Chapter 5
Content Filtering

This chapter describes how to use the content filtering features of the RangeMax 240 Wireless Router WPNT834 to protect your network. These features can be found by clicking on the **Content Filtering** heading in the main menu of the browser interface.

Content Filtering Overview

The RangeMax 240 Wireless Router WPNT834 provides you with Web content filtering options, plus browser activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based on time of day, Web addresses and Web address keywords. You can also block Internet access by applications and services, such as chat or games.

To configure these features of your router, click on the subheadings under the **Content Filtering** heading in the main menu of the browser interface. The subheadings are described below:

Blocking Access to Internet Sites

The WPNT834 router allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list. The Block Sites menu is shown in the figure below:

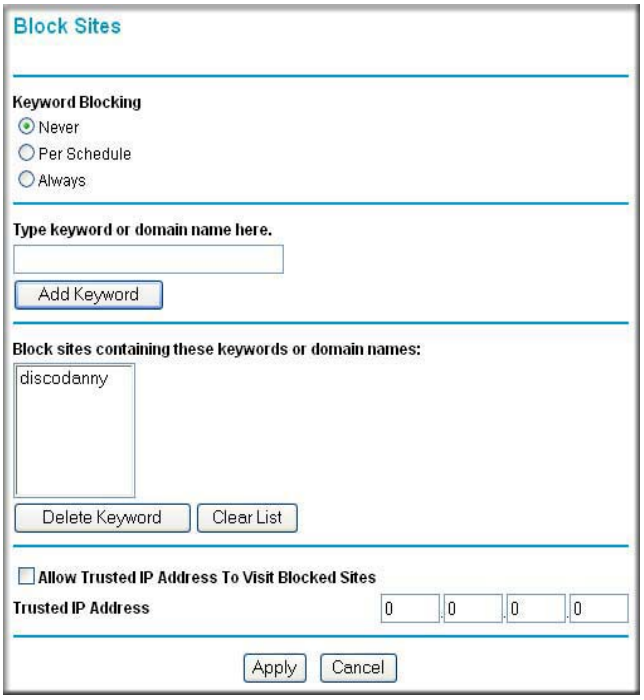

Figure 5-1

To enable keyword blocking, select either **Per Schedule** or **Always**, then click **Apply**. If you want to block by schedule, be sure to specify a time period in the Schedule menu. For scheduling, see "Scheduling When Blocking Will Be Enforced" on page 5-5.

To add a keyword or domain, type it in the Keyword box, click **Add Keyword**, then click **Apply**.

To delete a keyword or domain, select it from the list, click **Delete Keyword**, then click **Apply**.

Keyword application examples:

- If the keyword "XXX" is specified, the URL <http://www.badstuff.com/xxx.html> is blocked.
- If the keyword ".com" is specified, only Web sites with other domain suffixes (such as .edu or .gov) can be viewed.

- If you wish to block all Internet browsing access during a scheduled period, enter the keyword "." and set the schedule in the Schedule menu.

To specify a Trusted User, enter that computer's IP address in the Trusted User box and click **Apply**.

You may specify one Trusted User, which is a computer that is exempt from blocking and logging. Since the Trusted User is identified by IP address, you should configure that computer with a fixed IP address.

Blocking Access to Internet Services

The WPNT834 router allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. The Block Services menu is shown below:

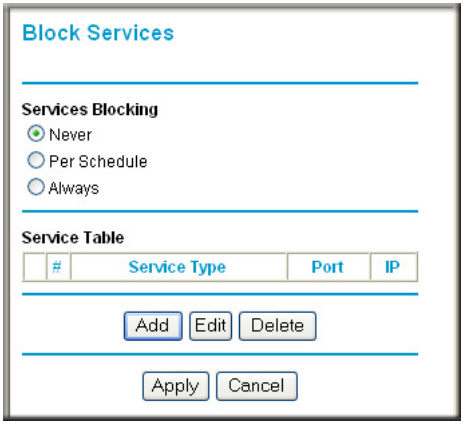

Figure 5-2

Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on your network sends a request for service to a server computer on the Internet, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

To enable service blocking, select either **Per Schedule** or **Always**, then click **Apply**. If you want to block by schedule, be sure to specify a time period in the Schedule menu. For scheduling, see "Scheduling When Blocking Will Be Enforced" on page 5-5.

To specify a service for blocking, click **Add**. The Block Services Setup menu appears, as shown below:

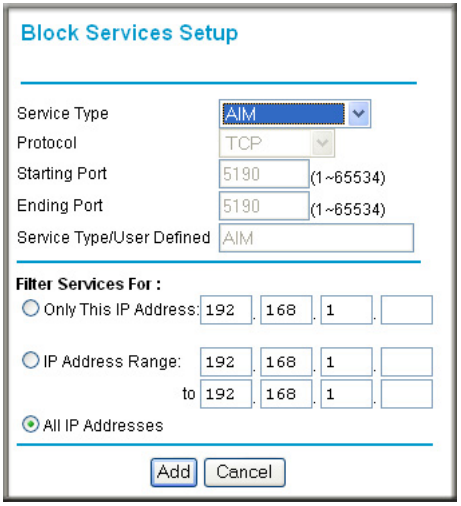

Figure 5-3

From the **Service Type** list, select the application or service to be allowed or blocked. The list already displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select **User Defined**.

Configuring a User Defined Service

To define a service, first you must determine which port number or range of numbers is used by the application. The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, “Assigned Numbers.” Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. This information can usually be determined by contacting the publisher of the application or from user groups of newsgroups.

