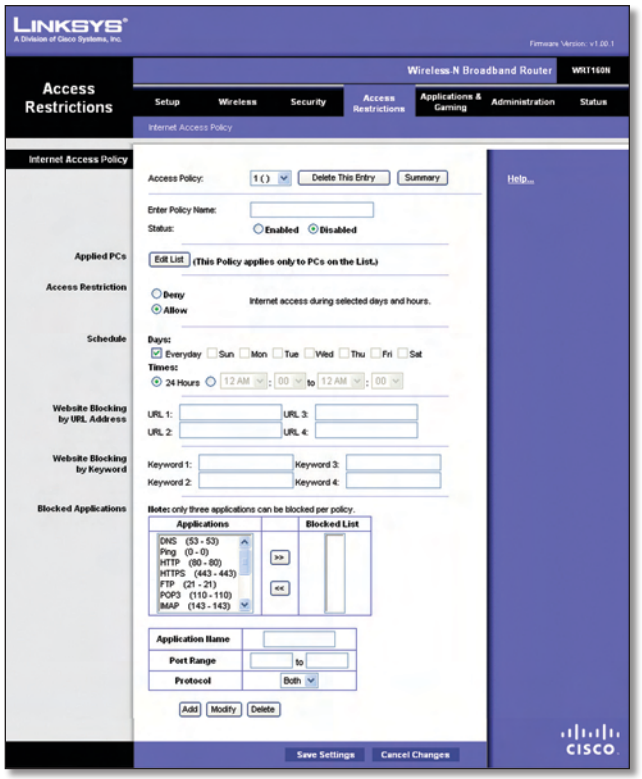


Access Restrictions > Internet Access

Internet Access Policy

Access Policy Access can be managed by a policy. Use the settings on this screen to establish an access policy (after **Save Settings** is clicked). Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click **Delete This Policy**. To view all the policies, click **Summary**.

Summary

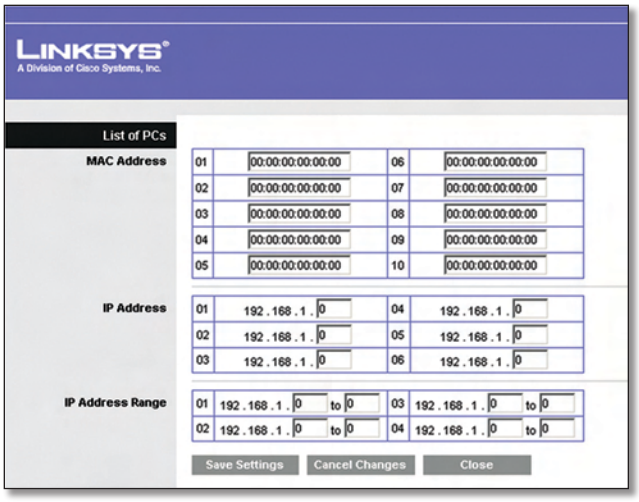
The policies are listed with the following information: No., Policy Name, Access, Days, Time, and status (Enabled). To enable a policy, select **Enabled**. To delete a policy, click **Delete**. Click **Save Settings** to save your changes, or click **Cancel Changes** to cancel your changes. To return to the *Internet Access Policy* screen, click **Close**.

Summary

Status Policies are disabled by default. To enable a policy, select the policy number from the drop-down menu, and select **Enabled**.

To create a policy, follow steps 1-11. Repeat these steps to create additional policies, one at a time.

1. Select a number from the *Access Policy* drop-down menu.
2. Enter a Policy Name in the field provided.
3. To enable this policy, select **Enabled**.
4. Click **Edit List** to select which PCs will be affected by the policy. The *List of PCs* screen appears. You can select a PC by MAC address or IP address. You can also enter a range of IP addresses if you want this policy to affect a group of PCs. After making your changes, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Then click **Close**.



List of PCs

5. Select the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen.
6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.
7. You can block websites with specific URL addresses. Enter each URL in a separate *URL* field.
8. You can also block websites using specific keywords. Enter each keyword in a separate *Keyword* field.

9. You can filter access to various services accessed over the Internet, such as FTP or telnet. (You can block up to three applications per policy.)

   From the Applications list, select the application you want to block. Then click the >> button to move it to the Blocked List. To remove an application from the Blocked List, select it and click the << button.

