP Address | Status | Expiration |
|---|---|---|---|
| 00:23:DF:39:06:25 | 10.11.1.11 | bound | 00:09:15 |
| 00:13:02:C5:BF:F8 | 10.11.1.16 | bound | 00:42:54 |
| 00:24:36:05:68:73 | 10.11.1.20 | bound | 00:27:24 |
| 00:1A:92:D6:4F:D2 | 10.11.1.23 | bound | 00:46:14 |
| 00:26:C6:B7:B5:20 | 10.11.1.26 | bound | 00:43:02 |
| 00:19:D2:4F:3D:58 | 10.11.1.27 | bound | 00:32:01 |
| 00:24:2B:2E:FA:43 | 10.11.1.29 | bound | 00:34:31 |

**DHCP Server (Guest Network → DHCP Server)**
This screen controls the DHCP server settings on the guest network ports. By default, the DHCP server hands out IP addresses on the 10.11.0.0/16network. This may be changed in the DHCP Server screen. This will also change the primary IP, which may be viewed in the Guest Network → IP Addresses screen.

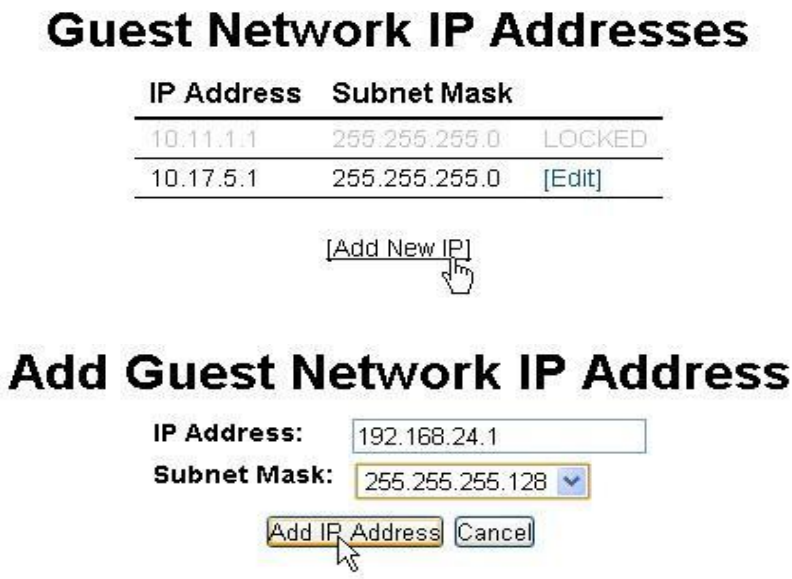



Copyright © 2021 Radius Gateway LLC. All rights reserved.

**IP Addresses (Guest Network → IP Address)**

The **Guest Network → IP Address** screen controls the gateway's IP addresses on the guest network. This dialog allows for assigning multiple IP addresses on the guest network ports which helps to segregate network equipment (statically assigned IPs) from guest user machines.

- From the main menu, click **Guest Network → IP Addresses**.
- Click the **Add New IP** button.
- Add the address and subnet mask.

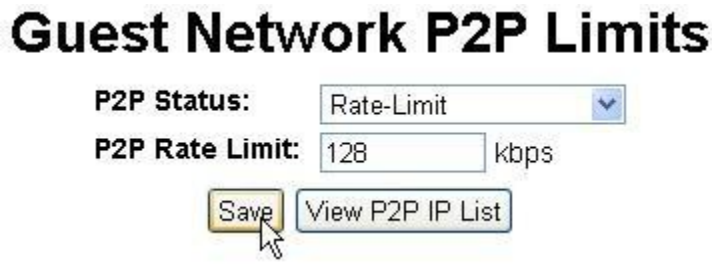



**NOTE:** The primary IP address of the guest network is locked and is only modifiable in the DHCP Server configuration. To change this IP address, use the Guest Network → DHCP Server configuration screen.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

### P2P File Sharing (Guest Network → P2P File Sharing)

This screen defines peer-to-peer file sharing settings. The bandwidth restrictions defined here are for the entire ISP connection and not for each user on the guest network. For example, if P2P sharing is set to 128kbps and two users are both attempting to max out their P2P connections at the same time, each user will be allocated 64kbps. The Connection Limiting feature is also helpful to mitigate some of the network traffic problems that can be caused by P2P file sharing.

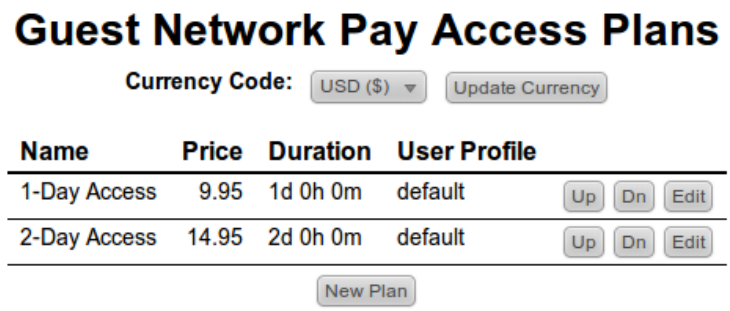



- **P2P Status**
  - **Allow All —** Allows all P2P on guest network. Users are only limited by their individual bandwidth caps (if defined).
  - **Rate-Limit —** Gateway limits unencrypted P2P sharing on Internet connection to the defined bandwidth.
  - **Aggressive Rate-Limit** — Gateway aggressively limits P2P sharing. When P2P is detected, the IP address of the detected client is put into a bandwidth queue with all other P2P offenders. ALL traffic generated from the offending IP addresses is limited through this single queue. To be removed from the queue, the offender must close all P2P applications and wait 1 to 2 minutes. This method is useful to limit the transmission of encrypted P2P traffic.
  - **Block All —** Gateway blocks all unencrypted P2P.
- **P2P Rate Limit** — When Rate-Limit or Aggressive Rate-Limit status is selected, this input may be filled in with the desired P2P rate limit bandwidth.

**NOTE:** P2P is an ever-changing technology that is difficult to detect, monitor, limit, and block. Therefore, P2P limits are best effort.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Pay Access Plans (Guest Network → Pay Access Plans)**
This screen defines the available pay access plans for PayPal or PMS integrations. The working currency code may also be defined on this screen. The **Up**/**Down** buttons move the selected plan up or down in the user's select box on their create/renew account page.




**Currency Code**
To set the working currency code, choose the desired currency from the drop-down menu and click the **Update Currency** button. Available currency codes are USD ($), AUD ($), CAD ($), EUR (€), GBP (£), INR (Rs) and NZD ($). This setting is used for display and integration purposes for PayPal and PMS authentication.

**IMPORTANT:** INR Rupees should not be used when using PayPal authentication. PayPal currently does not support the INR currency code.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

### New Plan

To create a new pay plan, click the **New Plan** button.

**Plan Name** — The name of the plan presented to the user on the create/renew account page.

- **Price** — The price in the selected currency (available on the PayPal configuration screen).
- **Days / Hours / Minutes** — These fields control how much time the user will be allotted after successful payment is made. The time is based on how much time is used. For example, if a user signs up for a 1-day plan, they may use 2 hours the first day, 1 hour the second day and still have 21 hours left for future use.
- **RADIUS User Profile** — The RADIUS profile assigned to a user after successful login. (**RADIUS Server → RADIUS User Profiles**)

### Edit Plan

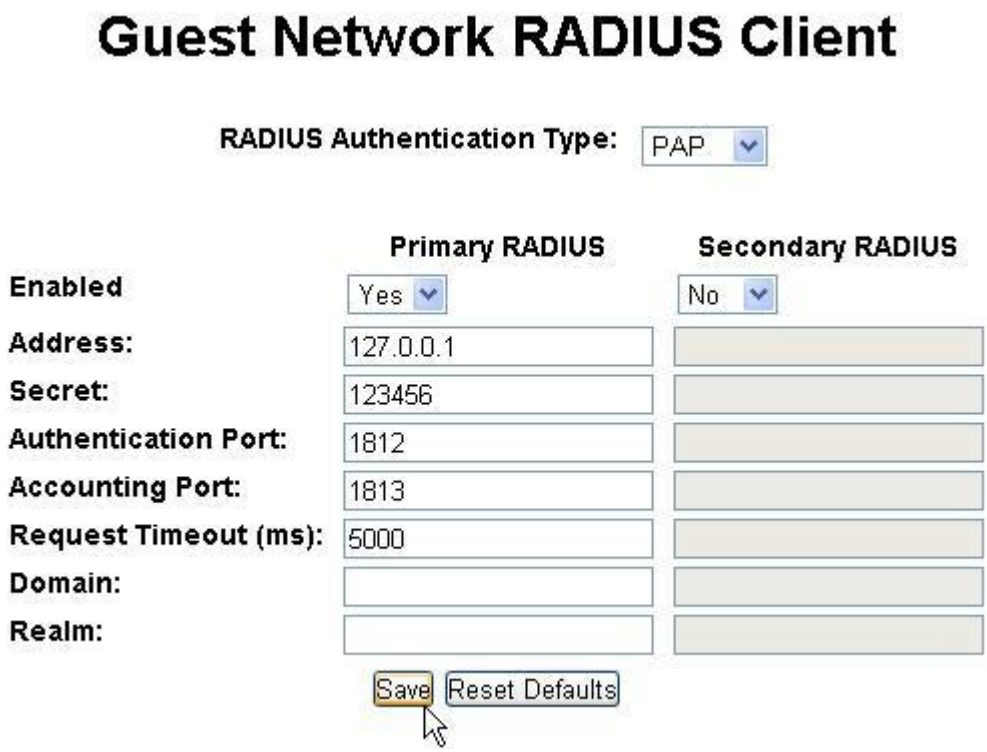
To edit a plan, click the **Edit** button on the desired plan. The form fields behave identically to the New Plan fields (see above).

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**RADIUS Client (Guest Network → RADIUS Client)**

This screen is used to set up RADIUS client settings for an external RADIUS server(s). There are two possible server definitions. By default, the server is set to 127.0.0.1, which points to the internal RADIUS server on the Radius Gateway. When RADIUS authentication is desired, only the primary RADIUS server entry is required. See Appendix A for available RADIUS attributes. The **Reset Defaults** button will revert the fields back to local RADIUS server settings.

- **RADIUS Authentication Type** — PAP and CHAP are currently available.
- **Address —** The IP address of the desired RADIUS server.
- **Secret —** The RADIUS shared secret used to access the RADIUS server.
- **Authentication Port** — The RADIUS server port used for authentication requests.
- **Accounting Port** — The RADIUS server port used for accounting requests.
- **Request Timeout** — The request re-send timeout value.
- **Domain** — The Microsoft Windows domain of the client passed to RADIUS servers that require domain validation. This field is typically left blank.
- **Realm —** The explicitly stated realm (user domain), included so end users do not have to provide the proper ISP domain name in the username. This field is typically left blank.




Copyright © 2021 Radius Gateway LLC. All rights reserved.

**SMTP Redirect (Guest Network → SMTP Redirect)**

This screen defines the outgoing SMTP server settings. When users on the guest network attempt to send e-mail through the SMTP port (TCP 25), the gateway intercepts the e-mail and redirects it to the server defined on this screen.

**NOTE:** It is a good practice to use outbound spam filtering such as ASSP (http://assp.sourceforge.net/) on the SMTP server. Many users unknowingly have spambots on their computers. If too many spam messages go out through the Internet connection, the IP address may be permanently blacklisted by any number of spam lists. If it is desired to block all outbound e-mail on port 25, the IP address 127.0.0.1 may be entered in this screen or a firewall filter may be set up for this port in the **Advanced → Firewall Filter** screen.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

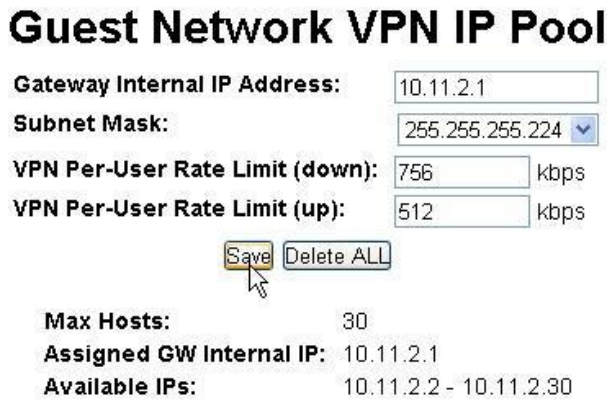
Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Public IPs (Guest Network → VPN IP Pool)**

This screen, along with the **Guest Network → VPN Mappings** screen, is used to set up mapping between private IP addresses on the guest network and public IP addresses on the Internet. It is used primarily to assure VPN connectivity from guest network users to their VPNs and ensures greater reliability for end-user VPN connections. When this mapping occurs, all network traffic destined for the mapped public IP address is translated directly to the private IP address. This includes all protocols and ports.

