**Figure 77** Internet Connection Properties: Advanced Settings

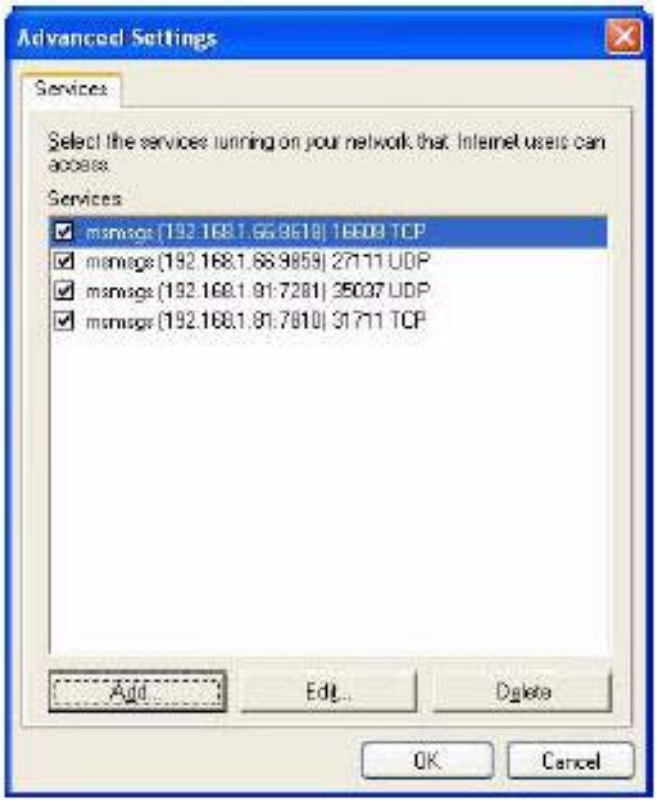
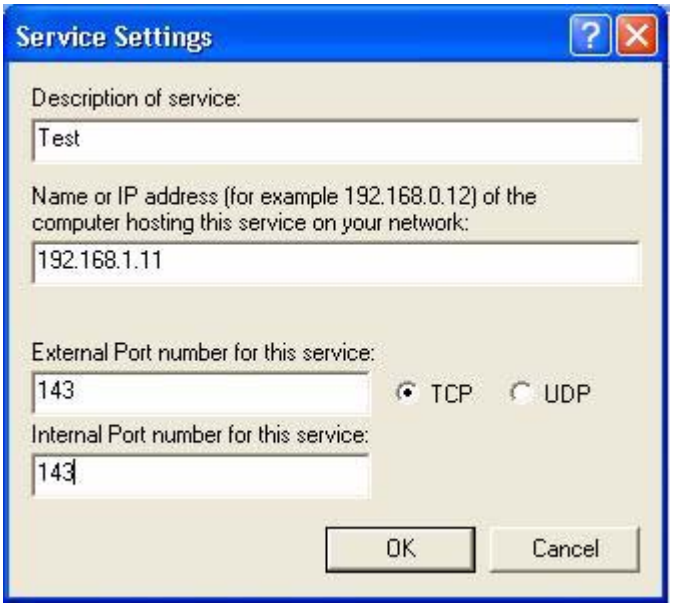



**Figure 78** Internet Connection Properties: Advanced Settings: Add




5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

**Figure 79** System Tray Icon


7 Double-click on the icon to display your current Internet connection status.

**Figure 80** Internet Connection Status


### Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the Prestige without finding out the IP address of the Prestige first. This comes helpful if you do not know the IP address of the Prestige.

Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

**Figure 81** Network Connections


4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your Prestige and select **Invoke**. The web configurator login screen displays.

**Figure 82** Network Connections: My Network Places


**6** Right-click on the icon for your Prestige and select **Properties**. A properties window displays with basic information about the Prestige.

**Figure 83** Network Connections: My Network Places: Properties: Example

# CHAPTER 15
# Logs Screens

This chapter contains information about configuring general log settings and viewing the Prestige's logs. Refer to the appendix for example log message explanations.

## 15.1 Logs Overview

The web configurator allows you to choose which categories of events and/or alerts to have the Prestige log and then display the logs or have the Prestige send them to an administrator (as e-mail) or to a syslog server.

### 15.1.1 Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

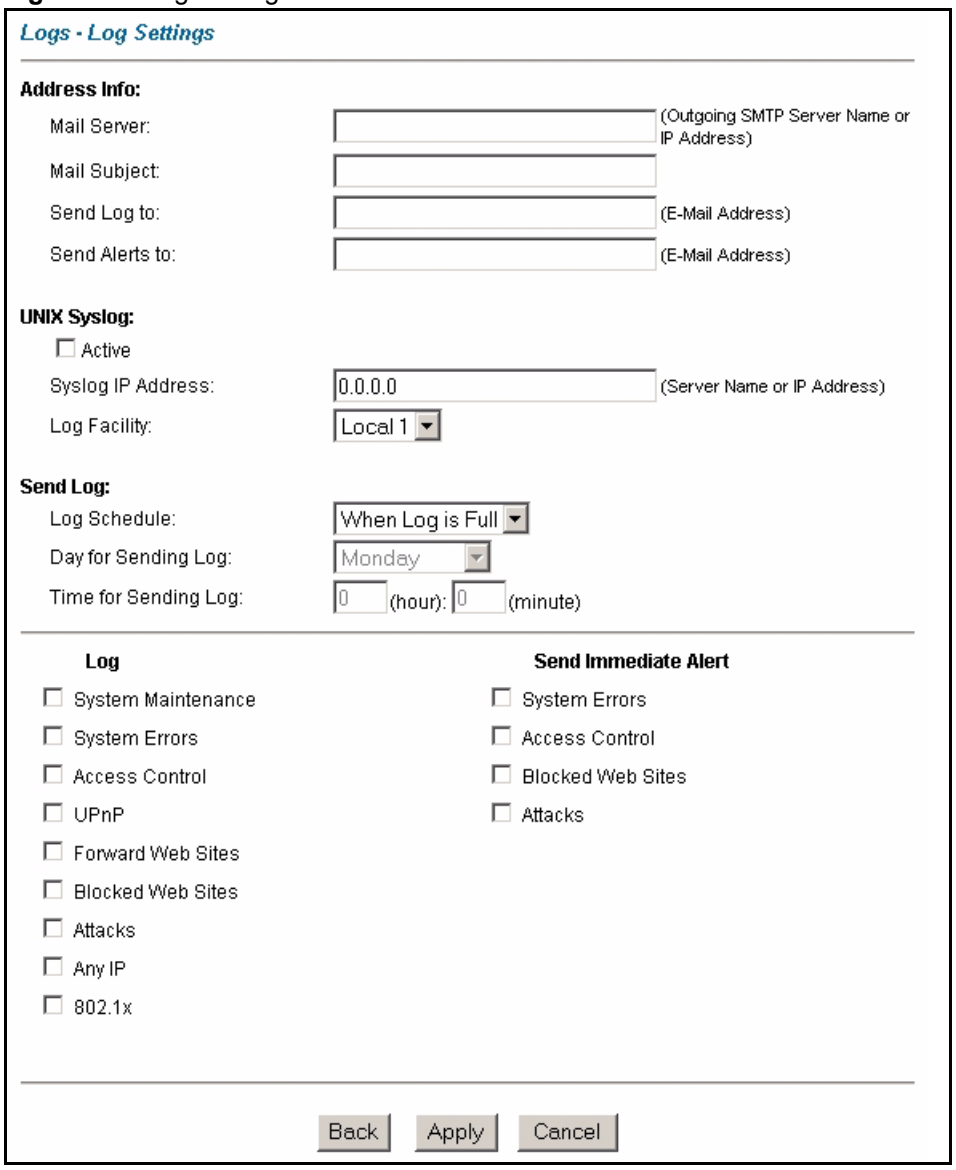
## 15.2 Configuring Log Settings

Use the **Log Settings** screen to configure to where the Prestige is to send logs; the schedule for when the Prestige is to send the logs and which logs and/or immediate alerts the Prestige is to record. See Section 15.1 on page 176 for more information.

To change your Prestige's log settings, click **Logs**, then the **Log Settings**. The screen appears as shown.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full. Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

**Figure 84** Log Settings




The following table describes the fields in this screen.

**Table 51** Log Settings

| LABEL | DESCRIPTION |
|---|---|
| Address Info | |
| Mail Server | Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail. |
| Mail Subject | Type a title that you want to be in the subject line of the log e-mail message that the Prestige sends. |
| Send log to | Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail. |

**Table 51** Log Settings

| LABEL | DESCRIPTION |
|---|---|
| Send alerts to | Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail. |
| UNIX Syslog | Syslog logging sends a log to an external syslog server used to store logs. |
| Active | Click **Active** to enable syslog logging. |
| Syslog IP Address | Enter the server name or IP address of the syslog server that will log the selected categories of logs. |
| Log Facility | Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| Send Log | |
| Log Schedule | This drop-down menu is used to configure the frequency of log messages being sent as E-mail:<br>• Daily<br>• Weekly<br>• Hourly<br>• When Log is Full<br>• None.<br>If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent |
| Day for Sending Log | Use the drop down list box to select which day of the week to send the logs. |
| Time for Sending Log | Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs. |
| Log | Select the categories of logs that you want to record. Logs include alerts. |
| Send Immediate Alert | Select the categories of alerts for which you want the Prestige to instantly e-mail alerts to the e-mail address specified in the **Send Alerts To** field. |
| Back | Click **Back** to return to the previous screen. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to return to the previously saved settings. |

## 15.3 Displaying the Logs

Click **Logs** and then **View Log** to open the **View Logs** screen. Use the **View Logs** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 15.2 on page 176).

Log entries in red indicate alerts. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

**Figure 85** View Logs


The following table describes the fields in this screen.

**Table 52** View Logs

| LABEL | DESCRIPTION |
|---|---|
| Display | The categories that you select in the **Log Settings** screen display in the drop-down list box.<br>Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page. |
| Time | This field displays the time the log was recorded. |
| Message | This field states the reason for the log. |
| Source | This field lists the source IP address and the port number of the incoming packet. |
| Destination | This field lists the destination IP address and the port number of the incoming packet. |
| Notes | This field displays additional information about the log entry. |
| Back | Click **Back** to return to the previous screen |
| Email Log Now | Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **Address Info** fields in **Log Settings**). |
| Refresh | Click **Refresh** to renew the log screen. |
| Clear Log | Click **Clear Log** to delete all the logs. |

# 15.4 SMTP Error Messages

If there are difficulties in sending e-mail the following error messages appear.

E-mail error messages appear in SMT menu 24.3.1 as "SMTP action request failed. ret= ??". The "??"are described in the following table.

**Table 53** SMTP Error Messages

| |
|---|
| -1 means Prestige out of socket |
| -2 means tcp SYN fail |
| -3 means smtp server OK fail |
| -4 means HELO fail |
| -5 means MAIL FROM fail |

**Table 53** SMTP Error Messages

| |
|---|
| -6 means RCPT TO fail |
| -7 means DATA fail |
| -8 means mail data send fail |

## 15.4.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- "`End of Log`" message shows that a complete log has been sent.

**Figure 86** E-mail Log Example

```
Subject:
        Firewall Alert From Prestige
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10 |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
……..{snip}……..
……..{snip}……..
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |
End of Firewall Log
```

# CHAPTER 16
# Media Bandwidth Management Advanced Setup

This chapter describes bandwidth management with one level of child class.

## 16.1 Media Bandwidth Management Overview

Bandwidth management allows you to allocate an interface's outgoing capacity to specific types of traffic. It can also help you make sure that the Prestige forwards certain types of traffic (especially real-time applications) with minimum delay. With the use of real-time applications such as Voice-over-IP (VoIP) increasing, the requirement for bandwidth allocation is also increasing.

Bandwidth management addresses questions such as:

- Who gets how much access to specific applications?
- What priority level should you give to each type of traffic?
- Which traffic must have guaranteed delivery?
- How much bandwidth should be allotted to guarantee delivery?