Enter the Starting Port and Ending Port numbers. If the application uses a single port number, enter that number in both boxes.

If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **Both**.

Blocking Services by IP Address Range

Under “Filter Services For”, you can block the specified service for a single computer, a range of computers (having consecutive IP addresses), or all computers on your network.

Scheduling When Blocking Will Be Enforced

The WPNT834 router allows you to specify when blocking is enforced. The Schedule menu is shown below:

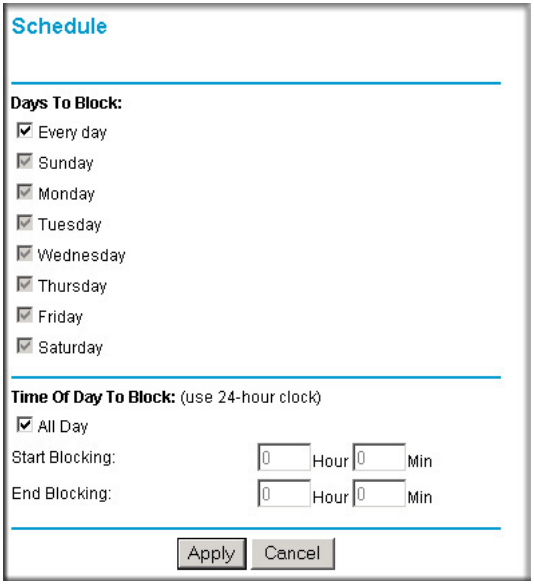

Figure 5-4

Use this schedule for blocking content.

- Days to Block. Select days to block by checking the appropriate boxes. Select **Every day** to check the boxes for all days. Click **Apply**.
- Time of Day to Block. Select a start and end time in 24-hour format. Select **All day** for 24-hour blocking. Click **Apply**.

Be sure to select your Time Zone in the E-Mail menu.

Viewing Logs of Web Access or Attempted Web Access

The log is a detailed record of the Web sites you have accessed or attempted to access. Up to 128 entries are stored in the log. Log entries only appear when keyword blocking is enabled, and no log entries are made for the Trusted User. An example is shown below:

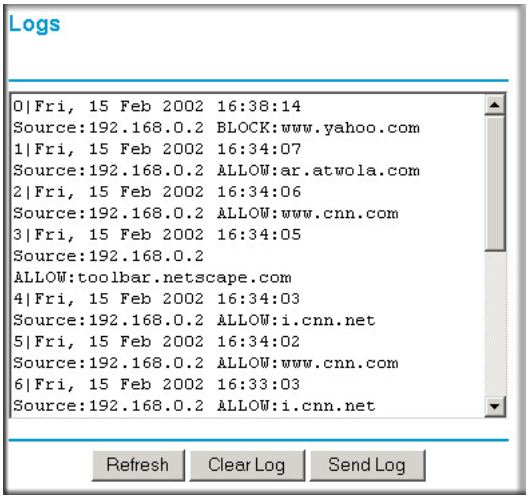

Figure 5-5

Log entries are described in the following table.

Table 5-1. Log entry descriptions

Field	Description
Date and Time	The date and time the log entry was recorded.
Source IP	The IP address of the initiating device for this log entry.
Target address	The name or IP address of the Web site or newsgroup visited or attempted to access.
Action	This field displays whether the access was blocked or allowed.

Log action buttons are described in the following table.

Table 5-2. Log action buttons

Field	Description
Refresh	Click this button to refresh the log screen.
Clear Log	Click this button to clear the log entries.
Send Log	Click this button to E-mail the log immediately.

Configuring E-Mail Alert and Web Access Log Notifications

In order to receive logs and alerts by E-mail, you must provide your E-mail information in the E-Mail menu, shown below:

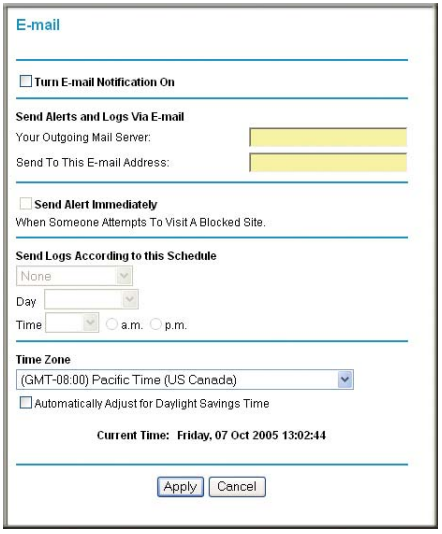

Figure 5-6

- Turn e-mail notification on.
  Check this box if you wish to receive e-mail logs and alerts from the router.
- Your outgoing mail server .
  Enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. If you leave this box blank, log and alert messages will not be sent via e-mail.

- Send to this e-mail address .
  Enter the e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via e-mail.

You can specify that logs are automatically sent to the specified e-mail address with these options:

- Send alert immediately.
  Check this box if you would like immediate notification of attempted access to a blocked site.
- Send logs according to this schedule
  Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
  - Day for sending log.
    Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.
  - Time for sending log .
    Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

  If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer may fill up. In this case, the router overwrites the log and discards its contents.

The WPNT834 router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. In order to localize the time for your log entries, you must specify your Time Zone:

- Time Zone.
  Select your local time zone. This setting is used for the blocking schedule and for time-stamping log entries.
- Adjust for Daylight Savings Time.
  Check this box if your time zone is currently under daylight savings time.