**IMPORTANT:** The VPN mapping feature will only function properly when the ISP connection is configured to a public static IP address.

**IMPORTANT:** If the gateway is configured in Failover or Load Balance mode, VPN public IP addresses are only able to be mapped on the primary connection (ether1).




Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Setting Up Public VPN IP Addresses**

To begin setting up VPN IP addresses, a separate private IP pool must be defined that will map to public IP addresses.

- **Gateway Internal IP Address —** May be any private IP address that is not already assigned on the gateway. This IP address must be the first usable IP address in the selected subnet. If it is not, it will be defaulted to the first IP address in the selected subnet.
- **Subnet Mask** — The subnet mask of the desired pool. For most applications, a /24 (255.255.255.0) subnet is sufficient. This subnet mask does not need to match the subnet mask of the public IP address configured on ether1.
- Based on the selected internal IP and internal subnet mask, the **maximum hosts**, **assigned GW internal IP**, and **available IP addresses** will be calculated and displayed automatically.
- **VPN User Rate Limit (rx/tx)** — Bandwidth limits on the VPN user profile (which is generated from this form).

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**VPN Mappings (Guest Network → VPN Mappings)**
After the initial pool is set up, the VPN Mappings screen may be used to map public IP addresses to the private IP pool.

**Add/Edit VPN Mapping**
To add a new VPN mapping, click the **Add New VPN IP** link. To edit a mapping, click the **Edit** link.

- **Public IP Address** — The desired public IP address to map. It is advisable to verify that the selected IP address is owned and routable. VPN IP address mapping will not function properly if the IP address is not available and routable through the ISP connection.
- **Public Subnet** — This is the subnet mask of the public IP address obtained from the ISP. It will typically match the public static IP address configuration.
- **Private Pool Address** (Edit Screen) — The private address to which the public IP will be mapped. This is calculated automatically and is not editable.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**NOTE:** When the guest network is configured for internal authentication, the **Use Public VPN** checkbox should be checked in the **Guest Network → Authentication** screen. When this is checked, a new checkbox is presented to the user on the accept button authentication pages, which will allow him or her to choose a public IP address. For standard username/password login pages, the address pool is defined by the user profile. See the **RADIUS Server → RADIUS User Profiles** section of this manual for more information on these related settings.

**NOTE:** When performing external RADIUS authentication, if a public VPN IP address is required, a "Framed-Pool" RADIUS attribute must be sent with the RADIUS reply message from the RADIUS server. The Framed-Pool attribute should be set to "subscriber-pool-public" when a public IP address is needed. If a public IP address is not needed, this attribute should not be sent in the RADIUS reply. See Appendix A for supported RADIUS attributes.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Walled Garden (Guest Network → Walled Garden)**

This screen defines the domains that are allowed to be accessed by an unauthenticated user on the guest network.

## Guest Network Walled Garden

| Host / IP Address | Hits | Comment | | |
|---|---|---|---|---|
| *.akadns.net | 0 | Paypal | [Edit] | [Delete] |
| *.akamaiedge.net | 0 | Paypal | [Edit] | [Delete] |
| *.edgekey.net | 0 | Paypal | [Edit] | [Delete] |
| *.ipchicken.com | 0 | | [Edit] | [Delete] |
| *.paypal.com | 0 | | [Edit] | [Delete] |
| *.paypalobjects.com | 0 | Paypal | [Edit] | [Delete] |
| *.radiusgateway.com | 0 | | [Edit] | [Delete] |
| *.speakeasy.net | 0 | | [Edit] | [Delete] |
| 10.255.255.254 | | RADConfig-Web Server | LOCKED | |
| 10.255.255.254 | | RADConfig-Web Server | LOCKED | |
| login.radiusgateway.com | 0 | RADConfig-Web Server | LOCKED | |
| www.paypal.com | 0 | | [Edit] | [Delete] |
| www.sandbox.paypal.com | 0 | | [Edit] | [Delete] |

[Add New Walled Garden Entry]

Copyright © 2021 Radius Gateway LLC. All rights reserved.

### Add Walled Garden Entry

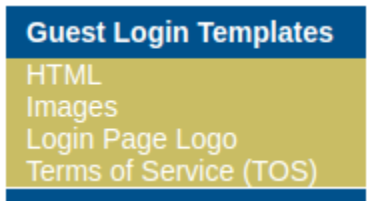
To add a domain to the walled garden, click the **Add New Walled Garden Entry** link.

- **DNS Name / IP Address —** This field defines the target that will be allowed. This field is capable of handling the * wildcard. For example, if all subdomains of newdomain.com are desired, "*.newdomain.com" would be entered in the DNS Name/IP Address field. As the field title indicates, IP addresses are also allowed in this field.
- **Comment** — The comment for the walled garden entry.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

## *Guest Login Templates*

When doing internal Radius Gateway authentication, the HTML, javascript, and images on the login page may be changed. This is done in the Guest Login Templates menu tree.




**HTML**

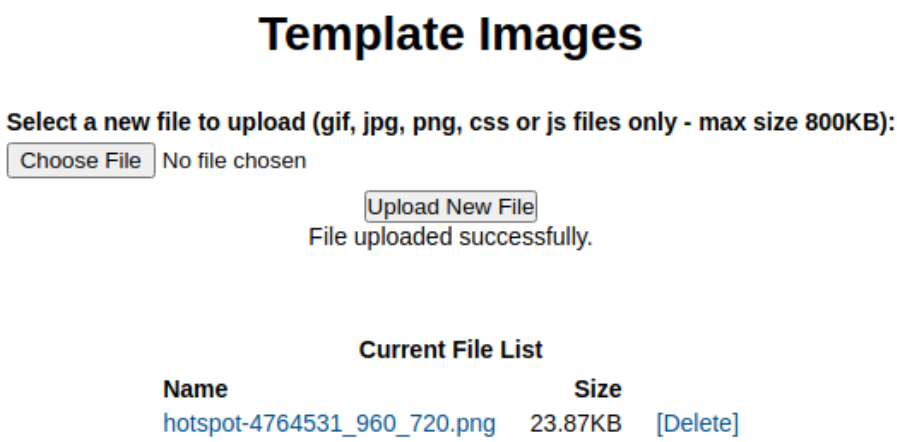
The HTML configuration screen defines the HTML presented to the user during the login process. A template file may be chosen, and HTML is editable on this screen. There are several variables available to the templating system. Variables are used in the HTML by placing their names inside of curly brackets as outlined here:

- {images} - The image directory for custom-uploaded images. See next section for image upload instructions.
- {loginForm} - Automatically generated login form.
- {logo} - The logo uploaded in the Login Page Logo screen.
- {required} - The required code for this template (usually JavaScript code).
- {tosHtml} - Terms of service html version.
- {tosText} - Terms of service text version.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

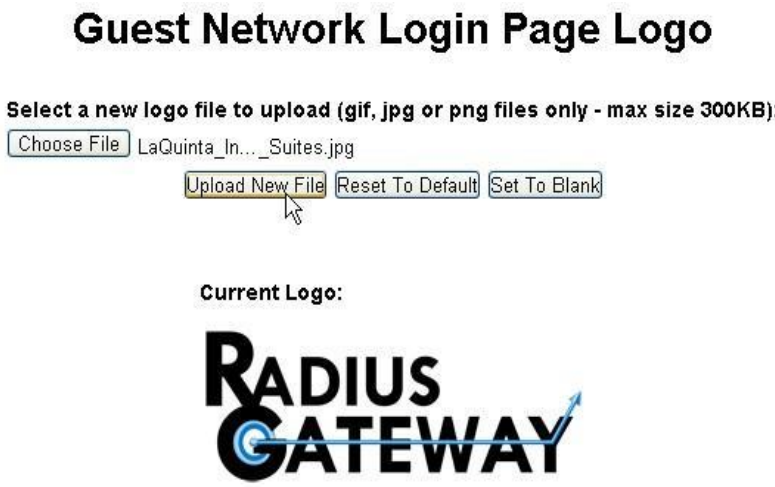
**Images**

This is the screen used to upload custom images for placement in the login page HTML. This screen is to upload extra images (not the site logo image). After files are uploaded, they are displayed in the current file list. They may be used in the HTML template screen by inserting an img tag with the src="{images}/uploaded-image-file.jpg"




**Login Page Logo (Guest Network → Login Page Logo)**

The logo in the HTML templates may be changed via the web interface. To use the logo in the HTML template, place the {logo} variable in the desired position. This variable will render the entire <img> tag structure.




Copyright © 2021 Radius Gateway LLC. All rights reserved.

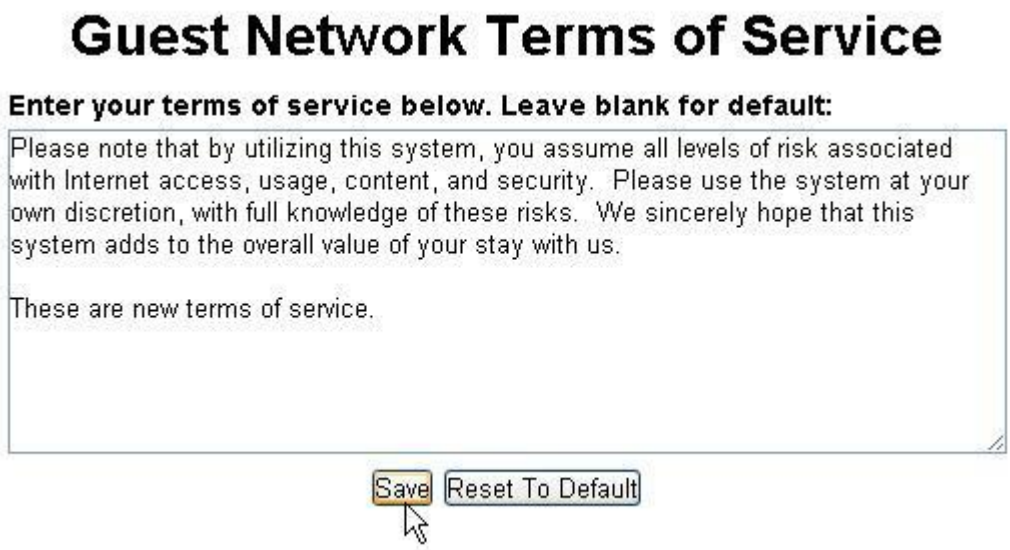
To change the logo:

- Click the **Choose File** button and choose the file you wish to upload. Please note that the file cannot exceed the size of 300KB and only gif, jpg, or png files will be accepted.
- Click the **Upload New File** button.

To reset the logo back to the default Radius Gateway logo, click the **Reset To Default** button.

To remove the logo altogether, click the **Set To Blank** button.

**Terms of Service (Guest Network → Terms of Service)**
Guest Network Terms of service may be changed on this screen. To reset the terms back to default, click the **Reset To Default** button.




Copyright © 2021 Radius Gateway LLC. All rights reserved.