Bandwidth management also allows you to configure the allowed output for an interface to match what the network can handle. This helps reduce delays and dropped packets at the next routing device. For example, you can set the WAN interface speed to 1000kbps if the ADSL connection has an upstream speed of 1Mbps. All configuration screens display measurements in kbps (kilobits per second), but this User's Guide also uses Mbps (megabits per second) for brevity's sake.

Refer to Section 16.9 on page 188 to enable and configure bandwidth on the interfaces.

Refer to Section 16.10 on page 190 to configure bandwidth classes.

Refer to Section 16.11 on page 194 to view bandwidth usage information.

## 16.2 Bandwidth Classes and Filters

Use bandwidth classes and child-classes to allocate specific amounts of bandwidth capacity (bandwidth budgets). Configure a bandwidth filter to define a bandwidth class (or child-class) based on a specific application and/or subnet. Use the **Class Configuration** screen (see Section 16.10 on page 190) to set up a bandwidth class's name, bandwidth allotment, and

bandwidth filter. You can configure up to one bandwidth filter per bandwidth class. You can also configure bandwidth classes without bandwidth filters. However, it is recommended that you configure child-classes with filters for any classes that you configure without filters. The Prestige leaves the bandwidth budget allocated and unused for a class that does not have a filter itself or child-classes with filters. View your configured bandwidth classes and child-classes in the **Class Setup** screen (see Section 16.10 on page 190 for details).

The total of the configured bandwidth budgets for child-classes cannot exceed the configured bandwidth budget speed of the parent class.

## 16.3 Proportional Bandwidth Allocation

Bandwidth management allows you to define how much bandwidth each class gets; however, the actual bandwidth allotted to each class decreases or increases in proportion to actual available bandwidth.

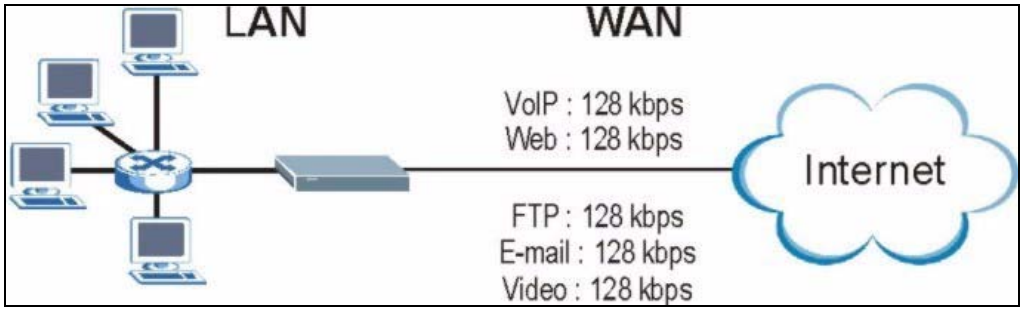
## 16.4 Bandwidth Management Usage Examples

These examples show bandwidth management allotments on a WAN interface that is configured for 640Kbps.

### 16.4.1 Application-based Bandwidth Management Example

The bandwidth classes in the following example are based solely on application. Each bandwidth class (VoIP, Web, FTP, E-mail and Video) is allotted 128kbps.

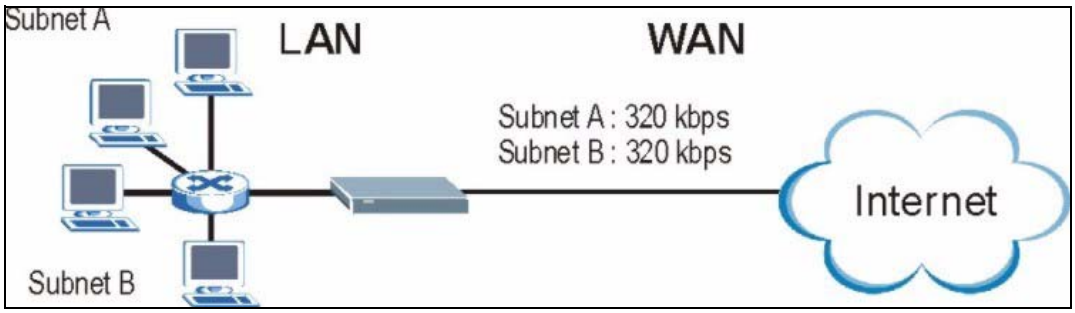
**Figure 87** Application-based Bandwidth Management Example




### 16.4.2 Subnet-based Bandwidth Management Example

The following example uses bandwidth classes based solely on LAN subnets. Each bandwidth class (Subnet A and Subnet B) is allotted 320kbps.

**Figure 88** Subnet-based Bandwidth Management Example



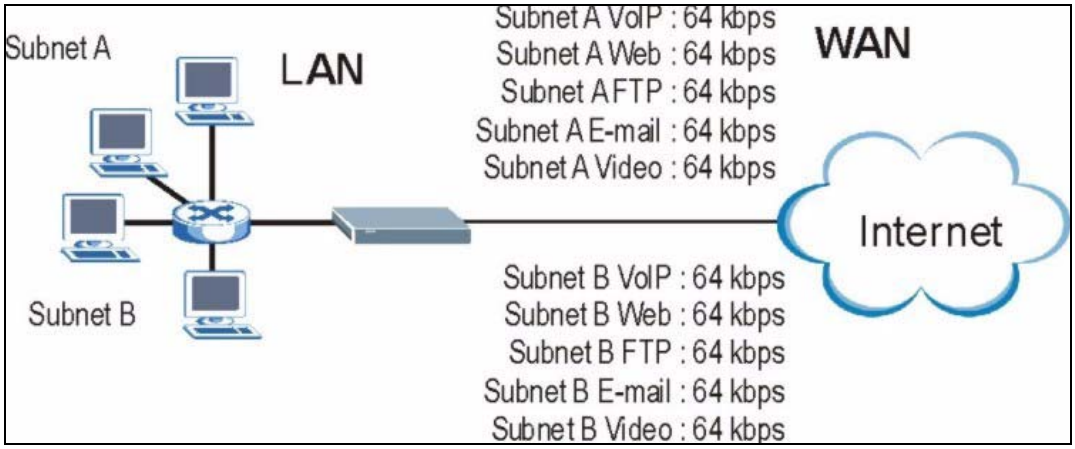

## 16.4.3 Application and Subnet-based Bandwidth Management Example

The following example uses bandwidth classes based on LAN subnets and applications (specific applications in each subnet are allotted bandwidth).

**Table 54** Application and Subnet-based Bandwidth Management Example

| TRAFFIC TYPE | FROM SUBNET A | FROM SUBNET B |
|---|---|---|
| VoIP | 64 kbps | 64 kbps |
| Web | 64 kbps | 64 kbps |
| FTP | 64 kbps | 64 kbps |
| E-mail | 64 kbps | 64 kbps |
| Video | 64 kbps | 64 kbps |

**Figure 89** Application and Subnet-based Bandwidth Management Example



# 16.5 Scheduler

The scheduler divides up an interface's bandwidth among the bandwidth classes. The Prestige has two types of scheduler: fairness-based and priority-based.

## 16.5.1 Priority-based Scheduler

With the priority-based scheduler, the Prestige forwards traffic from bandwidth classes according to the priorities that you assign to the bandwidth classes. The larger a bandwidth class's priority number is, the higher the priority. Assign real-time applications (like those using audio or video) a higher priority number to provide smoother operation.

## 16.5.2 Fairness-based Scheduler

The Prestige divides bandwidth equally among bandwidth classes when using the fairness-based scheduler; thus preventing one bandwidth class from using all of the interface's bandwidth.

# 16.6 Maximize Bandwidth Usage

The maximize bandwidth usage option (see Section 16.7.1 on page 187) allows the Prestige to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a class is not using) among the bandwidth classes that require more bandwidth.

When you enable maximize bandwidth usage, the Prestige first makes sure that each bandwidth class gets up to its bandwidth allotment. Next, the Prestige divides up an interface's available bandwidth (bandwidth that is unbudgeted or unused by the classes) depending on how many bandwidth classes require more bandwidth and on their priority levels. When only one class requires more bandwidth, the Prestige gives extra bandwidth to that class.

When multiple classes require more bandwidth, the Prestige gives the highest priority classes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority classes if there is still bandwidth available. The Prestige distributes the available bandwidth equally among classes with the same priority level.

## 16.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic

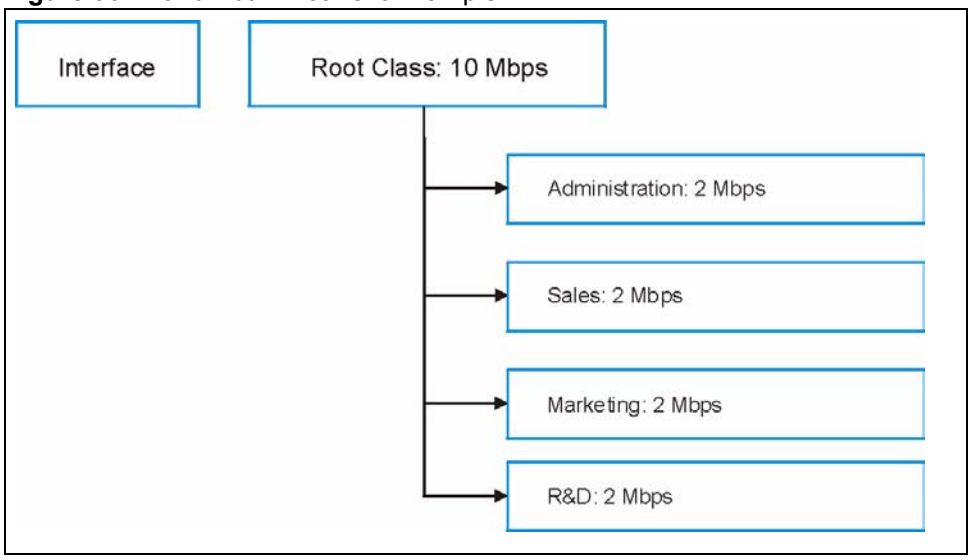
Do the following three steps to configure the Prestige to allow bandwidth for traffic that is not defined in a bandwidth filter.

1. Leave some of the interface's bandwidth unbudgeted.
2. Do not enable the interface's **Maximize Bandwidth Usage** option.
3. Do not enable bandwidth borrowing on the child-classes that have the root class as their parent (see Section 16.7 on page 187).

## 16.6.2 Maximize Bandwidth Usage Example

Here is an example of a Prestige that has maximized bandwidth usage enabled on an interface. The first figure shows each bandwidth class's bandwidth budget and priority. The classes are set up based on subnets. The interface is set to 10 Mbps. Each subnet is allocated 2 Mbps. The unbudgeted 2 Mbps allows traffic not defined in one of the bandwidth filters to go out when you do not select the maximize bandwidth option.

**Figure 90** Bandwidth Allotment Example

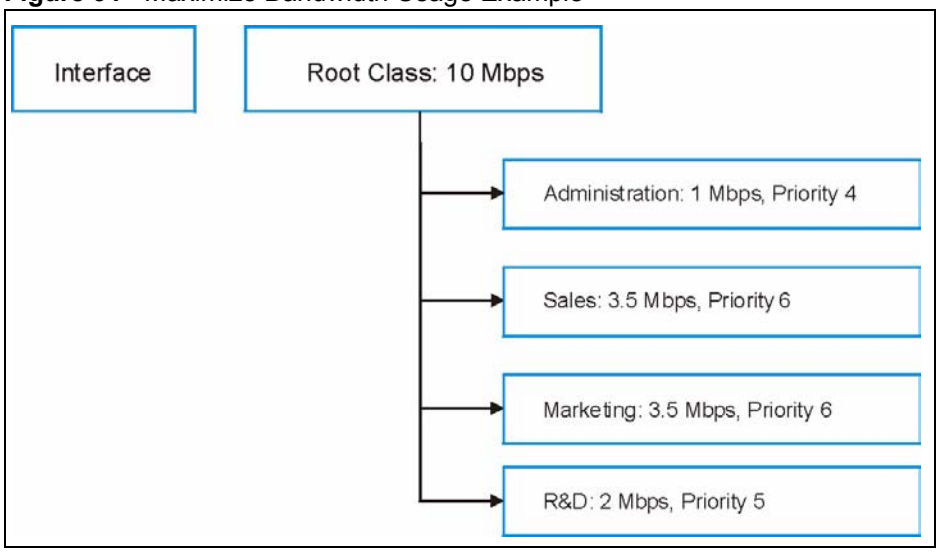



The following figure shows the bandwidth usage with the maximize bandwidth usage option enabled. The Prestige divides up the unbudgeted 2 Mbps among the classes that require more bandwidth. If the administration department only uses 1 Mbps of the budgeted 2 Mbps, the Prestige also divides the remaining 1 Mbps among the classes that require more bandwidth. Therefore, the Prestige divides a total of 3 Mbps total of unbudgeted and unused bandwidth among the classes that require more bandwidth.