10. If the application you want to block is not listed or you want to edit a service's settings, enter the application's name in the *Application Name* field. Enter its range in the **Port Range** fields. Select its protocol from the *Protocol* drop-down menu. Then click **Add**.

    To modify a service, select it from the Application list. Change its name, port range, and/or protocol setting. Then click **Modify**.

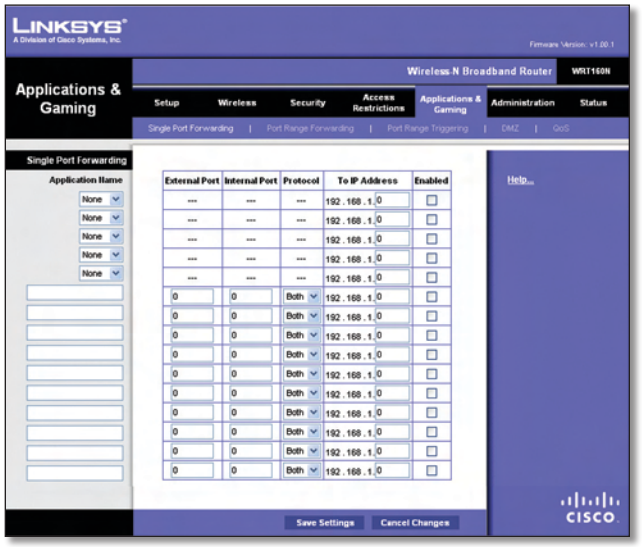
    To delete a service, select it from the Application list. Then click **Delete**.

11. Click **Save Settings** to save the policy's settings. To cancel the policy's settings, click **Cancel Changes**.

Applications and Gaming > Single Port Forwarding

The *Single Port Forwarding* screen allows you to customize port services for common applications on this screen.

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the *Basic Setup* screen).



Applications and Gaming > Single Port Forwarding

Single Port Forwarding

Common applications are available for the first five entries. Select the appropriate application. Then enter the IP address of the server that should receive these requests. Select **Enabled** to activate this entry.

For additional applications, complete the following fields:

Application Name Enter the name you wish to give the application. Each name can be up to 12 characters.

External Port Enter the external port number used by the server or Internet application. Check with the Internet application documentation for more information.

Internal Port Enter the internal port number used by the server or Internet application. Check with the Internet application documentation for more information.

Protocol Select the protocol used for this application, either **TCP** or **UDP**, or **Both**.

To IP Address For each application, enter the IP address of the PC that should receive the requests. If you assigned a static IP address to the PC, then you can click **DHCP Reservation** on the *Basic Setup* screen to look up its static IP address.

Enabled For each application, select **Enabled** to enable port forwarding.

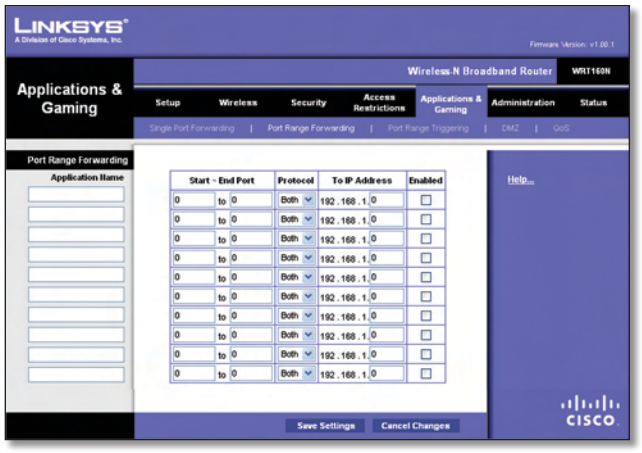
Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Applications and Gaming > Port Range Forwarding

The *Port Range Forwarding* screen allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the *Basic Setup* screen).

If you need to forward all ports to one computer, click the **DMZ** tab.



Applications and Gaming > Port Range Forwarding

Port Range Forwarding

To forward a port, enter the information on each line for the criteria required.

Application Name In this field, enter the name you wish to give the application. Each name can be up to 12 characters.

Start~End Port Enter the number or range of port(s) used by the server or Internet applications. Check with the Internet application documentation for more information.

Protocol Select the protocol used for this application, either **TCP** or **UDP**, or **Both**.