## *PMS Menu*

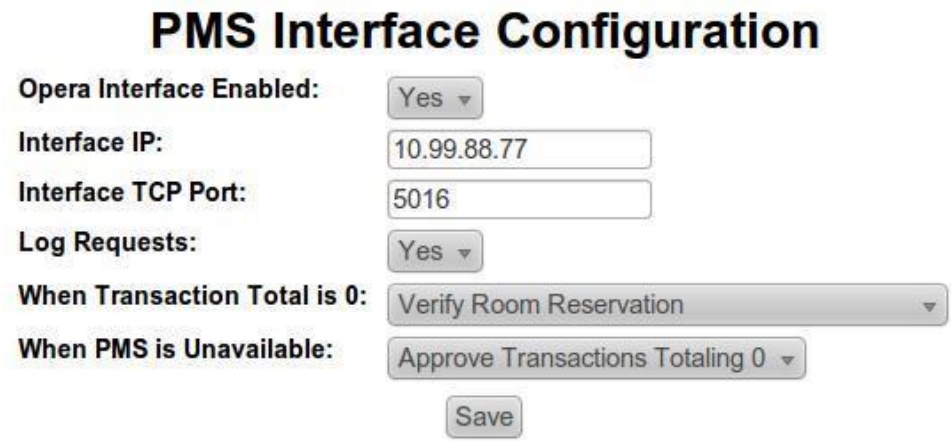
PMS integration is available as a separate purchasable module from Radius Gateway. There is also a required module that needs to be installed on the PMS system by the PMS vendor. The PMS Menu controls the parameters for integrating with a PMS system.

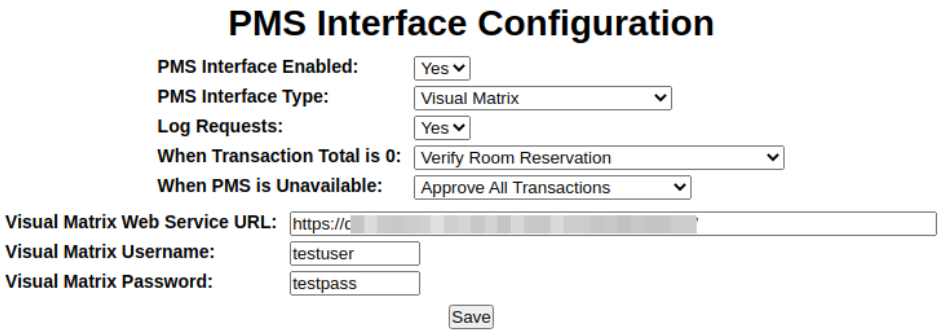
**PMS Interface Configuration (PMS → Configuration)**

This screen is used to set up the communication and operational parameters of the PMS interface with Opera.

- **PMS Interface Enabled —** Enables/disabled communication with the system.
- **PMS Interface Type —** This field defines what type of PMS communication is being configured. Currently, the available PMS types are: Agilysys, Amadeus, Infor, Lodging Link, Opera, and Visual Matrix. Other custom fields will be displayed specifically for the PMS type selected. The PMS vendor should be consulted to determine the appropriate configuration values for any specific venue. Other PMS types may become available with future released versions of Radius Gateway.
- **Log Requests —** Enables/disables log requests to or from the PMS system.
- **When Transaction Total is 0 —** This field defines how the Radius Gateway will react when a PMS transaction total is 0. This field only applies to internal Radius Gateway authentication. The two options are:
  - **Verify Room Reservation —** This setting requires the user to verify that they are staying at the hotel by verifying room number and last name.
  - **User Must Accept TOS (no room verification) —** This setting requires the user to accept the TOS as defined in the **Guest Network → Terms of Service** screen.
- **When PMS is Unavailable —** This field defines how the Radius Gateway will react if the PMS link goes down, becomes unresponsive, or is otherwise unavailable. This field only applies to internal Radius Gateway authentication. Available options are:
  - **Deny All Transactions —** When the link is unavailable, deny all PMS transactions. This effectively prevents creation of any new user accounts.
  - **Approve Transactions Totaling 0 —** When the link is unavailable, only approve transactions totaling 0, whether or not the room number/last name matches.
  - **Approve All Transactions —** When the link is unavailable, approve ALL transactions regardless of the transaction amount and regardless of whether the room number/last name matches.

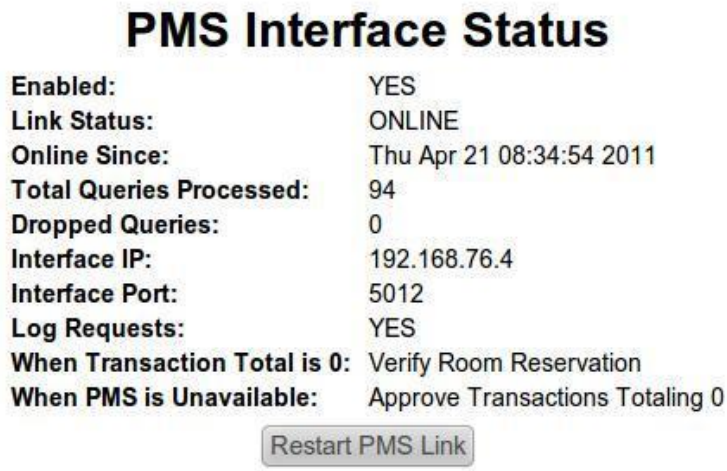
Copyright © 2021 Radius Gateway LLC. All rights reserved.




**PMS Status (PMS → Status)**

The PMS Status screen displays the current status of the PMS link. It is also possible to restart the PMS link from this screen.




Copyright © 2021 Radius Gateway LLC. All rights reserved.

**PMS Log (PMS → Log)**

The PMS Log screen displays the current PMS access log.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

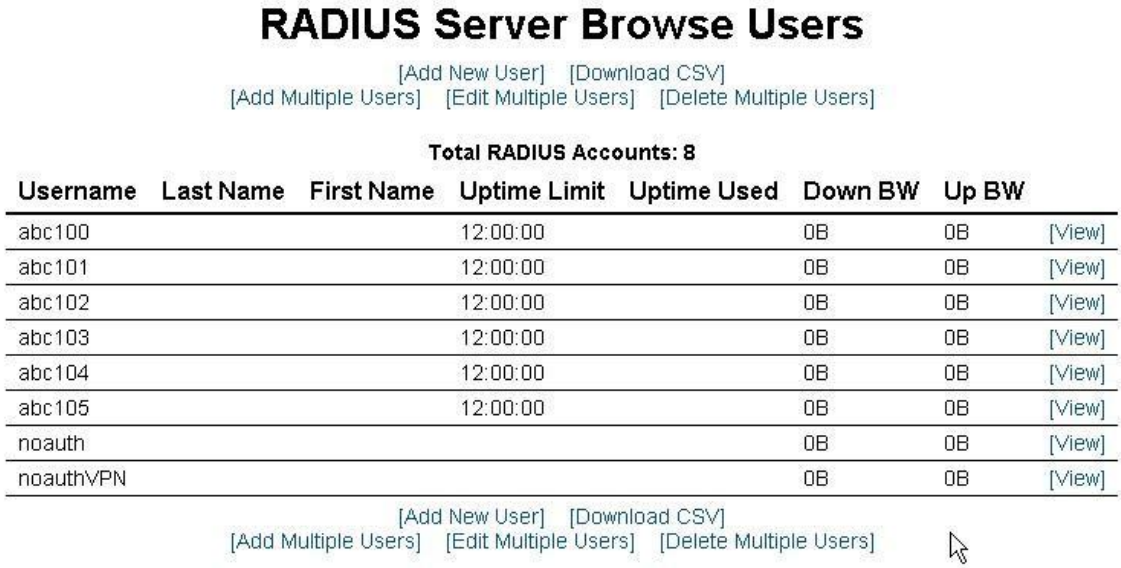
## *RADIUS Server Menu*

The RADIUS Server menu controls the internal RADIUS server features.

**Browse Users (Radius Server → Browse Users)**

This screen displays and controls the available users on the guest network stored in the internal RADIUS server. This dialog is primarily used when configuring internal gateway authentication.

**NOTE:** The noauth, noauthVPN, weekly, and weeklyVPN users are locked because they are used for internal accept button authentication. These users cannot be deleted, nor can the password be changed. Note also that other internal login methods that require username and password do not allow noauth or noauthVPN usernames to be used.




Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Add a New User**
To add a new user, simply click the **Add New User** link.

- **Username —** Defines the username.
- **Password** — Defines the password.
- **First Name** — User's first name.
- **Last Name** — User's last name.
- **E-Mail Address** — User's e-mail address.
- **RADIUS User Profile** — The profile that will be assigned to the user when logged in. See User profiles (**RADIUS Server → RADIUS User Profiles**).
- **Uptime Limit** — Amount of time user has available to be online. This refers to total time used, not clock time. For example, if a user is allowed 18 hours, he or she may use 1 hour today and 3 hours tomorrow with 14 hours left to use at a later date.

**Edit Existing User**
To edit an existing user, click the **View** link on the Browse User screen, then click the **Edit** button. All fields in normal user accounts are editable with the exception of the username.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Delete User**

To delete an existing user, click the **View** link on the Browse User screen, then click the **Delete** button. A pop-up will verify that deletion is really desired.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

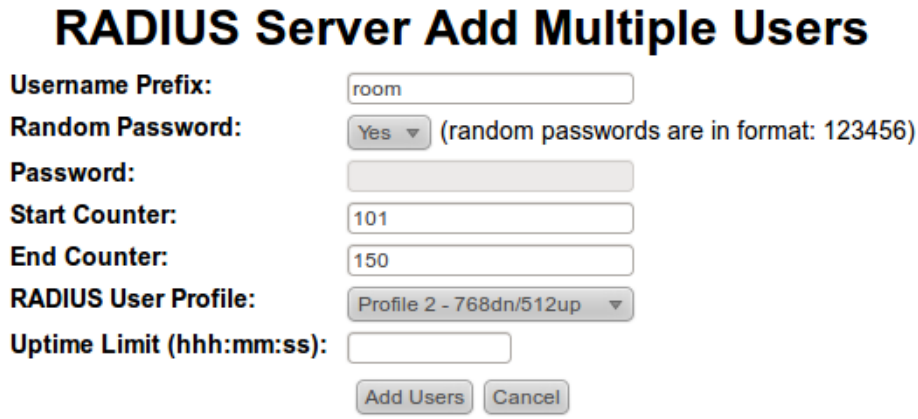
**Reset User Account (Reset Counters)**

If a user's time has expired and it is desired to renew the account manually, the **Reset Counters** button may be clicked from the View User page. A pop-up will verify that this action is really desired.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Add Multiple Users**

Multiple users may be added at a time. This is primarily used in a hotel situation wherein each room number has different login information. Each user created in this screen is assigned a specific username prefix. The username prefix is appended to the beginning of each user created. A numeric index is then appended to the end of the username prefix to create multiple new users. To begin this action, click the **Add Multiple Users** link on the Browse Users screen.




- **Username Prefix** — The desired username prefix.
- **Random Password —** Yes/No selection to generate random passwords or use the same password for all new accounts.
- **Password —** The desired password. This field is disabled if Random Password is set to "Yes".
- **Start Counter** — Where to start numbering the accounts.
- **End Counter** — Where to end numbering the accounts.
- **RADIUS User Profile** — The profile that will be assigned to the user when logged in. See User profiles (**RADIUS Server → RADIUS User Profiles**)
- **Uptime Limit** — Amount of time user has available to be online. This refers to total time used, not clock time. For example, if a user is allowed 18 hours, he or she may use 1 hour today and 3 hours tomorrow, with 14 hours left to use at a later date.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

### Edit Multiple Users

Multiple users may be modified at a single time. To do so, click the **Edit Multiple Users** link from the Browse Users screen.

| Edit | Username | Last Name | First Name | Uptime Limit | Uptime Used | Down BW | Up BW |
|---|---|---|---|---|---|---|---|
| ☐ | EDIT ALL | | | | | | |
| ☑ | GUEST | Lincoln | Abraham | | | 0B | 0B |
| ☑ | accessCode | | | | | 0B | 0B |
| ☑ | newUser | Smith | John | 18:00:00 | | 0B | 0B |
| ☐ | paypaltest | User | Test | 24:00:00 | | 0B | 0B |
| ☐ | paypaltest2 | User | Test | 24:00:00 | | 0B | 0B |
| ☐ | pmstest | miller | 101 | 24:00:00 | | 0B | 0B |

- In the top section, there are checkboxes. **Each checkbox determines if that field is updated for the chosen users below.** The users are chosen below. If it is desired to change all the users at one time, the **Edit All** checkbox may be checked.
- **Edit Random Password** — Yes/No select box to set random password.
- **Password —** If the password box is checked and random password is No, this password will be assigned to the chosen users.
- **Edit RADIUS User Profile** — The desired RADIUS profile for the chosen users.
- **Uptime Limit** — Amount of time chosen users have available to be online. This refers to total time used, not clock time. For example, if a user is allowed 18 hours, he or she may use 1 hour today and 3 hours tomorrow, with 14 hours left to use at a later date.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Delete Multiple Users**

Multiple users may be deleted at a single time. To do so, click the **Delete Multiple Users** link from the Browse Users screen. When users are selected, the **Delete Users** button may be clicked. A pop-up will be presented for verification.