In this case, suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1 Mbps of its budgeted 2 Mbps.
- Sales and Marketing are first to get extra bandwidth because they have the highest priority (6). If they each require 1.5 Mbps or more of extra bandwidth, the Prestige divides the total 3 Mbps total of unbudgeted and unused bandwidth equally between the sales and marketing departments (1.5 Mbps extra to each for a total of 3.5 Mbps for each) because they both have the highest priority level.
- R&D requires more bandwidth but only gets its budgeted 2 Mbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing classes.
- The Prestige does not send any traffic that is not defined in the bandwidth filters because all of the unbudgeted bandwidth goes to the classes that need it.

**Figure 91** Maximize Bandwidth Usage Example




# 16.7 Bandwidth Borrowing

Bandwidth borrowing allows a child-class to borrow unused bandwidth from its parent class, whereas maximize bandwidth usage allows bandwidth classes to borrow any unused or unbudgeted bandwidth on the whole interface.

Enable bandwidth borrowing on a child-class to allow the child-class to use its parent class's unused bandwidth. A parent class's unused bandwidth is given to the highest-priority child-class that has bandwidth borrowing configured, first.

The total of the bandwidth allotments for child-classes cannot exceed the bandwidth allotment of their parent class. The Prestige uses the scheduler to divide a parent class's unused bandwidth among the child-classes.

## 16.7.1 Maximize Bandwidth Usage With Bandwidth Borrowing

If you configure both maximize bandwidth usage (on the interface) and bandwidth borrowing (on individual child-classes), the Prestige functions as follows.

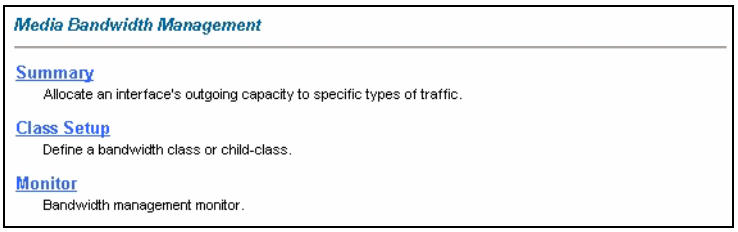
1. The Prestige sends traffic according to each bandwidth class's bandwidth budget.
2. The Prestige assigns a parent class's unused bandwidth to its child-classes that have more traffic than their budgets and have bandwidth borrowing enabled. The Prestige gives priority to bandwidth child-classes of higher priority and treats bandwidth classes of the same priority equally.
3. The Prestige assigns any remaining unused or unbudgeted bandwidth on the interface to any bandwidth class that requires it. The Prestige gives priority to bandwidth classes of higher priority and treats bandwidth classes of the same level equally.

4 The Prestige assigns any remaining unbudgeted bandwidth to traffic that does not match any of the bandwidth classes.

## 16.8 The Main Media Bandwidth Management Screen

Click **Media Bandwidth Mgnt.** to display the main **Media Bandwidth Management** screen as shown.

**Figure 92** Media Bandwidth Mgnt.




The following table describes the links in this screen.

**Table 55** Media Bandwidth Mgnt.

| LINK | DESCRIPTION |
|---|---|
| Summary | Click this link to display a screen where you can enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface. |
| Class Setup | Click this link to display a screen thwere you can configure bandwidth classes. |
| Monitor | Click this link to display a screen wehre you can view bandwidth usage. |

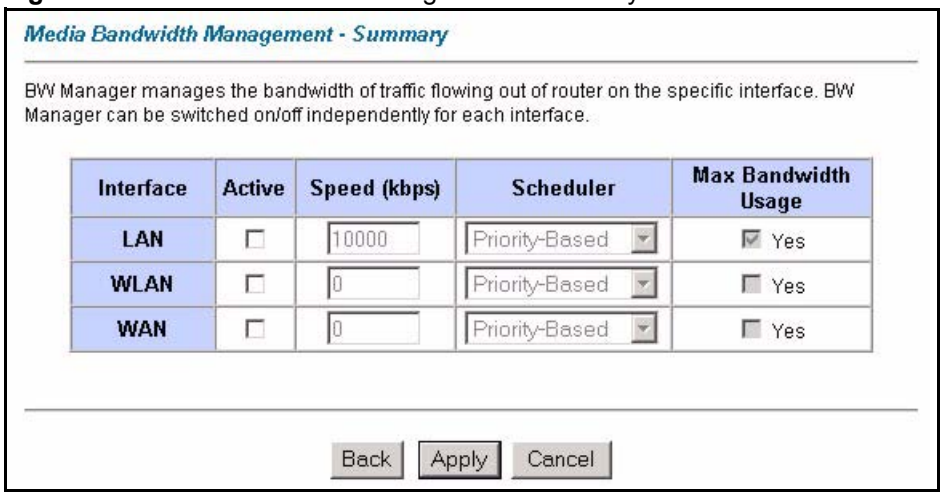
## 16.9 Configuring Summary

Click **Media Bandwidth Management**, **Summary** to open the screen as shown next.

Enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.

Refer to Section 16.1 on page 182 for more information.

**Figure 93** Media Bandwidth Management: Summary




The following table describes the labels in this screen.

**Table 56** Media Bandwidth Management: Summary

| LABEL | DESCRIPTION |
|---|---|
| LAN<br>WLAN<br>WAN | These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source.<br>Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the Prestige and be managed by bandwidth management. |
| Active | Select an interface's check box to enable bandwidth management on that interface. |
| Speed (kbps) | Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management.<br>This appears as the bandwidth budget of the interface's root class. The recommendation is to set this speed to match what the interface's connection can handle. For example, set the WAN interface speed to 10000 kbps if the ADSL connection has an upstream speed of 10Mbps. |
| Scheduler | Select either **Priority-Based** or **Fairness-Based** from the drop-down menu to control the traffic flow.<br>Select **Priority-Based** to give preference to bandwidth classes with higher priorities.<br>Select **Fairness-Based** to treat all bandwidth classes equally. |
| Maximize Bandwidth Usage | Select this check box to have the Prestige divide up all of the interface's unallocated and/or unused bandwidth among the bandwidth classes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class or you want to limit the speed of this interface (see the **Speed** field description). |
| Back | Click **Back** to go to the main **Media Bandwidth Management** screen. |
| Apply | Click **Apply** to save your settings back to the Prestige. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

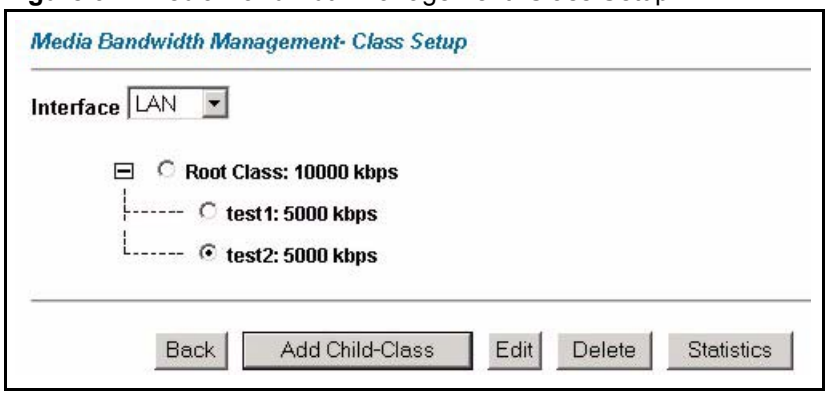
# 16.10 Configuring Class Setup

The class setup screen displays the configured bandwidth classes by individual interface. Select an interface and click the buttons to perform the actions described next. Click "+" to expand the class tree or click "-"to collapse the class tree. Each interface has a permanent root class. The bandwidth budget of the root class is equal to the speed you configured on the interface (see Section 16.9 on page 188 to configure the speed of the interface). Configure child-class layers for the root class.

Refer to Section 16.1 on page 182 for more information.

To add or delete child classes on an interface, click **Media Bandwidth Management**, then **Class Setup**. The screen appears as shown (with example classes).

**Figure 94** Media Bandwidth Management: Class Setup




The following table describes the labels in this screen.

**Table 57** Media Bandwidth Management: Class Setup

| LABEL | DESCRIPTION |
|---|---|
| Interface | Select an interface from the drop-down list box for which you wish to set up classes. |
| Back | Click **Back** to go to the main **Media Bandwidth Management** screen. |
| Add Child-Class | Click **Add Child-class** to add a sub-class. |
| Edit | Click **Edit** to configure the selected class. You cannot edit the root class. |
| Delete | Click **Delete** to delete the class and all its child-classes. You cannot delete the root class. |
| Statistics | Click **Statistics** to display the status of the selected class. |

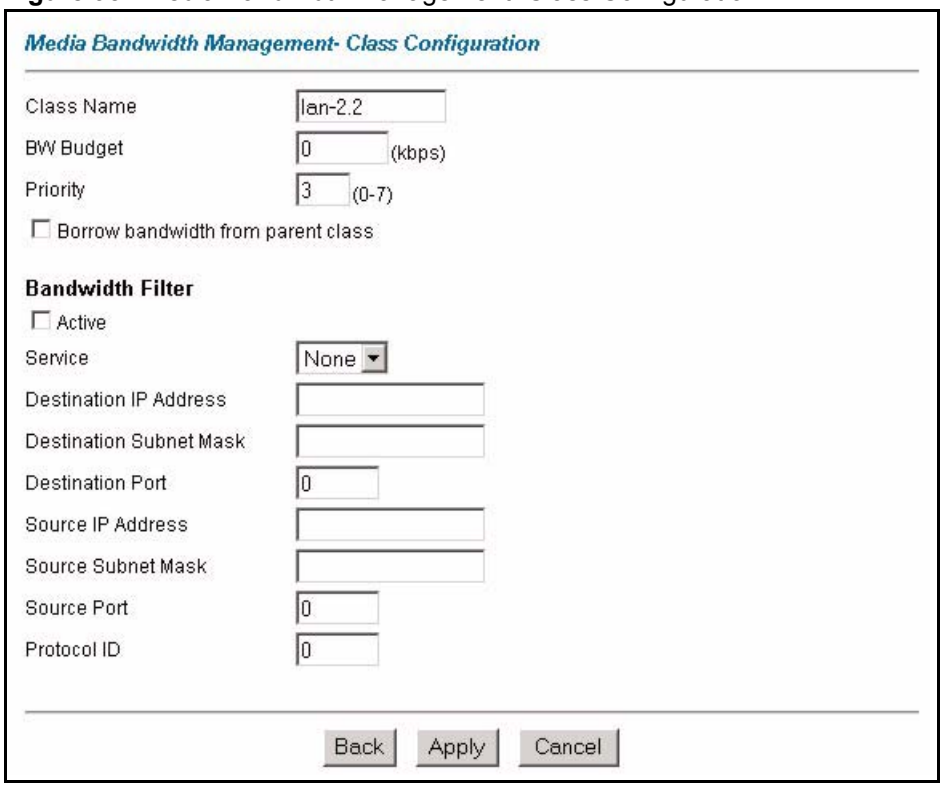
## 16.10.1 Media Bandwidth Management Class Configuration

Configure a bandwidth management class in the **Class Configuration** screen. You must use the **Media Bandwidth Management - Summary** screen to enable bandwidth management on an interface before you can configure classes for that interface.