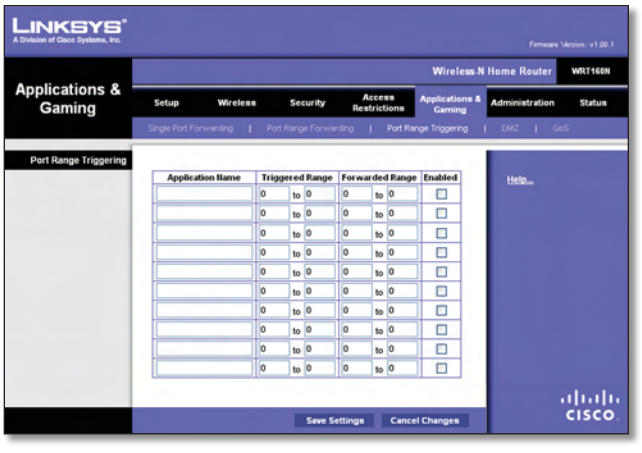
To IP Address For each application, enter the IP address of the PC running the specific application. If you assigned a static IP address to the PC, then you can click **DHCP Reservation** on the *Basic Setup* screen to look up its static IP address.

Enabled Select **Enabled** to enable port forwarding for the applications you have defined.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Applications & Gaming > Port Range Triggering

The *Port Range Triggering* screen allows the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.



Applications and Gaming > Port Range Triggering

Port Range Triggering

Application Name Enter the application name of the trigger.

Triggered Range For each application, enter the starting and ending port numbers of the triggered port number range. Check with the Internet application documentation for the port number(s) needed.

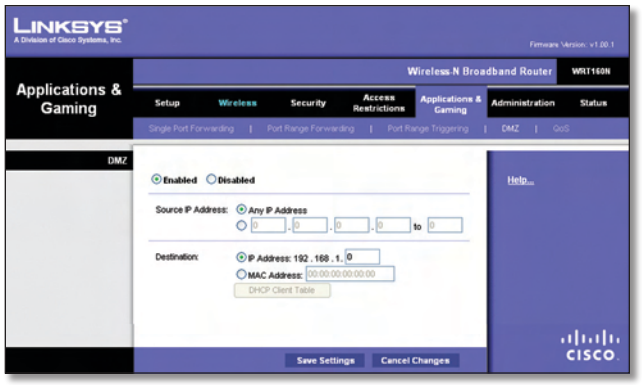
Forwarded Range For each application, enter the starting and ending port numbers of the forwarded port number range. Check with the Internet application documentation for the port number(s) needed.

Enabled Select **Enabled** to enable port triggering for the applications you have defined.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Applications and Gaming > DMZ

The DMZ feature allows one network computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet.



Applications and Gaming > DMZ

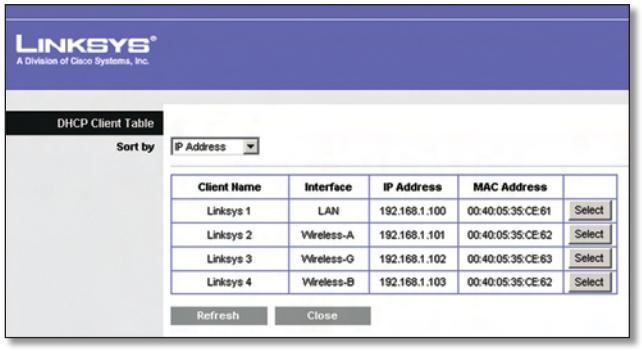
DMZ

Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

Enabled/Disabled To disable DMZ hosting, select **Disabled**. To expose one PC, select **Enabled**. Then configure the following settings:

Source IP Address If you want any IP address to be the source, select **Any IP Address**. If you want to specify an IP address or range of IP addresses as the designated source, select and complete the IP address range fields.

Destination If you want to specify the DMZ host by IP address, select **IP Address** and enter the IP address in the field provided. If you want to specify the DMZ host by MAC address, select **MAC Address** and enter the MAC address in the field provided. To retrieve this information, click **DHCP Client Table**.