**Download User CSV file**

A CSV file of current users may be downloaded from the gateway. Click the **Download CSV** link from the Browse Users screen. Spreadsheet programs such as Open Office Calc or Microsoft Excel may be used to open the CSV file for printing or electronic transmission.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Search Users (RADIUS Server → Search Users)**

The user list may be searched by username, first name, last name, or e-mail address. Enter the terms and click the **Search** button.

**Delete Old Users (RADIUS Server → Delete Old Users)**

Users who have signed up for an account will remain in the system until they are deleted. The Delete Old Users screen automatically deletes users who have not had any activity since a specific time. If an authentication type that requires user account creation is in place (e.g., PayPal authentication), the Delete Old Users function can be very useful when performed on a regular basis.

**RADIUS User Profiles (RADIUS Server → RADIUS User Profiles)**

This screen displays and configures available user profiles. User profiles are applied to available users on the local RADIUS server. A user profile must be assigned to all available users. The primary purpose of user profiles is to define timeouts and bandwidth restrictions.

**RADIUS User Profiles**

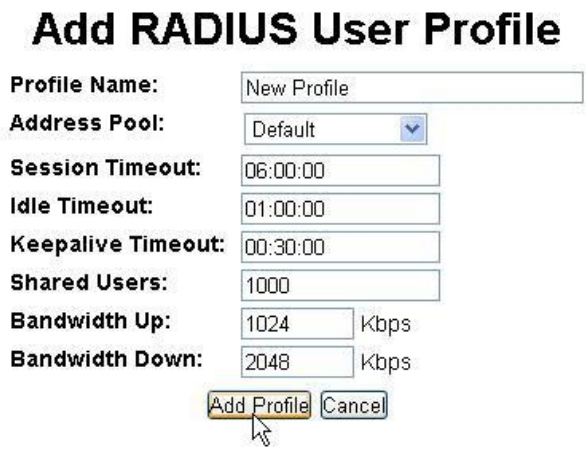
| Name | Rate Limit | Session Timeout | Idle Timeout | Shared Users | | |
|---|---|---|---|---|---|---|
| default | 512k/512k | | 1h | 1000 | [Edit] | |
| Profile 1 - 512dn/512up | 512k/512k | 06:00:00 | 1h | 1000 | [Edit] | [Delete] |
| Profile 2 - 768dn/512up | 512k/768k | 06:00:00 | 1h | 1000 | [Edit] | [Delete] |
| Profile 3 - 1024dn/768up | 1000k/768k | 06:00:00 | 1h | 1000 | [Edit] | [Delete] |

[Add New Profile]

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Add New Profile**

To add a new user profile, click the **Add New Profile** link.




- **Profile Name —** The name of the new profile.
- **Address Pool** — The DHCP address pool the user will be assigned to after login. This field is typically left as Default unless public VPN IP addresses are defined in the **Guest Network → VPN Mappings** menu and a public IP is desired for the new profile. See the **Guest Network → VPN Mappings** section of the manual for more information about setting up public IPs for VPN purposes.
- **Session Timeout** — Session timeout determines the total amount of time allowed in an individual login session. This is typically a large number like 6h or 12h. When this time limit is reached, the user is automatically logged off.
- **Idle Timeout** — Idle time is defined as the amount of time a user has not transmitted anything through the gateway (i.e., not accessed the Internet for anything). If this timeout is reached, the user will be automatically logged off.
- **Keepalive Timeout** — RADIUS Gateway can keep users alive for a period of time. Users are not alive if they are not detected on the guest network. Keepalive timeout will keep the user alive for this amount of time. If the user is determined to not be alive and this timeout has been reached, they will be automatically logged off.
- **Shared Users** — The total number of concurrent users allowed to use the profile.
- **Bandwidth Up/Down** — Bandwidth allocated to each user assigned to the user profile.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

## *Tools Menu*

The Tools menu contains useful tools for monitoring and troubleshooting guest and equipment connectivity.

**Ping (Tools → Ping)**

This screen is used to ping users or devices.

- Enter the equipment IP address
- If desired, check the ARP Ping checkbox. ARP Ping performs a ping by ARP address instead of IP address. It is required that the address being pinged be on the same subnet as the interface doing the pinging.
- Click the **Ping** button.
- Results will display below the form.

**NOTE:** If users or devices are not bypassed or authenticated, the ping may not succeed.

**IP Scan (Tools → IP Scan)**

This screen is used to scan IP ranges of users or devices on the guest network. It performs an ARP ping on the selected interface. Results are displayed below the form.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Netwatch (Tools → Netwatch)**

The Netwatch screen defines which IP addresses are monitored. When devices become unreachable from the gateway, the status will show "Down" in this dialog. When devices are added, they are automatically entered into the Netwatch Tool for convenience.

To add a new device, click the **Add Netwatch IP** link. Devices may be edited or deleted by clicking on the respective links for the desired device.

## Netwatch Tool

| IP Address | Interval | Timeout (ms) | Status | Since | Comment | |
|---|---|---|---|---|---|---|
| 10.17.5.235 | 00:01:00 | 3000 | up | jun/18/2010 06:38:00 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.236 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.237 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.238 | 00:01:00 | 3000 | up | jun/17/2010 05:50:00 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.239 | 00:01:00 | 3000 | down | jan/01/1970 19:00:42 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.240 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.241 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.242 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.243 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.244 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.245 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.246 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.247 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.248 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.249 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.250 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.251 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.252 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.253 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |
| 10.17.5.254 | 00:01:00 | 3000 | up | jun/17/2010 05:50:03 | Guest Network Device | [Edit] [Delete] |

[Add Netwatch IP]

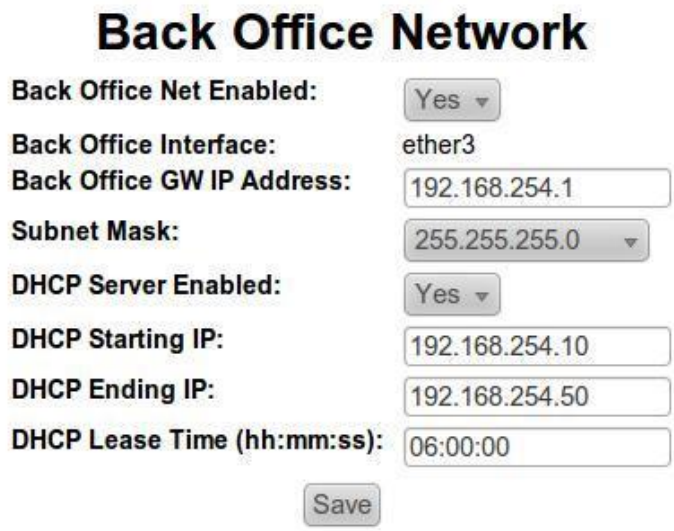
Copyright © 2021 Radius Gateway LLC. All rights reserved.

## *Advanced Menu*

The Advanced menu controls advanced gateway features and functions.

**Back Office Network (Advanced → Back Office Network)**

This screen is used to configure a back-office network with open access on the last available Ethernet port. This is useful for smaller networks that may need to share Internet resources between back office and guests. All communications from the guest network to the back-office network are blocked by the internal firewall, and the back-office network has QoS priority in the gateway.

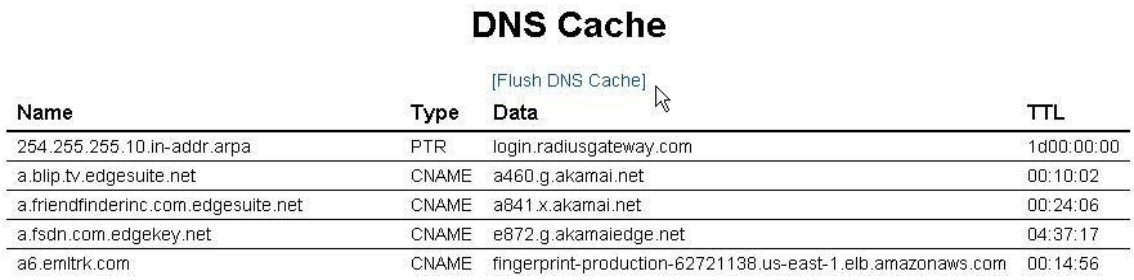



- **Back Office Net Enabled** — Enable or disable the back-office network.
- **Back Office Interface** — Interface on which to put the back-office network. This is unchangeable. This should use the last ETH port on the gateway.
- **Back Office GW IP Address** — Gateway IP address for the back-office network.
- **Subnet Mask** — Back-office subnet mask.
- **DHCP Server Enabled —** A setting to enable or disable a DHCP server for the back-office network.
- **DHCP Starting and Ending IP** — Starting and ending IP addresses for DHCP server.
- **DHCP Lease Time** — Lease time for DHCP addresses.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

### DNS Cache (Advanced → DNS Cache)

This screen displays the internal gateway DNS Cache with the option to flush the cache.



DNS Cache

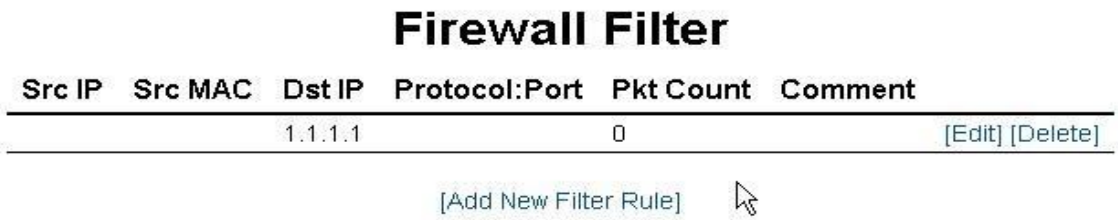
[Flush DNS Cache]

| Name | Type | Data | TTL |
|---|---|---|---|
| 254.255.255.10.in-addr.arpa | PTR | login.radiusgateway.com | 1d00:00:00 |
| a.blip.tv.edgesuite.net | CNAME | a460.g.akamai.net | 00:10:02 |
| a.friendfinderinc.com.edgesuite.net | CNAME | a841.x.akamai.net | 00:24:06 |
| a.fsdn.com.edgekey.net | CNAME | e872.g.akamaiedge.net | 04:37:17 |
| a6.emltrk.com | CNAME | fingerprint-production-62721138.us-east-1.elb.amazonaws.com | 00:14:56 |

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Firewall Filter (Advanced → Firewall Filter)**

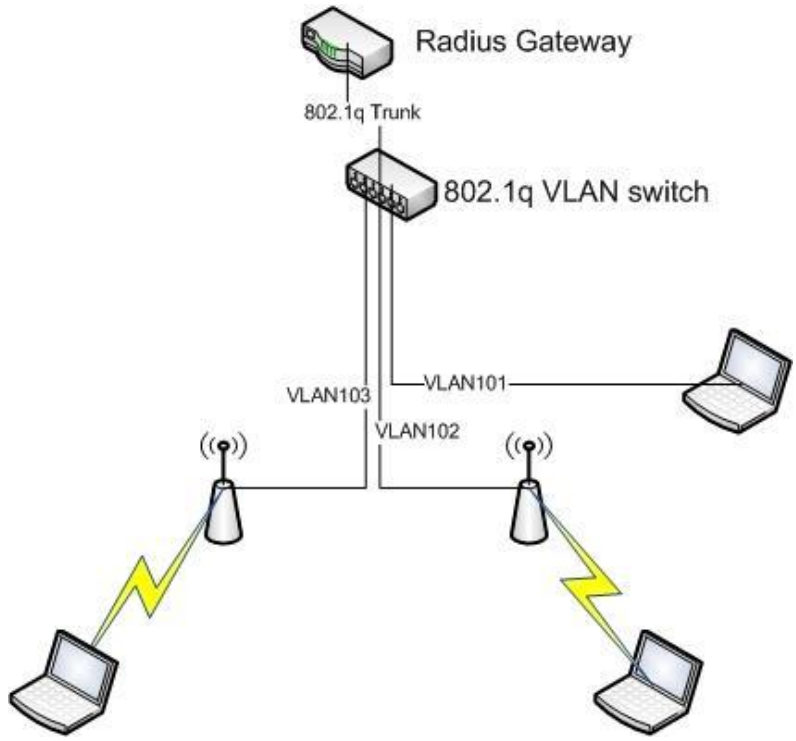
The Firewall Filter drops network traffic on the forward chain according to the specified rules. Traffic may be dropped by source IP, source MAC address, destination IP, protocol, and port, or multiple of the above options.