Refer to Section 16.1 on page 182 for more information.

To add a child class, click **Media Bandwidth Management**, then **Class Setup**. Click the **Add Child-Class** button to open the following screen.

**Figure 95** Media Bandwidth Management: Class Configuration




The following table describes the labels in this screen.

**Table 58** Media Bandwidth Management: Class Configuration

| LABEL | DESCRIPTION |
|---|---|
| Class Name | Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces. |
| BW Budget (kbps) | Specify the maximum bandwidth allowed for the class in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual class. |
| Priority | Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3. |
| Borrow bandwidth from parent class | Select this option to allow a child-class to borrow bandwidth from its parent class if the parent class is not using up its bandwidth budget.<br>Bandwidth borrowing is governed by the priority of the child-classes. That is, a child-class with the highest priority (7) is the first to borrow bandwidth from its parent class.<br>Do not select this for the classes directly below the root class if you want to leave bandwidth available for other traffic types or you want to set the interface's speed to match what the next device in network can handle (see the **Speed** field description in the **Summary** screen). |
| Bandwidth Filter<br>The Prestige uses a bandwidth filter to identify the traffic that belongs to a bandwidth class. | |

**Table 58** Media Bandwidth Management: Class Configuration (continued)

| LABEL | DESCRIPTION |
|---|---|
| Active | Select the check box to have the Prestige use this bandwidth filter when it performs bandwidth management. |
| Service | You can select a predefined service instead of configuring the **Destination Port**, **Source Port** and **Protocol ID** fields.<br>SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select **SIP** from the drop-down list box to configure this bandwidth filter for traffic that uses SIP.<br>File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. Select **FTP** from the drop-down list box to configure this bandwidth filter for FTP traffic.<br>**H.323** is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. Select **H.323** from the drop-down list box to configure this bandwidth filter for traffic that uses H.323.<br>When you select **None**, the bandwidth class applies to all services unless you specify one by configuring the **Destination Port**, **Source Port** and **Protocol ID** fields. |
| Destination IP Address | Enter the destination IP address in dotted decimal notation. A blank destination IP address means any destination IP address. |
| Destination Subnet Mask | Enter the destination subnet mask. This field is N/A if you do not specify a **Destination IP Address**. Refer to the appendix for more information on IP subnetting. |
| Destination Port | Enter the port number of the destination. A blank destination port means any destination port. |
| Source IP Address | Enter the source IP address. A blank source IP address means any source IP address. |
| Source Subnet Mask | Enter the source subnet mask. This field is N/A if you do not specify a **Source IP Address**. Refer to the appendix for more information on IP subnetting. |
| Source Port | Enter the port number of the source. See the following table for some common services and port numbers. A blank source port means any source port number. |
| Protocol ID | Enter the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP. A blank protocol ID means any protocol number. |
| Back | Click **Back** to go to the main **Media Bandwidth Management** screen. |
| Apply | Click **Apply** to save your changes back to the Prestige. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

**Table 59** Services and Port Numbers

| SERVICES | PORT NUMBER |
|---|---|
| ECHO | 7 |
| FTP (File Transfer Protocol) | 21 |

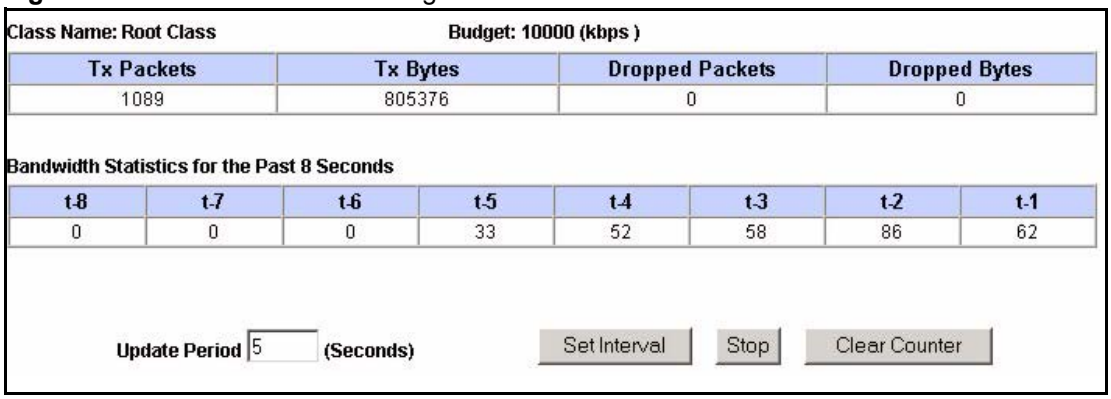
**Table 59** Services and Port Numbers

| SERVICES | PORT NUMBER |
|---|---|
| SMTP (Simple Mail Transfer Protocol) | 25 |
| DNS (Domain Name System) | 53 |
| Finger | 79 |
| HTTP (Hyper Text Transfer protocol or WWW, Web) | 80 |
| POP3 (Post Office Protocol) | 110 |
| NNTP (Network News Transport Protocol) | 119 |
| SNMP (Simple Network Management Protocol) | 161 |
| SNMP trap | 162 |
| PPTP (Point-to-Point Tunneling Protocol) | 1723 |

## 16.10.2 Media Bandwidth Management Statistics

Use the **Media Bandwidth Management Statistics** screen to view network performance information. Click the **Statistics** button in the **Class Setup** screen to open the **Statistics** screen.

**Figure 96** Media Bandwidth Management Statistics




The following table describes the labels in this screen.

**Table 60** Media Bandwidth Management Statistics

| LABEL | DESCRIPTION |
|---|---|
| Class Name | This field displays the name of the class the statistics page is showing. |
| Budget (kbps) | This field displays the amount of bandwidth allocated to the class. |
| Tx Packets | This field displays the total number of packets transmitted. |
| Tx Bytes | This field displays the total number of bytes transmitted. |
| Dropped Packets | This field displays the total number of packets dropped. |
| Dropped Bytes | This field displays the total number of bytes dropped. |
| Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1) | |

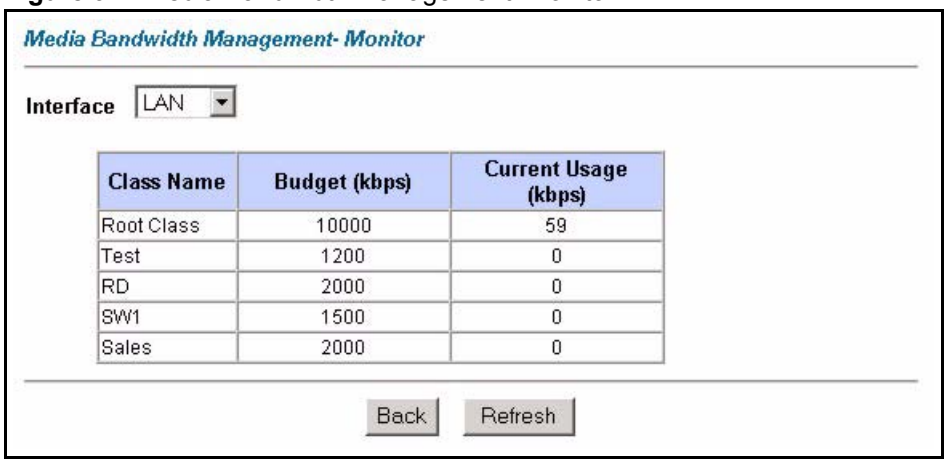
**Table 60** Media Bandwidth Management Statistics

| LABEL | DESCRIPTION |
|---|---|
| This field displays the bandwidth statistics (in bps) for the past one to eight seconds. For example, t-1 means one second ago. | |
| Update Period (seconds) | Enter the time interval in seconds to define how often the information should be refreshed. |
| Set Interval | Click **Set Interval** to apply the new update period you entered in the **Update Period** field above. |
| Stop Update | Click **Stop Update** to stop the browser from refreshing bandwidth management statistics. |
| Clear Counter | Click **Clear Counter** to clear all of the bandwidth management statistics. |

# 16.11 Bandwidth Monitor

To view the Prestige's bandwidth usage and allotments, click **Media Bandwidth Management**, then **Monitor**. The screen appears as shown.

**Figure 97** Media Bandwidth Management: Monitor




The following table describes the labels in this screen.

**Table 61** Media Bandwidth Management: Monitor

| LABEL | DESCRIPTION |
|---|---|
| Interface | Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth classes. |
| Class Name | This field displays the name of the class. |
| Budget (kbps) | This field displays the amount of bandwidth allocated to the class. |
| Current Usage (kbps) | This field displays the amount of bandwidth that each class is using. |
| Back | Click **Back** to go to the main **Media Bandwidth Management** screen. |
| Refresh | Click **Refresh** to update the page. |

# CHAPTER 17
# Maintenance

This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

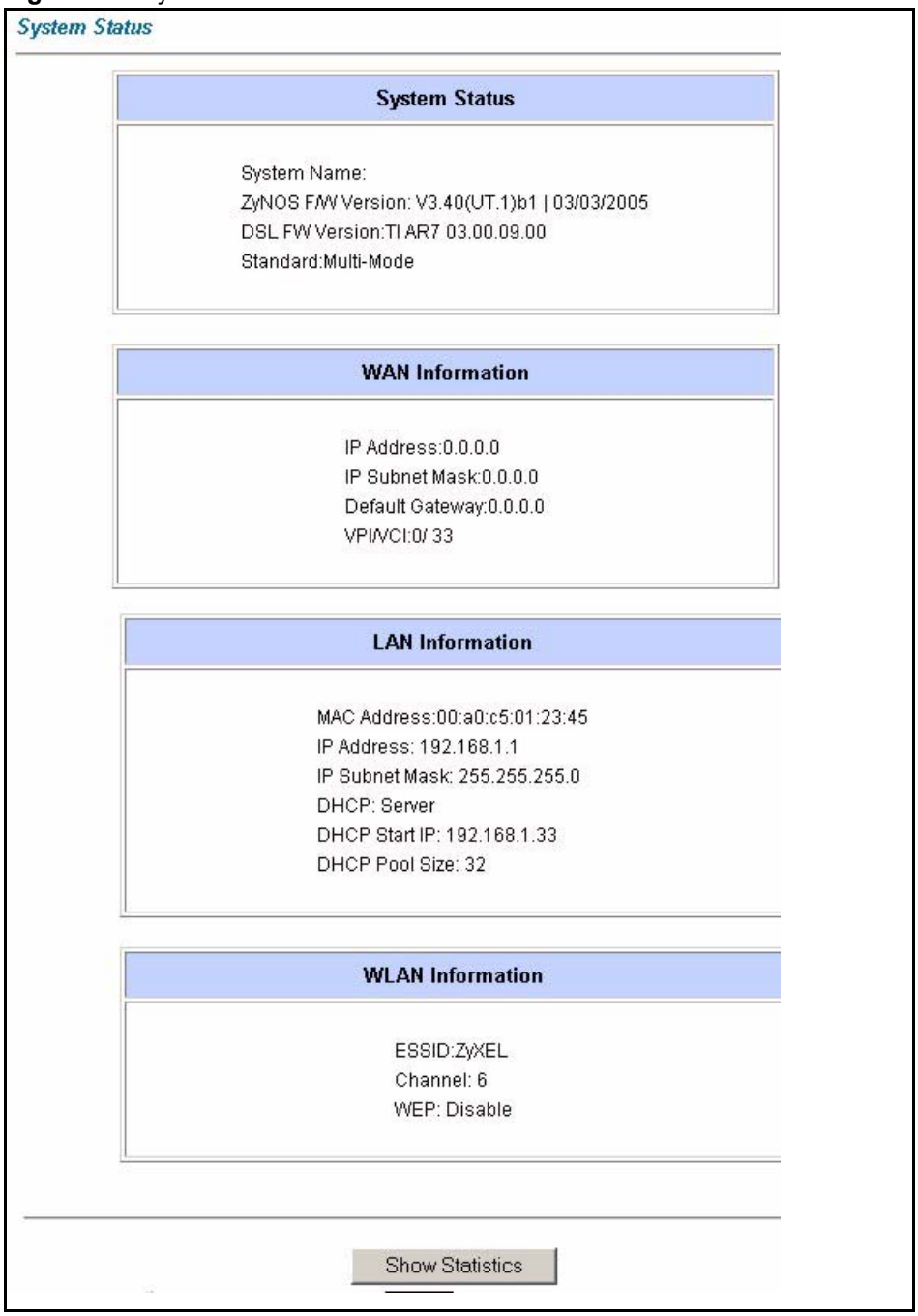
## 17.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your Prestige.