DMZ > DHCP Client Table

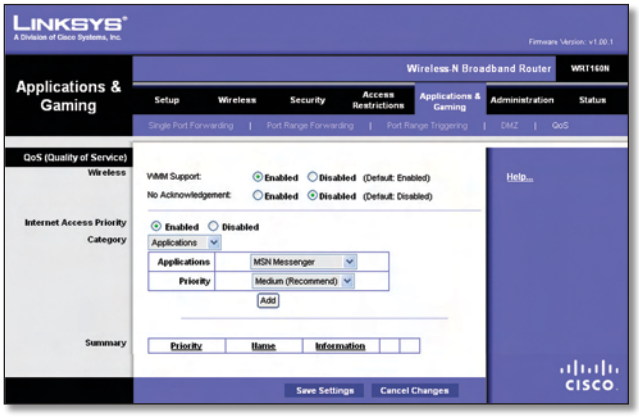
DHCP Client Table

The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the Router. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Expired Time (how much time is left for the current IP address). To select a DHCP client, click **Select**. To retrieve the most up-to-date information, click **Refresh**. To exit this screen and return to the *DMZ* screen, click **Close**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Applications and Gaming > QoS

Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing.



Applications and Gaming > QoS

QoS (Quality of Service)

Wireless

You can configure the support and No Acknowledgement settings in this section.

WMM Support If you have other devices that support Wi-Fi Multimedia (WMM) on your network, keep the default, **Enabled**. Otherwise, select **Disabled**.

No Acknowledgement If you want to disable the Router's Acknowledgement feature, so the Router will not re-send data if an error occurs, then select **Enabled**. Otherwise, keep the default, **Disabled**.

Internet Access Priority

In this section, you can set the bandwidth priority for a variety of applications and devices. There are four levels priority: High, Medium, Normal, or Low. When you set priority, do not set all applications to High, because this will defeat the purpose of allocating the available bandwidth. If you want to select below normal bandwidth, select Low. Depending on the application, a few attempts may be needed to set the appropriate bandwidth priority.

Enabled/Disabled To use the QoS policies you have set, keep the default, **Enabled**. Otherwise, select **Disabled**.

Category

There are four categories available. Select one of the following: **Applications**, **Online Games**, **MAC Address**, **Ethernet Port**, or **Voice Device**. Proceed to the instructions for your selection.

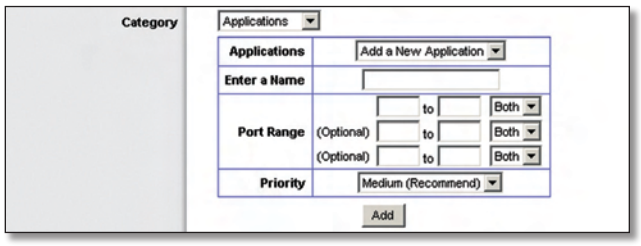
Applications

Applications Select the appropriate application. If you select Add a New Application, follow the Add a New Application instructions.

Priority Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Add a New Application



QoS > Add a New Application

Enter a Name Enter any name to indicate the name of the entry.

Port Range Enter the port range that the application will be using. For example, if you want to allocate bandwidth for FTP, you can enter 21-21. If you need services for an application that uses from 1000 to 1250, you enter 1000-1250 as your settings. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535. Check your application's documentation for details on the service ports used.

Select the protocol **TCP** or **UDP**, or select **Both**.

Priority Select the appropriate priority: **High**, **Medium (Recommend)**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Online Games

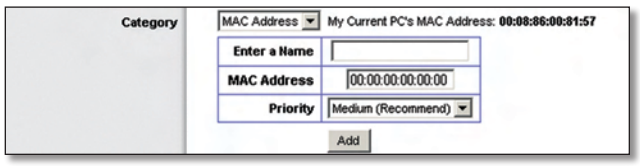
QoS > Online Games

Games Select the appropriate game.

Priority Select the appropriate priority: **High**, **Medium (Recommend)**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

MAC Address



QoS > MAC Address

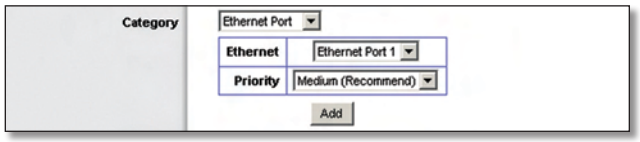
Enter a Name Enter a name for your device.

MAC Address Enter the MAC address of your device.

Priority Select the appropriate priority: **High**, **Medium (Recommend)**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Ethernet Port



QoS > Ethernet Port

Ethernet Select the appropriate Ethernet port.

Priority Select the appropriate priority: **High**, **Medium (Recommend)**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Voice Device

QoS > Voice Device

Enter a Name Enter a name for your voice device.

MAC Address Enter the MAC address of your voice device.

Priority Select the appropriate priority: **High (Recommend)**, **Medium**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.