To add a new rule, click the **Add New Filter Rule** link. Define the desired rule and click the **Add Filter Rule** button.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Guest Network VLAN Mode (Advanced → Guest Net VLAN Mode)**
VLAN Mode allows the gateway to read and handle 802.1q VLAN tags. This function is useful if the guest network needs to be segmented via VLANs.



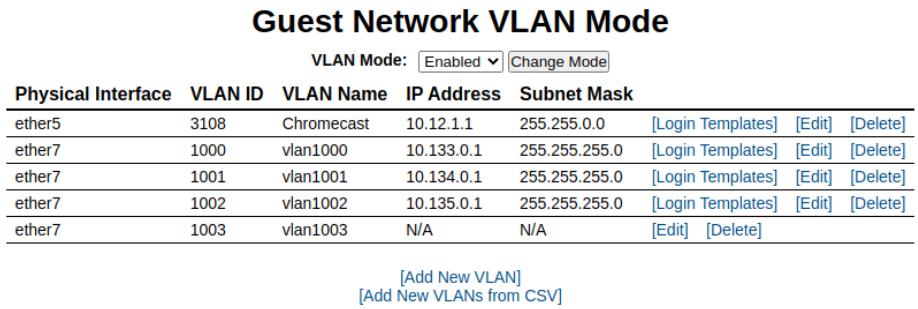

# Guest Network VLAN Mode

**VLAN Mode:** Enabled Change Mode

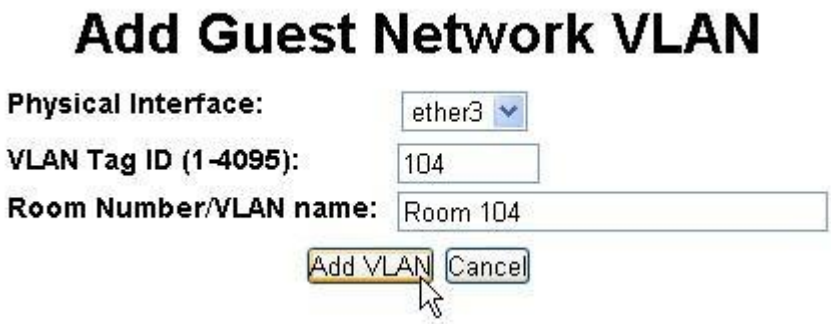
| Physical Interface | VLAN ID | Room Number | | |
|---|---|---|---|---|
| ether3 | 10 | Equipment | [Edit] | [Delete] |
| ether3 | 101 | Rm 101 | [Edit] | [Delete] |
| ether3 | 102 | Rm 102 | [Edit] | [Delete] |
| ether3 | 103 | Rm 103 | [Edit] | [Delete] |

[Add New VLAN]

Copyright © 2021 Radius Gateway LLC. All rights reserved.



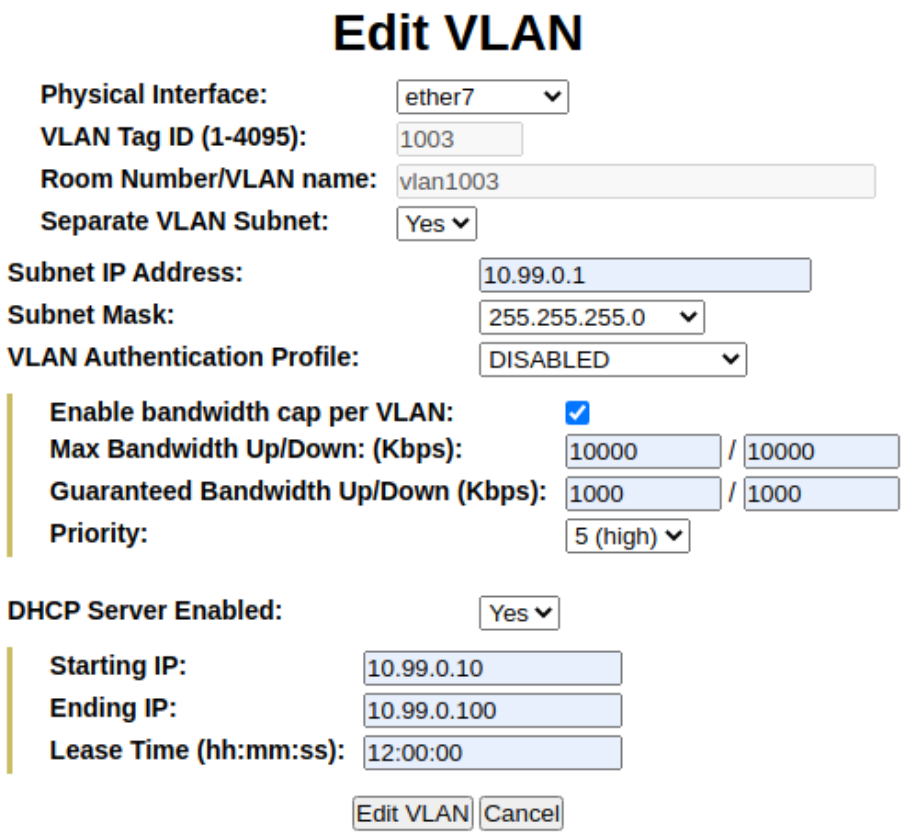

To enable VLAN mode, choose **Enabled** and click the **Change Mode** button. A pop-up will verify whether or not VLAN mode should really be enabled. To add a new VLAN to the guest network, click the **Add New VLAN** button.




- **Physical Interface —** The gateway physical interface that will be handling the VLAN tag.
- **VLAN Tag ID** — VLAN tag for the new VLAN.
- **Room Number/VLAN Name** — A human-readable VLAN identity.

By default, any new VLANs are on the guest network and tagged as such. If it is required to separate the VLAN from the guest network, the edit screen may be used to do this.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

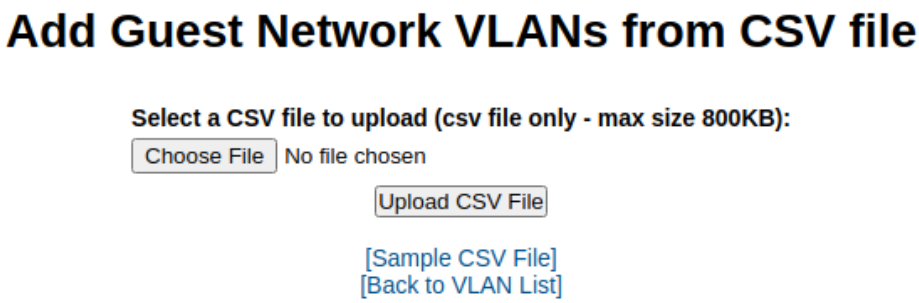



- If a separate subnet is desired for this VLAN, set the Separate VLAN Subnet field to "Yes". When Separate VLAN subnet field is Yes, the other fields will be displayed
- Subnet IP Address: This is the IP address of the gateway on the VLAN
- Subnet Mask: This is the subnet mask of the gateway on the VLAN
- VLAN Authentication Profile: Separate guest login profiles may be configured per VLAN/subnet. Set these here. Options are: DISABLED, default-AcceptButton default-Login, and RADIUS-external. Each login method will display different options depending on the profile selected.
- DHCP Server Enabled: Yes/No. If Yes, starting IP, Ending IP and Lease Time are available to be configured.

**Add Guest Network VLANs from CSV file**

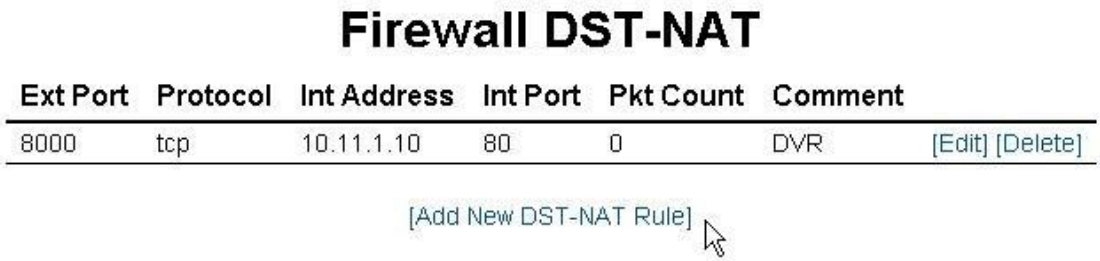
This screen is used to import a large number of VLANS into the gateway. See the sample CSV file link on this page for the file format.

Copyright © 2021 Radius Gateway LLC. All rights reserved.



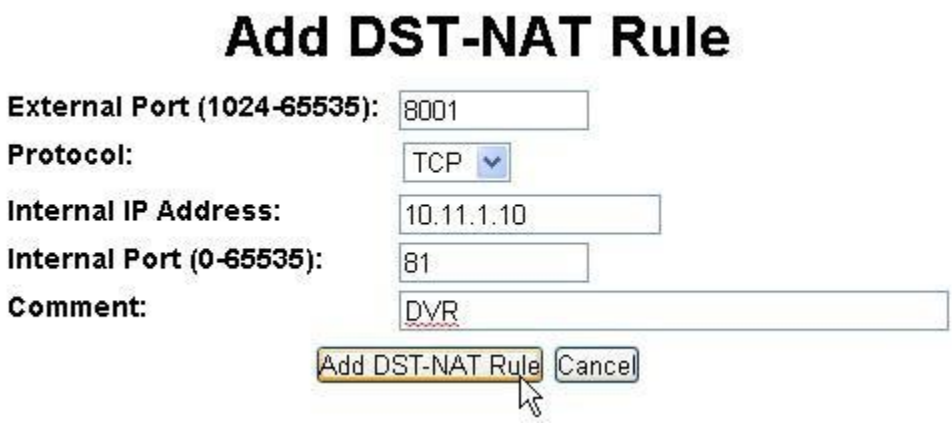

**Guest 2 Guest (Advanced → Guest 2 Guest)**
By default, all communication from guest to guest on the guest network is disabled. If it is desired to enable guest to guest communication, this screen may be used to enable it.

**Destination NAT (Advanced → NAT (DST-NAT))**
Destination NAT rules may be configured to permit external ports to map to internal devices and ports. Devices that are mapped externally in the **Guest Network → Devices** configuration screen are also visible here. This screen may also be used to define extra port mapping rules for existing devices if needed.




To add a new Destination NAT rule, click the **Add New DST-NAT Rule** link.

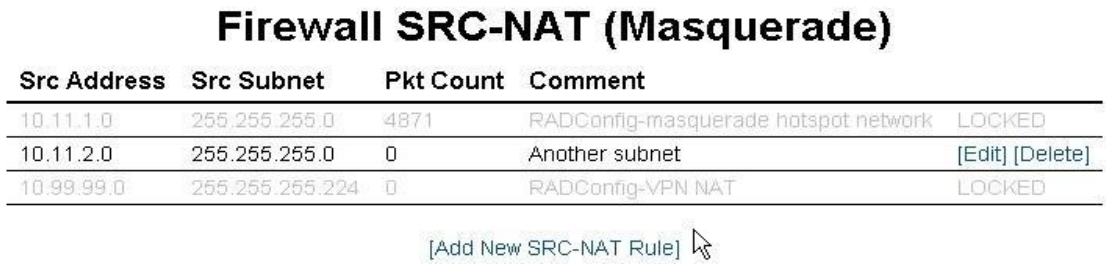
Copyright © 2021 Radius Gateway LLC. All rights reserved.