## 17.2 System Status Screen

Click **System Status** under **Maintenance** to open the following screen, where you can use to monitor your Prestige. Note that these fields are READ-ONLY and only for diagnostic purposes.

**Figure 98** System Status




The following table describes the fields in this screen.

**Table 62** System Status

| LABEL | DESCRIPTION |
|---|---|
| System Status | |
| System Name | This is the name of your Prestige. It is for identification purposes. |

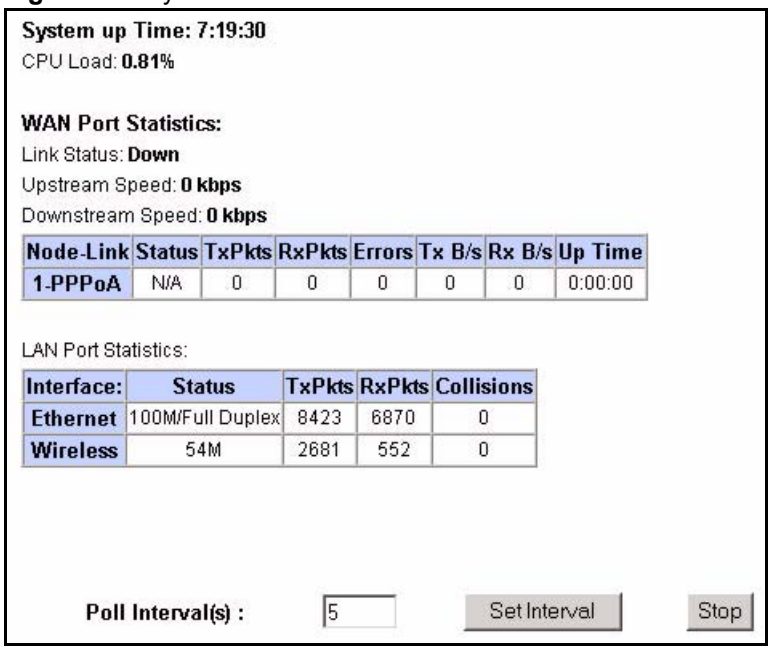
**Table 62** System Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| ZyNOS Firmware Version | This is the ZyNOS firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design. |
| DSL FW Version | This is the DSL firmware version associated with your Prestige. |
| Standard | This is the standard that your Prestige is using. |
| WAN Information | |
| IP Address | This is the WAN port IP address. |
| IP Subnet Mask | This is the WAN port IP subnet mask. |
| Default Gateway | This is the IP address of the default gateway, if applicable. |
| VPI/VCI | This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the first Wizard screen. |
| LAN Information | |
| MAC Address | This is the MAC (Media Access Control) or Ethernet address unique to your Prestige. |
| IP Address | This is the LAN port IP address. |
| IP Subnet Mask | This is the LAN port IP subnet mask. |
| DHCP | This is the WAN port DHCP role - **Server**, **Relay** (not all Prestige models) or **None**. |
| DHCP Start IP | This is the first of the contiguous addresses in the IP address pool. |
| DHCP Pool Size | This is the number of IP addresses in the IP address pool. |
| WLAN Information | |
| ESSID | This is the descriptive name used to identify the Prestige in the wireless LAN. |
| Channel | This is the channel number used by the Prestige now. |
| WEP | This displays the status of WEP data encryption. |
| Show Statistics | Click **Show Statistics** to see the performance statistics such as number of packets sent and number of packets received for each port. |

## 17.2.1 System Statistics

Click **Show Statistics** in the **System Status** screen to open the following screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

**Figure 99** System Status: Show Statistics




The following table describes the fields in this screen.

**Table 63** System Status: Show Statistics

| LABEL | DESCRIPTION |
|---|---|
| System up Time | This is the elapsed time the system has been up. |
| CPU Load | This field specifies the percentage of CPU utilization. |
| LAN or WAN Port Statistics | This is the WAN or LAN port. |
| Link Status | This is the status of your WAN link. |
| Upstream Speed | This is the upstream speed of your Prestige. |
| Downstream Speed | This is the downstream speed of your Prestige. |
| Node-Link | This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE. |
| Interface | This field displays the type of port. |
| Status | For the WAN port, this displays the port speed and duplex setting if you're using Ethernet encapsulation and **down** (line is down), **idle** (line (ppp) idle), **dial** (starting to trigger a call) and **drop** (dropping a call) if you're using PPPoE encapsulation.<br>For a LAN port, this shows the port speed and duplex setting. |
| TxPkts | This field displays the number of packets transmitted on this port. |
| RxPkts | This field displays the number of packets received on this port. |
| Errors | This field displays the number of error packets on this port. |
| Tx B/s | This field displays the number of bytes transmitted in the last second. |
| Rx B/s | This field displays the number of bytes received in the last second. |
| Up Time | This field displays the elapsed time this port has been up. |
| Collisions | This is the number of collisions on this port. |

**Table 63** System Status: Show Statistics (continued)

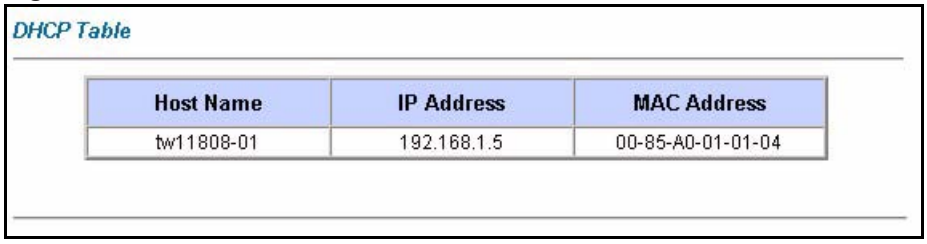
| LABEL | DESCRIPTION |
|---|---|
| Poll Interval(s) | Type the time interval for the browser to refresh system statistics. |
| Set Interval | Click this button to apply the new poll interval you entered in the **Poll Interval** field above. |
| Stop | Click this button to halt the refreshing of the system statistics. |

## 17.3 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Prestige as a DHCP server or disable it. When configured as a server, the Prestige provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **Maintenance**, and then the **DHCP Table** tab. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP Client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the DHCP server.

**Figure 100** DHCP Table




The following table describes the fields in this screen.

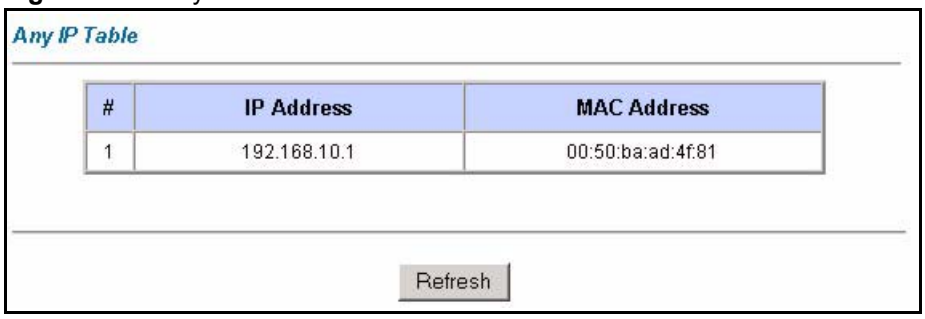
**Table 64** DHCP Table

| LABEL | DESCRIPTION |
|---|---|
| Host Name | This is the name of the host computer. |
| IP Address | This field displays the IP address relative to the **Host Name** field. |
| MAC Address | This field displays the MAC (Media Access Control) address of the computer with the displayed host name.<br>Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. |

# 17.4 Any IP Table Screen

Click **Maintenance**, **Any IP**. The Any IP table shows current read-only information (including the IP address and the MAC address) of all network devices that use the Any IP feature to communicate with the Prestige.

**Figure 101** Any IP Table




The following table describes the labels in this screen.

**Table 65** Any IP Table

| LABEL | DESCRIPTION |
|---|---|
| # | This field displays the index number. |
| IP Address | This field displays the IP address of the network device. |
| MAC Address | This field displays the MAC (Media Access Control) address of the computer with the displayed IP address.<br>Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. |
| Refresh | Click **Refresh** to update this screen. |

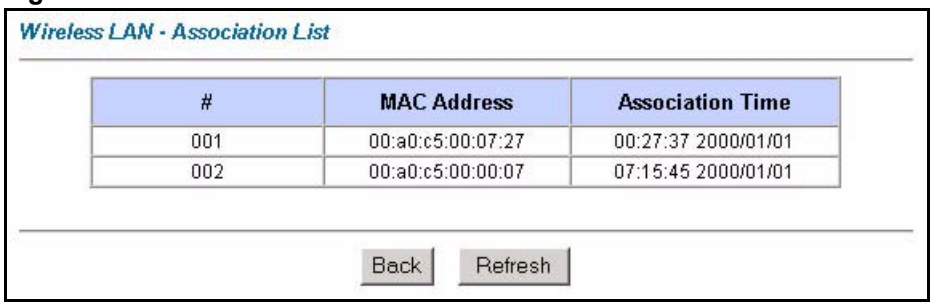
# 17.5 Wireless Screen

The read-only screen displays information about the Prestige's wireless LAN.

## 17.5.1 Association List

This screen displays the MAC address(es) of the wireless stations that are currently logged in to the network. Click **Wireless LAN** and then **Association List** to open the screen shown next.

**Figure 102** Association List




The following table describes the fields in this screen.

**Table 66** Association List

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of an associated wireless station. |
| MAC Address | This field displays the MAC (Media Access Control) address of an associated wireless station.<br>Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. |
| Association Time | This field displays the time a wireless station is associated to the Prestige. |
| Back | Click **Back** to return to the previous screen. |
| Refresh | Click **Refresh** to renew the information in the table. |

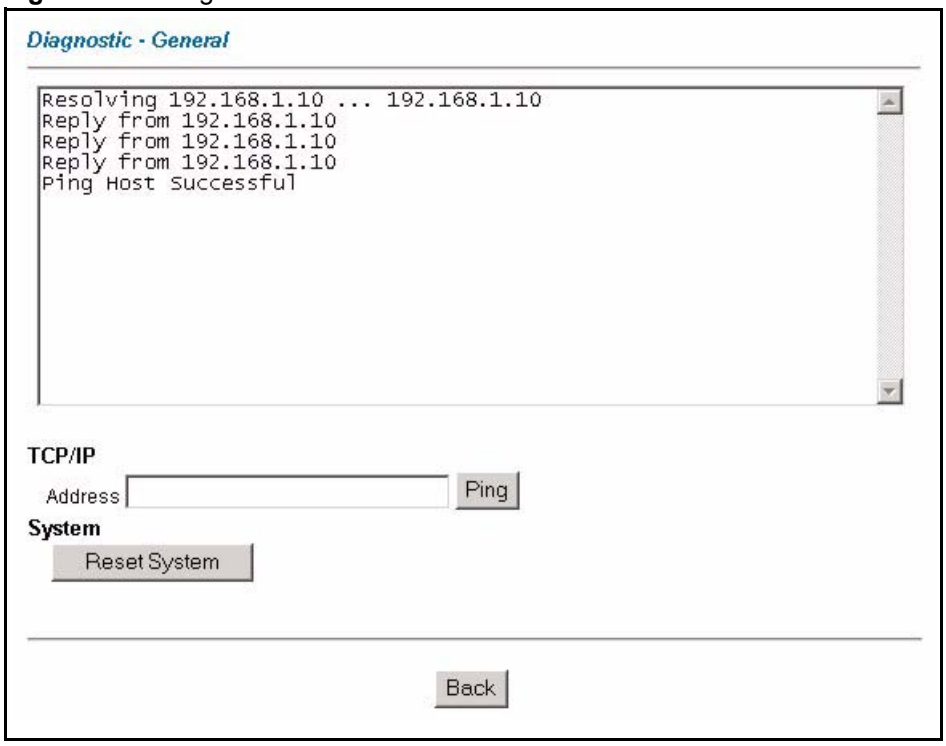
# 17.6 Diagnostic Screens

These read-only screens display information to help you identify problems with the Prestige.