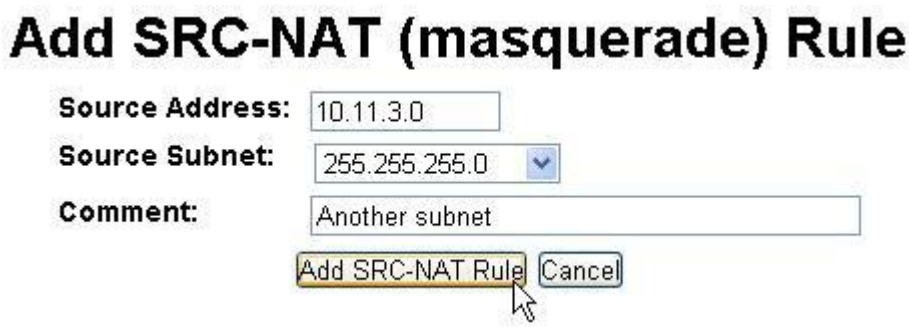

- **External Port —** The external port to bind to the external IP address.
- **Protocol** — Desired protocol (TCP or UDP).
- **Internal IP Address** — The internal IP address to map.
- **Internal Port** — The internal port to map.
- **Comment** — Human-readable comment for the destination NAT rule.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Source NAT (Advanced → NAT (SRC-NAT))**
Source NAT rules may be configured to NAT devices on a different subnet than the guest network has configured in the DHCP server settings.




To add a new source NAT entry, click the **Add New SRC-NAT Rule** link.

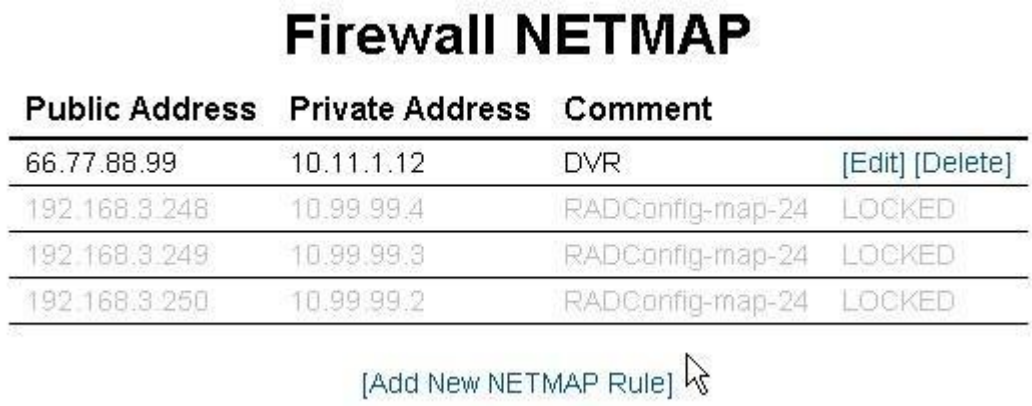



- **Source Address —** Network address for the new rule.
- **Source Subnet —** Subnet mask for the new rule.
- **Comment —** Human-readable comment for the source NAT rule.

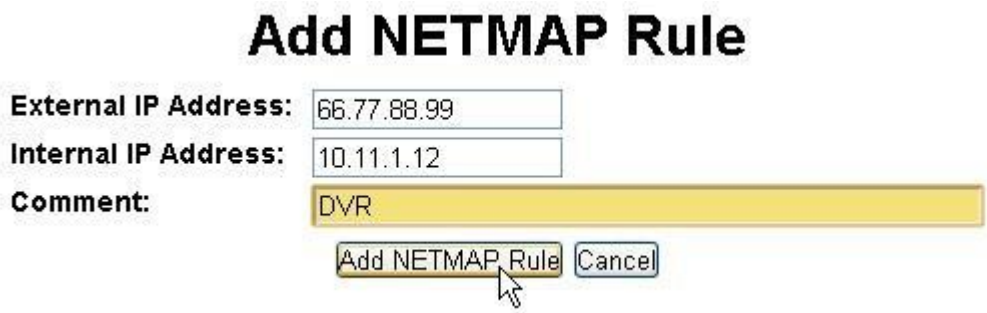
Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Firewall Netmap (Advanced → NAT (Netmap))**

The Firewall Netmap screen defines which public IP addresses are netmapped to which private IP addresses. This feature is useful when a device or workstation needs to be bypassed manually and mapped to a public IP address. Any VPN IP addresses defined in Guest Network →VPN Mappings are also visible here in read-only mode.



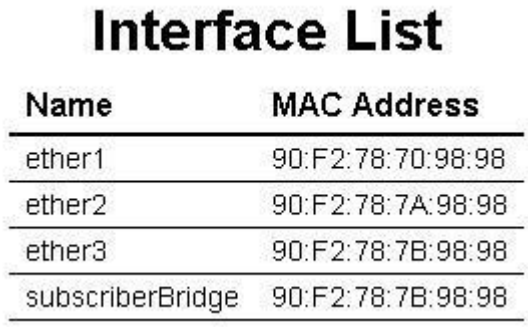

To create a new netmap rule, click the **Add New NETMAP Rule** link. Define the desired rule and click the **Add NETMAP Rule** button.




**NOTE:** When manually adding netmap entries, the public IP address should also be added to ether1 on the public Internet interface.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Interface List (Advanced → Interface List)**
The interface list displays the name and MAC address of each physical interface on the gateway.



Interface List

| Name | MAC Address |
|---|---|
| ether1 | 90:F2:78:70:98:98 |
| ether2 | 90:F2:78:7A:98:98 |
| ether3 | 90:F2:78:7B:98:98 |
| subscriberBridge | 90:F2:78:7B:98:98 |

**IP Addresses (Advanced → IP Addresses)**
The IP Address screen displays IP addresses in use by the gateway itself. Most addresses in this list are not editable because they are modified in other configuration screens. However, if additional IP addresses are needed on some interface(s), they may be added here.

IP Addresses

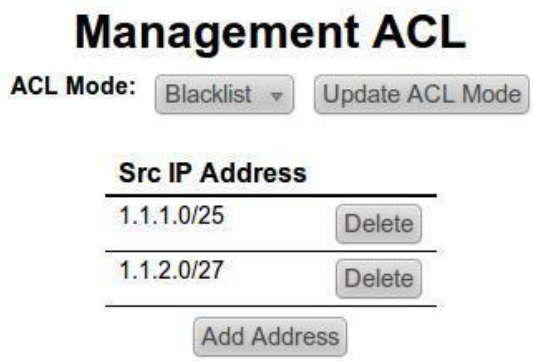
| Interface | IP Address | Subnet Mask | Comment |
|---|---|---|---|
| subscriberBridge | 10.11.1.1 | 255.255.255.0 | RADConfig-Private IP User Space |
| ether2 | 10.30.0.10 | 255.255.255.0 | RADConfig-LB Config Secondary |
| subscriberBridge | 10.99.99.1 | 255.255.255.224 | RADConfig-Public Pool IP |
| rgBridge | 10.255.255.253 | 255.255.255.252 | RADConfig-Web Server |
| ether1 | 192.168.3.102 | 255.255.255.0 | RADConfig-LB Config Primary |
| ether1 | 192.168.3.248 | 255.255.255.0 | RADConfig-map |
| ether1 | 192.168.3.249 | 255.255.255.0 | RADConfig-map |
| ether1 | 192.168.3.250 | 255.255.255.0 | RADConfig-map |

[Add New IP Address]

Copyright © 2021 Radius Gateway LLC. All rights reserved.

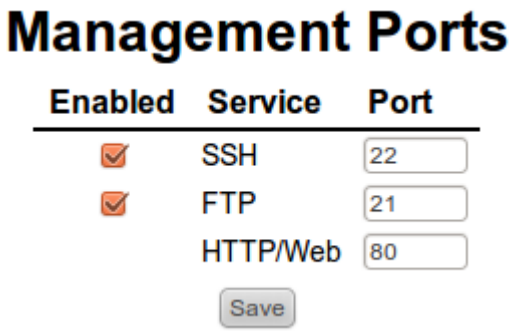
**Management ACL (Access Control List) (Advanced → Management ACL)**
The Management ACL list controls management access to the gateway by IP address. Two modes are available.

- **Allow All —** The allow all mode allows all IP addresses access to manage the gateway.
- **Blacklist** — The blacklist mode drops all management connections coming from the specified IP addresses in the Src IP Address list.




**IMPORTANT:** The guest network IP address range(s) should not be applied to the blacklist. This may cause guest network authentication to break.

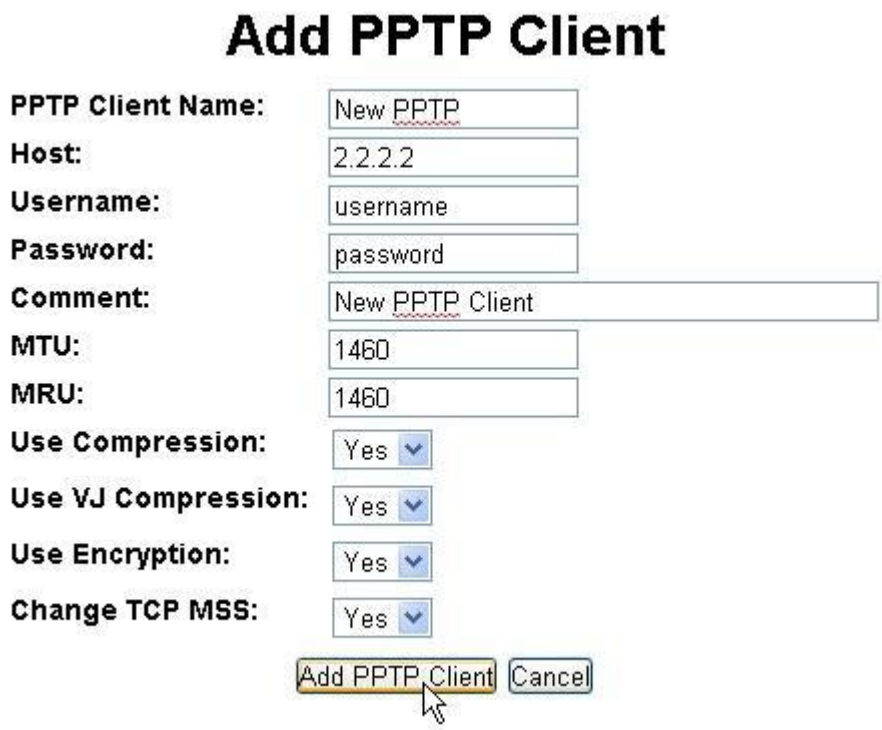
**Management Ports (Advanced → Management Ports)**
This screen controls which ports are open for remote management. The checkbox next to each service controls whether it is enabled or disabled.




Copyright © 2021 Radius Gateway LLC. All rights reserved.

**PPTP Clients (Advanced → PPTP Clients)**
The RADIUS gateway has the ability to connect to remote PPTP VPN servers.

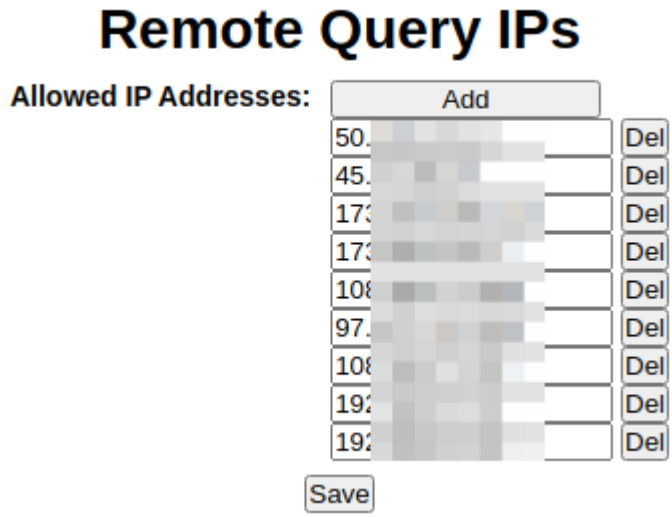
To add a new PPTP client, click the **Add New PPTP Client** link.




Copyright © 2021 Radius Gateway LLC. All rights reserved.