## 17.6.1 General Diagnostic

Click **Diagnostic** and then **General** to open the screen shown next.

**Figure 103** Diagnostic: General




The following table describes the fields in this screen.

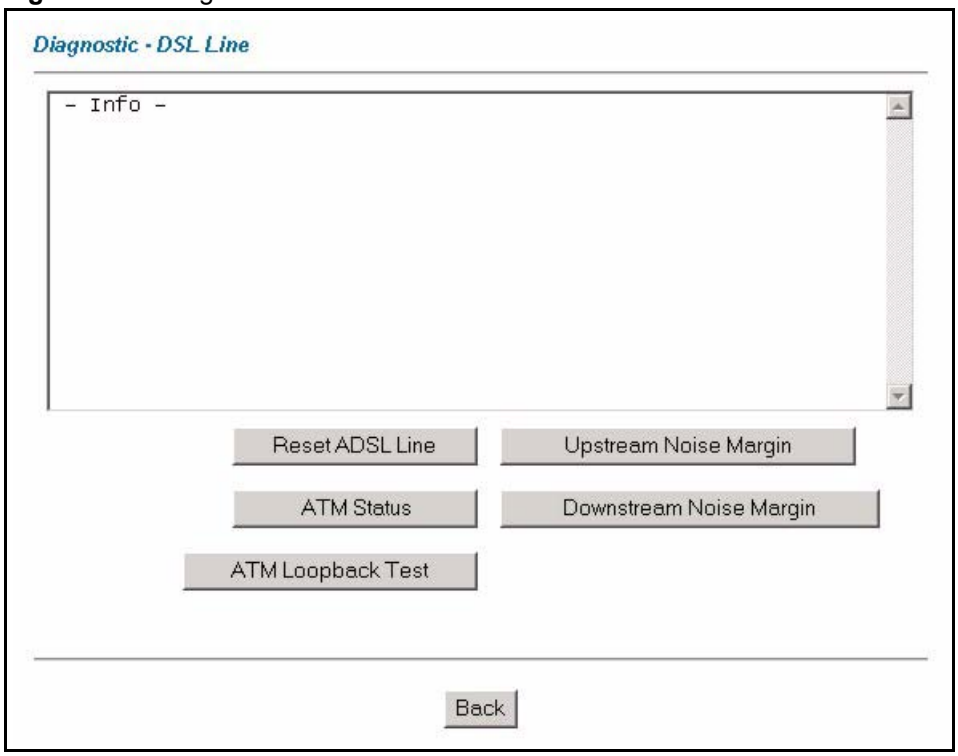
**Table 67** Diagnostic: General

| LABEL | DESCRIPTION |
|---|---|
| TCP/IP Address | Type the IP address of a computer that you want to ping in order to test a connection. |
| Ping | Click this button to ping the IP address that you entered. |
| Reset System | Click this button to reboot the Prestige. A warning dialog box is then displayed asking you if you're sure you want to reboot the system. Click **OK** to proceed. |
| Back | Click this button to go back to the main **Diagnostic** screen. |

## 17.6.2 DSL Line Diagnostic

Click **Diagnostic** and then **DSL Line** to open the screen shown next.

**Figure 104** Diagnostic: DSL Line




The following table describes the fields in this screen.

**Table 68** Diagnostic: DSL Line

| LABEL | DESCRIPTION |
|---|---|
| Reset ADSL Line | Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example:<br>"Start to reset ADSL<br>Loading ADSL modem F/W...<br>Reset ADSL Line Successfully!" |
| ATM Status | Click this button to view ATM status. |
| ATM Loopback Test | Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The Prestige sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the Prestige. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network. |
| Upstream Noise Margin | Click this button to display the upstream noise margin. |
| Downstream Noise Margin | Click this button to display the downstream noise margin. |
| Back | Click this button to go back to the main **Diagnostic** screen. |

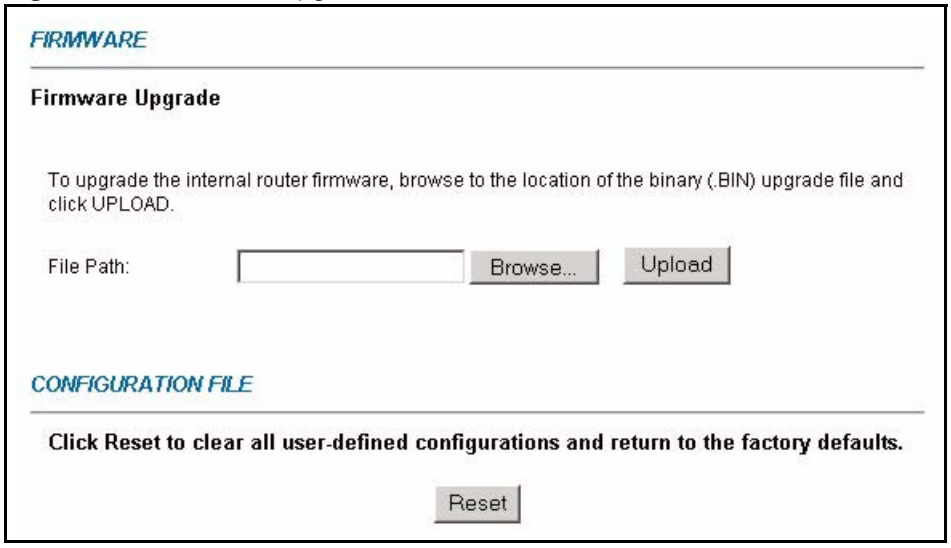
# 17.7 Firmware Upgrade

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a.bin extension, for example, "Prestige.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See Chapter 33 on page 306 for upgrading firmware using FTP/TFTP commands.

Only use firmware for your device's specific model. Refer to the label on the bottom of your device.

Click **Firmware** to open the following screen. Follow the instructions in this screen to upload firmware to your Prestige.

**Figure 105** Firmware Upgrade




The following table describes the labels in this screen.

**Table 69** Firmware Upgrade

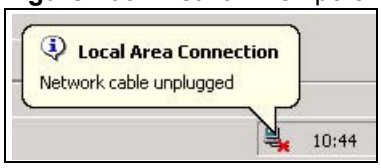
| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse ...** to find it. |
| Browse... | Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them. |
| Upload | Click **Upload** to begin the upload process. This process may take up to two minutes. |
| Reset | Click this button to clear all user-entered configuration information and return the Prestige to its factory defaults. |

**Note:** Do NOT turn off the Prestige while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the Prestige again.

The Prestige automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 106** Network Temporarily Disconnected




After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following screen will appear. Click **Back** to go back to the **Firmware** screen.

**Figure 107** Error Message

# CHAPTER 18
# Introducing the SMT

This chapter explains how to access and navigate the System Management Terminal and gives an overview of its menus.

## 18.1 SMT Introduction

The Prestige's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator over a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus via Telnet, how to navigate the SMT and how to configure SMT menus.

### 18.1.1 Procedure for SMT Configuration via Telnet

The following procedure details how to telnet into your Prestige.

1. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type "`telnet 192.168.1.1`" (the default IP address) and click **OK**.
2. Enter "`1234`" in the **Password** field.
3. After entering the password you will see the main menu.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your Prestige will automatically log you out. You will then have to telnet into the Prestige again.

### 18.1.2 Entering Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown next.

For your first login, enter the default password "`1234`". As you type the password, the screen displays an asterisk "`*`" for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your Prestige will automatically log you out.

**Figure 108** Login Screen

```
Enter Password: ****
```

## 18.1.3 Prestige SMT Menus Overview

The following table gives you an overview of your Prestige's various SMT menus.

**Table 70** SMT Menus Overview

| MENUS | SUB MENUS | | |
|---|---|---|---|
| 1 General Setup | 1.1 Configure Dynamic DNS | | |
| 2 WAN Backup Setup | | | |
| 3 LAN Setup | 3.1 LAN Port Filter Setup | | |
| | 3.2 TCP/IP and DHCP Setup | 3.2.1 IP Alias Setup | |
| | 3.5 Wireless LAN Setup | 3.5.1 WLAN MAC Address Filter | |
| 4 Internet Access Setup | | | |
| 11 Remote Node Setup | 11.1 Remote Node Profile | | |
| | 11.3 Remote Node Network Layer Options | | |
| | 11.5 Remote Node Filter | | |
| | 11.6 Remote Node ATM Layer Options | | |
| | 11.8 Advance Setup Options (PPPoE passthrough) | | |
| 12 Static Routing Setup | 12.1 Edit Static Route Setup | 12.1.1 Edit IP Static Route | |
| | 12.3 Bridge Static Route Setup | 12.3.1 Edit Bridge Static Route | |
| 14 Dial-in User Setup | 14.1 Edit Dial-in User | | |
| 15 NAT Setup | 15.1 Address Mapping Sets | 15.1.x Address Mapping Rules | 15.1.x.x Address Mapping Rule |
| | 15.2 NAT Server Sets | 15.2.x NAT Server Setup | |
| 21 Filter and Firewall Rule Setup | 21.1 Filter Setup | 21.1 Filter Rules Summary | 21.1.x.1 Generic Filter Rule |
| | | | 21.1.x.1 TCP/IP Filter Rule |
| | 21.2 Firewall Setup | | |
| 22 SNMP Configuration | | | |
| 23 System Security | 23.1 Change Password | | |
| | 23.2 RADIUS Server | | |
| | 23.4 IEEE 802.1X | | |

**Table 70** SMT Menus Overview (continued)

| MENUS | SUB MENUS | | |
|---|---|---|---|
| 24 System Maintenance | 24.1 Status | | |
| | 24.2 System Information and Console Port Speed | 24.2.1 Information | |
| | | 24.2.2 Change Console Port Speed | |
| | 24.3 Log and Trace | 24.3.1 View Error Log | |
| | | 24.3.2 UNIX Syslog | |
| | 24.4 Diagnostic | | |
| | 24.5 Backup Configuration | | |
| | 24.6 Restore Configuration | | |
| | 24.7 Upload Firmware | 24.7.1 Upload System Firmware | |
| | | 24.7.2 Upload System Configuration File | |
| | 24.8 Command Interpreter Mode | | |
| | 24.9 Call Control | 24.9.1 Budget Management | |
| | 24.10 Time and Date Setting | | |
| | 24.11 Remote Management Control | | |
| 25 IP Routing Policy Setup | 25.1 IP Routing Policy Setup | 25.1.1 IP Routing Policy | |
| 26 Schedule Setup | 26.1 Schedule Set Setup | | |

## 18.2 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your Prestige.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

**Table 71** Navigating the SMT Interface

| OPERATION | KEY STROKE | DESCRIPTION |
|---|---|---|
| Move down to another menu | [ENTER] | To move forward to a submenu, type in the number of the desired submenu and press [ENTER]. |
| Move up to a previous menu | [ESC] | Press [ESC] to move back to the previous menu. |
| Move to a hidden menu | Press [SPACE BAR] to change **No** to **Yes** then press [ENTER]. | Fields beginning with "Edit" lead to hidden menus and have a default setting of **No**. Press [SPACE BAR] once to change **No** to **Yes**, then press [ENTER] to go to the "hidden" menu. |
| Move the cursor | [ENTER] or [UP]/ [DOWN] arrow keys. | Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively. |

**Table 71** Navigating the SMT Interface

| OPERATION | KEY STROKE | DESCRIPTION |
|---|---|---|
| Entering information | Type in or press [SPACE BAR], then press [ENTER]. | You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR]. |
| Required fields | <? > or **ChangeMe** | All fields with the symbol <?> must be filled in order to be able to save the new configuration.<br>All fields with **ChangeMe** must not be left blank in order to be able to save the new configuration. |
| N/A fields | <N/A> | Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable. |
| Save your configuration | [ENTER] | Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu. |
| Exit the SMT | | Type 99, then press [ENTER].Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface. |

After you enter the password, the SMT displays the main menu, as shown next.

**Table 72** SMT Main Menu

```
                Copyright (c) 1994 - 2004 ZyXEL Communications Corp.

                           Prestige 660W-T1  Main Menu

    Getting Started                       Advanced Management
      1. General Setup                      21. Filter and Firewall Setup
      2. WAN Backup Setup                   22. SNMP Configuration
      3. LAN Setup                          23. System Security
      4. Internet Access Setup              24. System Maintenance
                                            25. IP Routing Policy Setup
    Advanced Applications                   26. Schedule Setup
      11. Remote Node Setup
      12. Static Routing Setup
      14. Dial-in User Setup                99. Exit
      15. NAT Setup




                          Enter Menu Selection Number:
```

## 18.2.1 System Management Terminal Interface Summary

**Table 73** Main Menu Summary

| # | MENU TITLE | DESCRIPTION |
|---|---|---|
| 1 | General Setup | Use this menu to set up your general information. |
| 2 | WAN Backup Setup | Use this menu to setup traffic redirect and dial-back up. |

**Table 73** Main Menu Summary

| # | MENU TITLE | DESCRIPTION |
|---|---|---|
| 3 | LAN Setup | Use this menu to set up your wireless LAN and LAN connection. |
| 4 | Internet Access Setup | A quick and easy way to set up an Internet connection. |
| 11 | Remote Node Setup | Use this menu to set up the Remote Node for LAN-to-LAN connection, including Internet connection. |
| 12 | Static Routing Setup | Use this menu to set up static routes. |
| 14 | Dial-in User Setup | Use this menu to set up local user profiles on the Prestige. |
| 15 | NAT Setup | Use this menu to specify inside servers when NAT is enabled. |
| 21 | Filter and Firewall Setup | Use this menu to configure filters, activate/deactivate the firewall and view the firewall log. |
| 22 | SNMP Configuration | Use this menu to set up SNMP related parameters. |
| 23 | System Security | Use this menu to set up wireless security and change your password. |
| 24 | System Maintenance | This menu provides system status, diagnostics, software upload, etc. |
| 25 | IP Routing Policy Setup | Use this menu to configure your IP routing policy. |
| 26 | Schedule Setup | Use this menu to schedule outgoing calls. |
| 99 | Exit | Use this to exit from SMT and return to a blank screen. |

## 18.3 Changing the System Password

Change the Prestige default password by following the steps shown next.

1. Enter 23 in the main menu to display **Menu 23 - System Security**.
2. Enter 1 to display **Menu 23.1 - System Security - Change Password** as shown next.
3. Type your existing system password in the **Old Password** field, for example "`1234`", and press [ENTER].

**Figure 109** Menu 23.1 Change Password

```
            Menu 23.1 - System Security - Change Password

                Old Password= ?
                New Password= ?
                Retype to confirm=?

            Enter here to CONFIRM or ESC to CANCEL:
```

4. Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].
5. Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].

**Note:** Note that as you type a password, the screen displays an "*" for each character you type.

# CHAPTER 19
# Menu 1 General Setup

**Menu 1 - General Setup** contains administrative and system-related information.

## 19.1 General Setup

**Menu 1 — General Setup** contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the **Identification** tab, note the entry for the **Computer name** field and enter it as the Prestige **System Name**.
- In Windows 2000 click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the Prestige **System Name**.
- In Windows XP, click **start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the Prestige **System Name**.

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the Prestige via DHCP.

## 19.2 Procedure To Configure Menu 1

Enter 1 in the Main Menu to open **Menu 1 — General Setup** (shown next).

**Figure 110** Menu 1 General Setup

```
                Menu 1 General Setup

                      System Name= ?
                      Location=
                      Contact Person's Name=
                      Domain Name=
                      Edit Dynamic DNS= No

                      Route IP= Yes
                      Bridge= No

          Press ENTER to Confirm or ESC to Cancel:
```

Fill in the required fields. Refer to the table shown next for more information about these fields.

**Table 74** Menu 1 General Setup

| FIELD | DESCRIPTION |
|---|---|
| System Name | Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. |
| Location (optional) | Enter the geographic location (up to 31 characters) of your Prestige. |
| Contact Person's Name (optional) | Enter the name (up to 30 characters) of the person in charge of this Prestige. |
| Domain Name | Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domainname" to see the current domain name used by your gateway.<br>If you want to clear this field just press the [SPACE BAR]. The domain name entered by you is given priority over the ISP assigned domain name. |
| Edit Dynamic DNS | Press the [SPACE BAR] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1 — Configure Dynamic DNS** (discussed next). |
| Route IP | Set this field to **Yes** to enable or **No** to disable IP routing. You must enable IP routing for Internet access. |
| Bridge | Turn on/off bridging for protocols not supported (for example, SNA) or not turned on in the previous **Route IP** field.<br>Select **Yes** to turn bridging on; select **No** to turn bridging off. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

## 19.2.1 Procedure to Configure Dynamic DNS

**Note:** If you have a private WAN IP address, then you cannot use dynamic DNS.

To configure dynamic DNS, go to **Menu 1 — General Setup** and select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1— Configure Dynamic DNS** as shown next.

**Figure 111** Menu 1.1 Configure Dynamic DNS

```
                Menu 1.1 - Configure Dynamic DNS
           Service Provider= WWW.DynDNS.ORG
           Active= No
           Host=
           EMAIL=
           USER=
           Password= ********
           Enable Wildcard= No

                Press ENTER to Confirm or ESC to Cancel:
```

Follow the instructions in the next table to configure dynamic DNS parameters.

**Table 75** Menu 1.1 Configure Dynamic DNS

| FIELD | DESCRIPTION |
|---|---|
| Service Provider | This is the name of your dynamic DNS service provider. |
| Active | Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active. |
| Host | Enter the domain name assigned to your Prestige by your dynamic DNS provider. |
| EMAIL | Enter your e-mail address. |
| User | Enter your user name. |
| Password | Enter the password assigned to you. |
| Enable Wildcard | Your Prestige supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** This field is **N/A** when you choose DDNS client as your service provider. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

# CHAPTER 20
# Menu 2 WAN Backup Setup

This chapter describes how to configure traffic redirect and dial-backup using menu 2 and 2.1.

## 20.1 Introduction to WAN Backup Setup

This chapter explains how to configure the Prestige for traffic redirect and dial backup connections.

## 20.2 Configuring Dial Backup in Menu 2

From the main menu, enter 2 to open menu 2.

**Figure 112** Menu 2 WAN Backup Setup

```
                    Menu 2 - Wan Backup Setup

                Check Mechanism = DSL Link
                Check WAN IP Address1 = 0.0.0.0
                Check WAN IP Address2 = 0.0.0.0
                Check WAN IP Address3 = 0.0.0.0
                  KeepAlive Fail Tolerance = 0
                  Recovery Interval(sec) = 0
                  ICMP Timeout(sec) = 0
                Traffic Redirect = No

          Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 76** Menu 2 WAN Backup Setup

| FIELD | DESCRIPTION |
|---|---|
| Check Mechanism | Press [SPACE BAR] and then press [ENTER] to select the method that the Prestige uses to check the DSL connection.<br>Select **DSL Link** to have the Prestige check the DSL connection's physical layer. Select **ICMP** to have the Prestige periodically ping the IP addresses configured in the **Check WAN IP Address** fields. |
| Check WAN IP Address1-3 | Configure this field to test your Prestige's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). When using a WAN backup connection, the Prestige periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response. |

**Table 76** Menu 2 WAN Backup Setup (continued)

| FIELD | DESCRIPTION |
|---|---|
| KeepAlive Fail Tolerance | Type the number of times (2 recommended) that your Prestige may ping the IP addresses configured in the **Check WAN IP Address** field without getting a response before switching to a WAN backup connection (or a different WAN backup connection). |
| Recovery Interval(sec) | When the Prestige is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection.<br>Type the number of seconds (30 recommended) for the Prestige to wait between checks. Allow more time if your destination IP address handles lots of traffic. |
| ICMP Timeout | Type the number of seconds for an ICMP session to wait for the ICMP response |
| Traffic Redirect | Press [SPACE BAR] to select **Yes** or **No**.<br>Select **Yes** and press [ENTER] to configure **Menu 2.1 Traffic Redirect Setup**.<br>Select **No** (default) if you do not want to configure this feature. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

## 20.2.1 Traffic Redirect Setup

Configure parameters that determine when the Prestige will forward WAN traffic to the backup gateway using **Menu 2.1 — Traffic Redirect Setup**.

**Figure 113** Menu 2.1Traffic Redirect Setup

```
                    Menu 2.1 - Traffic Redirect Setup
                Active= No
                Configuration:
                  Backup Gateway IP Address= 0.0.0.0
                  Metric= 15

                Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 77** Menu 2.1Traffic Redirect Setup

| FIELD | DESCRIPTION |
|---|---|
| Active. | Press [SPACE BAR] and select **Yes** (to enable) or **No** (to disable) traffic redirect setup. The default is **No** |
| Configuration | |
| Backup Gateway IP Address | Enter the IP address of your backup gateway in dotted decimal notation.<br>The Prestige automatically forwards traffic to this IP address if the Prestige's Internet connection terminates. |

**Table 77** Menu 2.1Traffic Redirect Setup

| FIELD | DESCRIPTION |
|---|---|
| Metric | This field sets this route's priority among the routes the Prestige uses.<br>The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost" |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

# CHAPTER 21
# Menu 3 LAN Setup

This chapter covers how to configure your wired Local Area Network (LAN) settings.

## 21.1 LAN Setup

This section describes how to configure the Ethernet using **Menu 3 — LAN Setup**. From the main menu, enter 3 to display menu 3.

**Figure 114** Menu 3 LAN Setup

```
Menu 3 - LAN Setup

1. LAN Port Filter Setup
2. TCP/IP and DHCP Setup

5. Wireless LAN Setup

Enter Menu Selection Number:
```

### 21.1.1 General Ethernet Setup

This menu allows you to specify filter set(s) that you wish to apply to the Ethernet traffic. You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.

**Figure 115** Menu 3.1 LAN Port Filter Setup

```
Menu 3.1 - LAN Port Filter Setup

  Input Filter Sets:
    protocol filters=
    device filters=
  Output Filter Sets:
    protocol filters=
    device filters=

Press ENTER to Confirm or ESC to Cancel:
```

If you need to define filters, please read Chapter 29 on page 272 first, then return to this menu to define the filter sets.

## 21.2 Protocol Dependent Ethernet Setup

Depending on the protocols for your applications, you need to configure the respective Ethernet Setup, as outlined below.

- TCP/IP Ethernet setup
- Bridging Ethernet setup

# 21.3 TCP/IP Ethernet Setup and DHCP

Use menu 3.2 to configure your Prestige for TCP/IP.

To edit menu 3.2, enter 3 from the main menu to display **Menu 3 — LAN Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**, as shown next:

**Figure 116** Menu 3.2 TCP/IP and DHCP Ethernet Setup

```
                    Menu 3.2 - TCP/IP and DHCP Setup

DHCP Setup
  DHCP= Server
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 32
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0
  Remote DHCP Server= N/A
TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= None
    Version= N/A
  Multicast= None
  IP Policies=
  Edit IP Alias= No

Press ENTER to Confirm or ESC to Cancel:
```

Follow the instructions in the following table on how to configure the DHCP fields.

**Table 78** DHCP Ethernet Setup

| FIELD | DESCRIPTION |
|---|---|
| DHCP Setup | |
| DHCP | If set to **Server**, your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.<br>If set to **None**, the DHCP server will be disabled.<br>If set to **Relay**, the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server in this case.<br>When DHCP server is used, the following items need to be set: |
| Client IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Size of Client IP Pool | This field specifies the size or count of the IP address pool. |
| Primary DNS Server<br>Secondary DNS Server | Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask. |
| Remote DHCP Serve | If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here. |

Follow the instructions in the following table to configure TCP/IP parameters for the Ethernet port.