### Remote Query IPs (Advanced → Remote Query IPs)

The gateway supports some API calls. These calls are detailed in Appendix B: API. When using the API calls, the Remote Query IP page needs to be adjusted to reflect the source of the API calls.



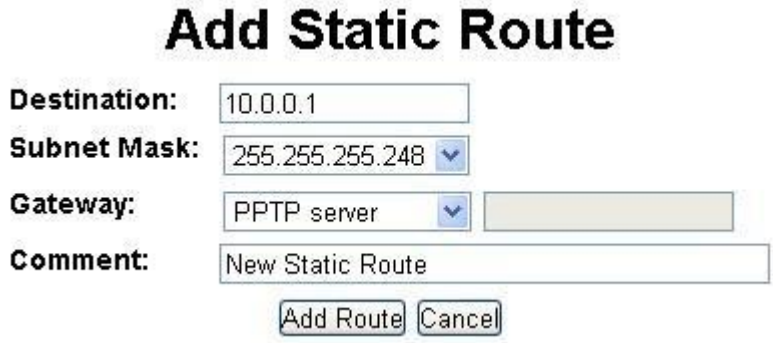

### SNMP (Advanced → SNMP)

Radius Gateway supports SNMP v1 protocol to read basic system information and port statistics. The standard RFC1213 mib file is compatible to read SNMP data from the gateway. SNMP is configured from the Advanced SNMP configuration screen.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**Static DNS (Advanced → Static DNS)**
Static DNS entries may be made on the gateway in order to define manually how users on the guest network resolve specific domain names. By default, the "login.radiusgateway.com" domain is defined to point to the internal web server. This feature may also be used to black-hole a specific domain for blocking purposes.

**Static Routes (Advanced → Static Routes)**
Static routes may be defined on the Static Routes screen. When adding new routes, a specific IP address or interface may be defined.




Copyright © 2021 Radius Gateway LLC. All rights reserved.

# CHAPTER 3: TROUBLESHOOTING

| Problem | Troubleshooting Steps |
|---|---|
| No lights on the gateway | Verify that the power is connected. |
| Unable to manage equipment that has been mapped | Verify that the equipment is programmed with the proper subnet mask and default gateway. |
| No login page is displayed to users on the guest network | By default, Radius Gateway is configured with authentication disabled on the guest network. Verify that an authentication method has been configured through the **Guest Network → Authentication** menu. |
| Unable to manage gateway remotely | Verify that the gateway is not double-NATed. See network diagram in Chapter 1. If it is double-NATed, ensure that the router facing the Internet is passing the necessary ports (port 80 TCP is required minimum). |
| Public IPs for VPN connections are not working | Verify that the ISP has routed the desired public IPs properly. If running failover or load balance mode, ensure that public IPs only reside on the primary connection (ether1). |

Copyright © 2021 Radius Gateway LLC. All rights reserved.

# APPENDIX A: SUPPORTED RADIUS ATTRIBUTES

Radius Gateway supports many standardized RADIUS attributes.

### *Access-Request*

- **Service-Type** — Always set to "Framed" (only for PPPs)
- **Framed-Protocol** — Always set to "PPP" (only for PPPs)
- **NAS-Identifier** — Gateway identity as set in **System → Identity**
- **NAS-IP-Address** — IP address of the gateway itself
- **NAS-Port** — Unique session ID
- **Acct-Session-Id** — Unique session ID
- **Calling-Station-Id** — Client MAC address in capital letters
- **Called-Station-Id** — Name of the gateway
- **Framed-IP-Address** — IP address of client
- **User-Name** — Client login name
- **User-Password** — PAP encrypted password

### *Access-Accept*

- **Framed-IP-Address** — IP address given to client. If address belongs to 127.0.0.0/8 or 224.0.0.0/3 networks, IP pool is used from the default profile to allocate client IP address. If Framed-IP-Address is specified, Framed-Pool is ignored.
- **Framed-Pool** — IP pool name (on the gateway) from which to get IP address for the client. Possible values are "subscriber-pool" or "subscriber-pool-public". An error will be generated if "subscriber-pool-public" is sent and there are no public VPN IP addresses defined. If **Framed-IP-Address** is specified, this attribute is ignored.
- **Idle-Timeout** — Client will be automatically logged out if they are idle for this time period (seconds).
- **Session-Timeout** — Client will be automatically logged out if they are online for this time period (seconds).
- **Framed-Route** — Routes to add on the server. Format is specified in RFC2865 (Ch. 5.22), can be specified as many times as needed.
- **Acct-Interim-Interval** — Interim-update for RADIUS client.
- **Ascend-Data-Rate** — Client **upload** rate limit (defined in bits per second). If Ascend-Xmit-Rate is not defined, this attribute will control both upload and download rate limit. This is 0 if unlimited.
- **Ascend-Xmit-Rate** — Client **download** rate limit (defined in bits per second). This is 0 if unlimited.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**NOTE** that the received attributes override the default ones (set in the default user profile), but if an attribute is not received from RADIUS server, the default one is to be used.

### *Accounting-Request*

The accounting request carries the same attributes as Access Request, plus the following:

- **Acct-Status-Type** — Start, Stop, or Interim-Update
- **Acct-Authentic** — Either authenticated by the RADIUS or Local authority
- **Class** — RADIUS server cookie, as received in Access-Accept
- **Acct-Delay-Time** — How long the gateway tried to send the Accounting-Request packet

### *Stop and Interim-Update Accounting-Request*

In addition to the accounting start request, the following messages will contain the following attributes:

- **Acct-Session-Time** — Connection uptime in seconds
- **Acct-Input-Octets** — Bytes received from the client
- **Acct-Input-Packets** — Number of packets received from the client
- **Acct-Output-Octets** — Bytes sent to the client
- **Acct-Output-Packets** — Number of packets sent to the client

### *Stop Accounting-Request*

These packets will, in addition to the Interim Update packets, have:

- **Acct-Terminate-Cause** — Session termination cause (see RFC2866 ch. 5.10)

Copyright © 2021 Radius Gateway LLC. All rights reserved.

# APPENDIX B: API

APIs are available to query/post to a PMS system (if the module is installed) and to manage the internal user database. These APIs are especially helpful when an external login page is configured. They are intended to be called in the background by a PHP, ASP, or similar scripting language via http query. These URLs are **not** intended to be called directly by guest network users.

## *PMS query/post*

**http://[ipaddress]/cgi-bin/query/pmsRoomName.cgi**

This URL may be used to query the PMS system for a room number and last name. Charges are **not** applied to the room as a result of a query.

This URL accepts the following parameters:

- roomNumber=[room number] REQUIRED
- lastName=[last name] REQUIRED
- xml=y OPTIONAL
  If the xml parameter is set to “y”, results are returned in XML format. If the xml parameter is set to “n” or otherwise not defined, the results are returned in a \n delimited URI format.

Return parameters:

- RoomNumber=[room number] — If the PMS system is unavailable, the RoomNumber parameter will be returned as “Unavailable”
- CreditLimit=[credit limit] — The credit limit of the guest.
- ReservationId=[reservation ID] — The reservation ID of the guest
- LastName=[last name] — The last name of the guest
- FirstName=[first name] — The first name of the guest
- error=[error string] — If the query results in an error, it will be passed in this field. The most common error is “Room Number or Last Name not found.”

Example:

http://1.1.1.1/cgi-bin/query/pmsRoomName.cgi?roomNumber=123&lastName=jones

Result:

RoomNumber=101&CreditLimit=1000.00&ReservationId=12345678&LastName=Jones&FirstName=David&error=

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**http://[ipaddress]/cgi-bin/query/pmsPostPayment.cgi**

This URL may be used to post a charge to a room.

This URL accepts the following parameters:

- roomNumber=[room number] REQUIRED
- lastName=[last name] REQUIRED
- amount=[amount to charge to room] REQUIRED
- xml=y OPTIONAL
  If the xml parameter is set to “y” results are returned in XML format. If the xml parameter is set to “n” or otherwise not defined, the results are returned in a \n delimited URI format.

Return parameters:

- result=[return result] — Return result of the PMS post request.
  - If set to 1, the post was successful.
  - If set to 0, the post was unsuccessful.
- error=[error string] — If the query results in an error, it will be passed in this field.
  - The most common error is “Room Number or Last Name not found.”
  - Another error that may be encountered is “Unable to verify payment. Please try again later.” This error typically means that the PMS was unavailable when the post was attempted.

Example (PMS charge success):

http://1.1.1.1/cgi-bin/query/pmsPostPayment.cgi?roomNumber=123&lastName=jones

Result:

result=1

Example (PMS charge fail):

http://1.1.1.1/cgi-bin/query/pmsPostPayment.cgi?roomNumber=999&lastName=nobody

Result:

result=0&error=Room%20Number%20or%20Last%20Name%20not%20found.

Example (PMS unavailable):

http://1.1.1.1/cgi-bin/query/pmsPostPayment.cgi?roomNumber=123&lastName=jones

Result:

result=0&error=Unable%20to%20verify%20payment.%20%20Please%20try%20again%20later.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

## *Internal User Database Management*

**http://[ipaddress]/cgi-bin/query/radiusUsers.cgi**

This URL may be used to manage the internal user database on the gateway. The main parameter used for each function is the *cmd* parameter.

*cmd* parameter

- *cmd=query*
  - Query a user or users
  - Parameters for query
    - username=[user] Optional user to search for. If not defined, it will return all available users on the gateway.
    - xml=y Optional parameter to return xml results. If xml is not defined, it will return results in a \n delimited URI format.
  - Returns available users in the selected format
- *cmd=add*
  - Add a new user
  - Parameters for add
    - username=[user] Account username. REQUIRED
    - password=[password] Account password. REQUIRED
    - firstName=[first name] First name. OPTIONAL
    - lastName=[last name] Last name. OPTIONAL
    - e-mail=[email address] Email address. OPTIONAL
    - userProfile=[name of user profile] User profile name to assign to the user. OPTIONAL
    - uptimeLimit=[uptime limit for account] Uptime limit (hhh:mm:ss format). OPTIONAL
    - comment=[comment string] Account comment
    - xml=y Optional parameter to return xml results. If xml is not defined, it will return results in URI format
  - If add is successful, the return result parameter is set to "ok".
  - If add is unsuccessful, the error parameter is set to indicate what the error is.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

- *cmd=update*
    - Update user account
        - username=[user] Account user name. REQUIRED
        - password=[password] Account password. OPTIONAL
        - firstName=[first name] First name. OPTIONAL
        - lastName=[last name] Last name. OPTIONAL
        - email=[email address] Email address. OPTIONAL
        - userProfile=[name of user profile] User profile name to assign to the user. OPTIONAL
        - uptimeLimit=[uptime limit for account] Uptime limit (hhh:mm:ss format). OPTIONAL
        - comment=[comment string] Account comment
        - xml=y Optional parameter to return xml results. If xml is not defined, it will return results in URI format.
    - If update is successful, the result parameter is set to "ok".
    - If update is unsuccessful, the error parameter is set to indicate what the error is.
- *cmd=delete*
    - Delete user account
        - username=[user] Account username to delete. REQUIRED
    - If the delete is successful, the result parameter is set to "ok".
    - If the delete is unsuccessful, the error parameter is set to indicate what the error is.
    - Delete function will log out the username if the username is currently logged in.

Copyright © 2021 Radius Gateway LLC. All rights reserved.

**wget examples**

- query
  - wget -O — "http://1.1.1.1/cgi-bin/query/radiusUsers.cgi?cmd=query&username=user" 2>/dev/null
- add user
  - wget -O — "http://1.1.1.1/cgi-bin/query/radiusUsers.cgi?cmd=add&username=newUser&password=pass&firstName=brandon&lastName=miller&userProfile=testProfile&comment=newComment" 2>/dev/null
- update user
  - wget -O — "http://1.1.1.1/cgi-bin/query/radiusUsers.cgi?cmd=update&username=newUser&password=newPass&comment=anotherNewComment" 2>/dev/null
- delete user
  - wget -O — "http://1.1.1.1/cgi-bin/query/radiusUsers.cgi?cmd=delete&username=newUser" 2>/dev/null

**PHP Hint:** In PHP, the CURL function library is recommended for these http calls (http://php.net/manual/en/book.curl.php). It is really good at calling external URLs and dealing with them. Also, for the URI returns, the parse_url function is very helpful (http://php.net/manual/en/function.parse-url.php).

Copyright © 2021 Radius Gateway LLC. All rights reserved.

# APPENDIX C: IPV4 SUBNET MASK TO CIDR NETWORK NUMBER CONVERSION

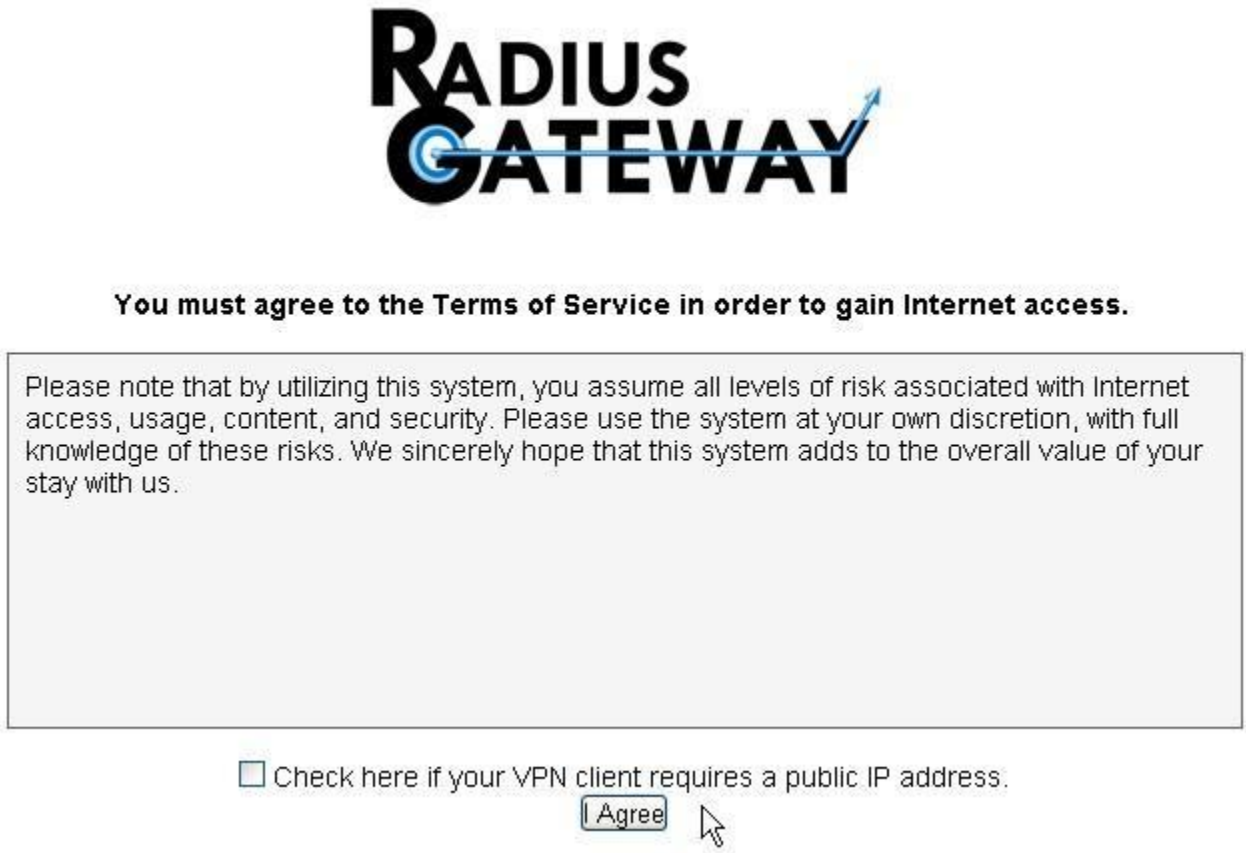
An online CIDR calculator is also available at http://www.subnet-calculator.com/cidr.php

| CIDR Notation: | Total number of addresses: | Network Mask: | Description: |
|---|---|---|---|
| /9 | 8,388,608 | 255.128.0.0 | 128 /16 nets |
| /10 | 4,194,304 | 255.192.0.0 | 64 /16 nets |
| /11 | 2,097,152 | 255.224.0.0 | 32 /16 nets |
| /12 | 1,048,576 | 255.240.0.0 | 16 /16 nets |
| /13 | 524,288 | 255.248.0.0 | 8 /16 nets |
| /14 | 262,144 | 255.252.0.0 | 4 /16 nets |
| /15 | 131.072 | 255.254.0.0 | 2 /16 nets |
| /16 | 65,536 | 255.255.0.0 | 1 /16 |
| /17 | 32,768 | 255.255.128.0 | 128 /24 nets |
| /18 | 16,384 | 255.255.192.0 | 64 /24 nets |
| /19 | 8,192 | 255.255.224.0 | 32 /24 nets |
| /20 | 4,096 | 255.255.240.0 | 16 /24 nets |
| /21 | 2,048 | 255.255.248.0 | 8 /24 nets |
| /22 | 1,024 | 255.255.252.0 | 4 /24 nets |
| /23 | 512 | 255.255.254.0 | 2 /24 nets |
| /24 | 256 | 255.255.255.0 | 1 /24 |
| /25 | 128 | 255.255.255.128 | Half of a /24 |
| /26 | 64 | 255.255.255.192 | Fourth of a /24 |
| /27 | 32 | 255.255.255.224 | Eighth of a /24 |
| /28 | 16 | 255.255.255.240 | 1/16th of a /24 |
| /29 | 8 | 255.255.255.248 | 5 Usable addresses |
| /30 | 4 | 255.255.255.252 | 1 Usable address |
| /31 | 2 | 255.255.255.254 | Unusable |
| /32 | 1 | 255.255.255.255 | Single host |

Copyright © 2021 Radius Gateway LLC. All rights reserved.

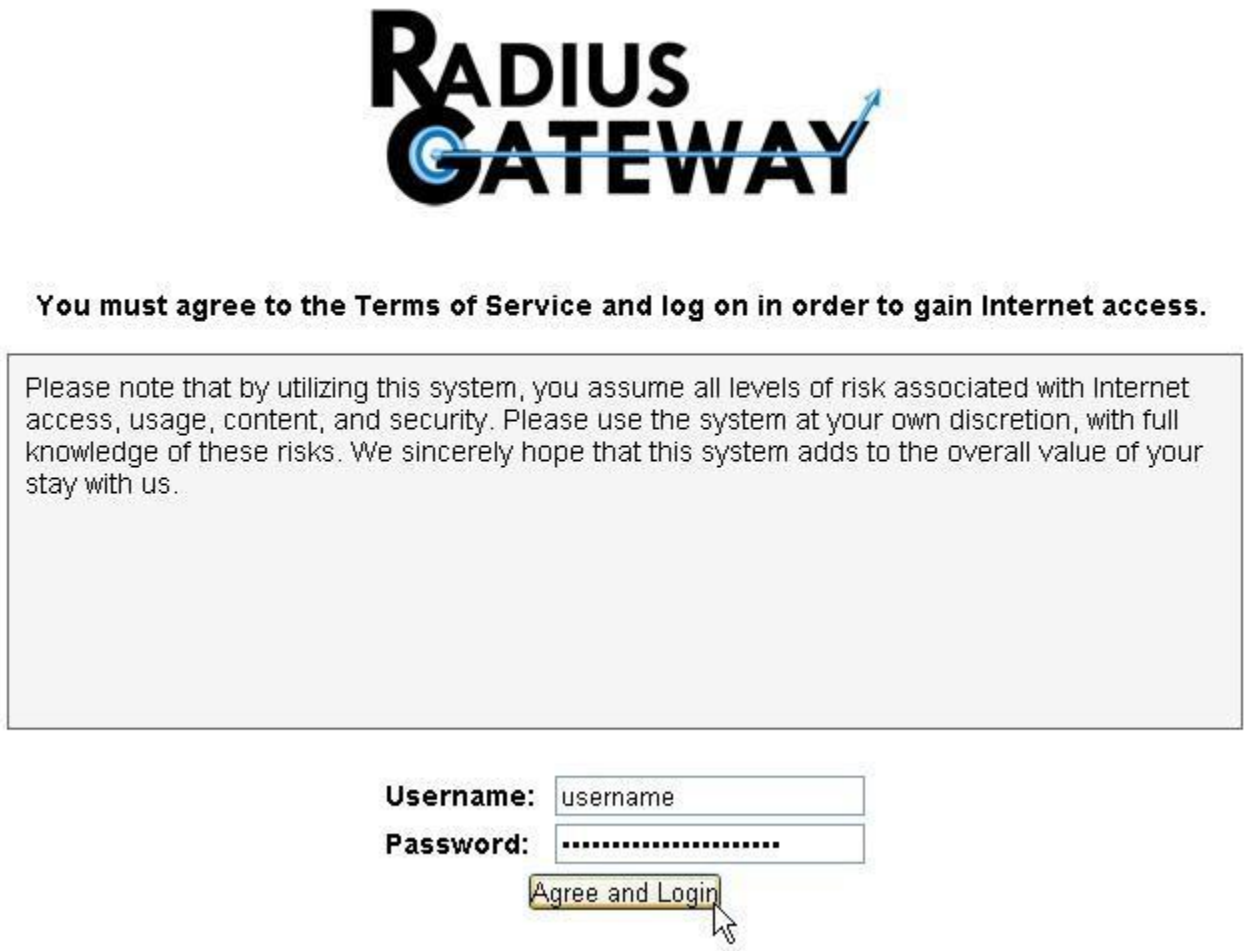
# APPENDIX D: GUEST NETWORK LOGIN PAGE SCREENSHOTS

## Standard Accept Button




Copyright © 2021 Radius Gateway LLC. All rights reserved.

## Standard Login Page




Copyright © 2021 Radius Gateway LLC. All rights reserved.

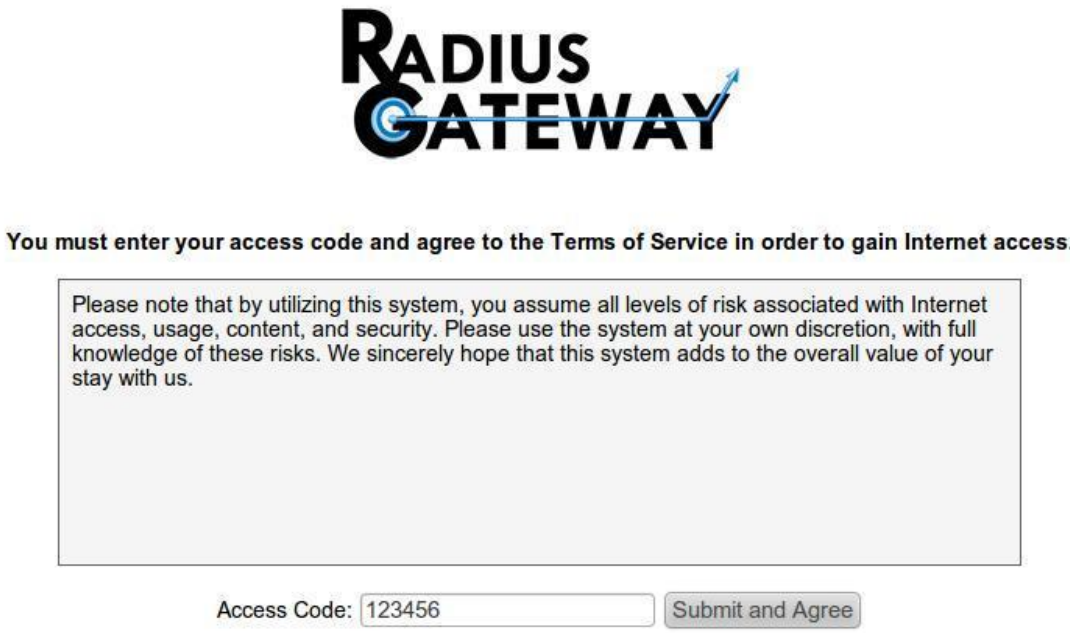
## PayPal Login Page

Copyright © 2021 Radius Gateway LLC. All rights reserved.

## PayPal Sign-up Pages

Copyright © 2021 Radius Gateway LLC. All rights reserved.

## Weekly Code




Copyright © 2021 Radius Gateway LLC. All rights reserved.