**Table 79** TCP/IP Ethernet Setup

| FIELD | DESCRIPTION |
|---|---|
| TCP/IP Setup | |
| IP Address | Enter the (LAN) IP address of your Prestige in dotted decimal notation |
| IP Subnet Mask | Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige (refer to the appendices for more information). |
| RIP Direction | Press [SPACE BAR] to select the RIP direction. Choices are **Both**, **In Only**, **Out Only** or **None**. |
| Version | Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**. |
| Multicast | IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it. |
| IP Policies | Create policies using SMT menu 25 and apply them on the Prestige LAN interface here. You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas. |
| Edit IP Alias | The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network. Press [SPACE BAR] to change **No** to **Yes** and press [ENTER] to display Menu 3.2.1. |

# CHAPTER 22
# Wireless LAN Setup

This chapter covers how to configure wireless LAN settings in SMT menu 3.5 for P-660HW and P-660W.

## 22.1 Wireless LAN Overview

Refer to the chapter on the wireless LAN screens for wireless LAN background information.

## 22.2 Wireless LAN Setup

Use menu 3.5 to set up your Prestige as the wireless access point. To edit menu 3.5, enter 3 from the main menu to display **Menu 3 – LAN Setup**. When menu 3 appears, press 5 and then press [ENTER] to display **Menu 3.5 – Wireless LAN Setup** as shown next.

**Figure 117** Menu 3.5 - Wireless LAN Setup

```
            Menu 3.5- Wireless LAN Setup
                        ESSID= Wireless
                        Hide ESSID= No
                        Channel ID= CH06 2437MHz
                        RTS Threshold= 2432
                        Frag. Threshold= 2432
                        WEP= Disable
                          Default Key= N/A
                          Key1= N/A
                          Key2= N/A
                          Key3= N/A
                          Key4= N/A
                        Edit MAC Address Filter= No

            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 80** Menu 3.5 - Wireless LAN Setup

| FIELD | DESCRIPTION |
|---|---|
| ESSID | The ESSID (Extended Service Set IDentifier) identifies the AP to which the wireless stations associate. Wireless stations associating to the Access Point must have the same ESSID. Enter a descriptive name of up to 32 printable 7-bit ASCII characters. |
| Hide ESSID | Press [SPACE BAR] and select **Yes** to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning. |

**Table 80** Menu 3.5 - Wireless LAN Setup (continued)

| FIELD | DESCRIPTION |
|---|---|
| Channel ID | Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/ channel depending on your particular region. |
| RTS Threshold | RTS(Request To Send) threshold (number of bytes) enables RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC Service Data Unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432. |
| Frag. Threshold | The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432. |
| WEP | WEP (Wired Equivalent Privacy) provides data encryption to prevent wireless stations from accessing data transmitted over the wireless network.<br>Select **Disable** allows wireless stations to communicate with the access points without any data encryption.<br>Select **64-bit WEP** or **128-bit WEP** to for the type of data encryption. WEP causes performance degradation. |
| Default Key | Enter the number of the key as an active key. |
| Key 1 to Key 4 | If you chose **64-bit WEP** in the **WEP Encryption** field, then enter 5 characters or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key (1-4).<br>If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key (1-4).<br>There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations. |
| Edit MAC Address Filter | To edit MAC address filtering table, press [SPACE BAR] to select **Yes** and press [ENTER] to open menu 3.5.1. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

## 22.2.1 Wireless LAN MAC Address Filter

The next layer of security is MAC address filter. To allow a wireless station to associate with the Prestige, enter the MAC address of the wireless LAN adapter on that wireless station in the MAC address table.

**Figure 118** Menu 3.5.1 WLAN MAC Address Filtering

```
                  Menu 3.5.1 - WLAN MAC Address Filter
                Active= No
                Filter Action= Allowed Association
------------------------------------------------------------------------------
  1=   00:00:00:00:00:00   13=   00:00:00:00:00:00   25=   00:00:00:00:00:00
  2=   00:00:00:00:00:00   14=   00:00:00:00:00:00   26=   00:00:00:00:00:00
  3=   00:00:00:00:00:00   15=   00:00:00:00:00:00   27=   00:00:00:00:00:00
  4=   00:00:00:00:00:00   16=   00:00:00:00:00:00   28=   00:00:00:00:00:00
  5=   00:00:00:00:00:00   17=   00:00:00:00:00:00   29=   00:00:00:00:00:00
  6=   00:00:00:00:00:00   18=   00:00:00:00:00:00   30=   00:00:00:00:00:00
  7=   00:00:00:00:00:00   19=   00:00:00:00:00:00   31=   00:00:00:00:00:00
  8=   00:00:00:00:00:00   20=   00:00:00:00:00:00   32=   00:00:00:00:00:00
  9=   00:00:00:00:00:00   21=   00:00:00:00:00:00
 10=   00:00:00:00:00:00   22=   00:00:00:00:00:00
 11=   00:00:00:00:00:00   23=   00:00:00:00:00:00
 12=   00:00:00:00:00:00   24=   00:00:00:00:00:00
------------------------------------------------------------------------------
                   Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

**Table 81** Menu 3.5.1 WLAN MAC Address Filtering

| FIELD | DESCRIPTION |
|---|---|
| Active | To enable MAC address filtering, press [SPACE BAR] to select **Yes** and press [ENTER]. |
| Filter Action | Define the filter action for the list of MAC addresses in the MAC address filter table.<br>To deny access to the Prestige, press [SPACE BAR] to select **Deny Association** and press [ENTER]. MAC addresses not listed will be allowed to access the router.<br>The default action, **Allowed Association**, permits association with the Prestige. MAC addresses not listed will be denied access to the router. |
| MAC Address Filter | |
| Address 1. | Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless stations that are allowed or denied access to the Prestige in these address fields. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

# CHAPTER 23
# Internet Access

This chapter shows you how to configure the LAN and WAN of your Prestige for Internet access.

## 23.1 Internet Access Overview

Refer to the chapters on the web configurator's wizard, LAN and WAN screens for more background information on fields in the SMT screens covered in this chapter.

## 23.2 IP Policies

Traditionally, routing is based on the destination address *only* and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. Create policies using SMT menu 25 and apply them on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN).

## 23.3 IP Alias

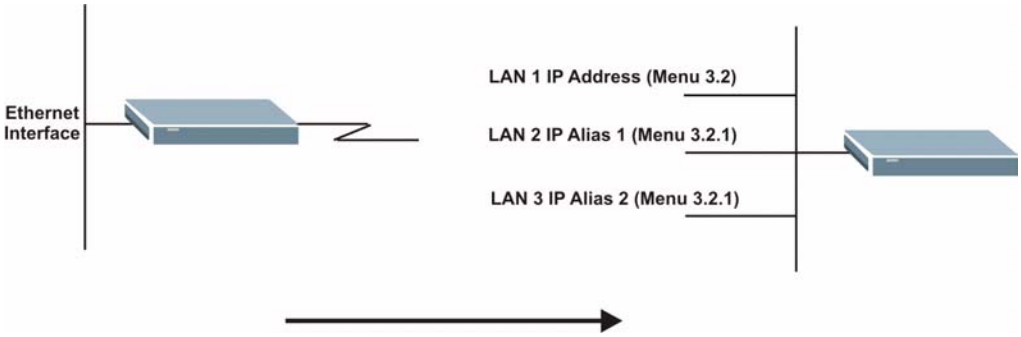
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

**Note:** Make sure that the subnets of the logical networks do not overlap.

The following figure shows a LAN divided into subnets A, B, and C.

**Figure 119** IP Alias Network Example




Use menu 3.2.1 to configure IP Alias on your Prestige.

## 23.4 IP Alias Setup

Use menu 3.2 to configure the first network. Move the cursor to **Edit IP Alias** field and press [SPACEBAR] to choose **Yes** and press [ENTER] to configure the second and third network.

**Figure 120** Menu 3.2 TCP/IP and DHCP Setup

```
                    Menu 3.2 - TCP/IP and DHCP Setup

                DHCP Setup
                  DHCP= Server
                  Client IP Pool Starting Address= 192.168.1.33
                  Size of Client IP Pool= 32
                  Primary DNS Server= 0.0.0.0
                  Secondary DNS Server= 0.0.0.0
                  Remote DHCP Server= N/A
                TCP/IP Setup:
                  IP Address= 192.168.1.1
                  IP Subnet Mask= 255.255.255.0
                  RIP Direction= None
                    Version= N/A
                  Multicast= None
                  IP Policies=
                  Edit IP Alias= No

                Press ENTER to Confirm or ESC to Cancel:
```

Pressing [ENTER] displays **Menu 3.2.1 — IP Alias Setup**, as shown next.

**Figure 121** Menu 3.2.1 IP Alias Setup

```
              Menu 3.2.1 - IP Alias Setup
                IP Alias 1= No
                  IP Address= N/A
                  IP Subnet Mask= N/A
                  RIP Direction= N/A
                  Version= N/A
                  Incoming protocol filters= N/A
                  Outgoing protocol filters= N/A
                IP Alias 2= No
                  IP Address= N/A
                  IP Subnet Mask= N/A
                  RIP Direction= N/A
                  Version= N/A
                  Incoming protocol filters= N/A
                  Outgoing protocol filters= N/A

                   Enter here to CONFIRM or ESC to CANCEL:
```

Follow the instructions in the following table to configure IP Alias parameters.

**Table 82** Menu 3.2.1 IP Alias Setup

| FIELD | DESCRIPTION |
|---|---|
| IP Alias | Choose **Yes** to configure the LAN network for the Prestige. |
| IP Address | Enter the IP address of your Prestige in dotted decimal notation |
| IP Subnet Mask | Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige |
| RIP Direction | Press [SPACE BAR] to select the RIP direction. Choices are **None**, **Both**, **In Only** or **Out Only**. |
| Version | Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**. |
| Incoming Protocol Filters | Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige. |
| Outgoing Protocol Filters | Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

# 23.5 Route IP Setup

The first step is to enable the IP routing in **Menu 1 — General Setup**.

To edit menu 1, type 1 in the main menu and press [ENTER]. Set the **Route IP** field to **Yes** by pressing [SPACE BAR].

**Figure 122** Menu 1 General Setup

```
Menu 1 - General Setup
          System Name= ?
          Location= location
          Contact Person's Name=
          Domain Name=
          Edit Dynamic DNS= No
          Route IP= Yes
          Bridge= No

Press ENTER to Confirm or ESC to Cancel:
```

# 23.6 Internet Access Configuration

Menu 4 allows you to enter the Internet Access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in menu 11. Before you configure your Prestige for Internet access, you need to collect your Internet account information.

Use the *Internet Account Information* table in the *Quick Start Guide* to record your. Note that if you are using PPPoA or PPPoE encapsulation, then the only ISP information you need is a login name and password. You only need to know the Ethernet Encapsulation Gateway IP address if you are using ENET ENCAP encapsulation.

From the main menu, type 4 to display **Menu 4 - Internet Access Setup**, as shown next.

**Figure 123** Menu 4 Internet Access Setup

```
Menu 4 - Internet Access Setup
  ISP's Name= MyISP
  Encapsulation= RFC 1483
  Multiplexing= LLC-based
  VPI #= 8
  VCI #= 35
  ATM QoS Type= CBR
    Peak Cell Rate (PCR)= 0
    Sustain Cell Rate (SCR)= 0
    Maximum Burst Size (MBS)= 0
  My Login= N/A
  My Password= N/A
  ENET ENCAP Gateway= N/A
  IP Address Assignment= Static
    IP Address= 0.0.0.0
  Network Address Translation= SUA Only
    Address Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:
```

The following table contains instructions on how to configure your Prestige for Internet access

.

**Table 83** Menu 4 Internet Access Setup

| FIELD | DESCRIPTION |
|---|---|
| ISP's Name | Enter the name of your Internet Service Provider (ISP). This information is for identification purposes only. |
| Encapsulation | Press [SPACE BAR] to select the method of encapsulation used by your ISP. Choices are **PPPoE**, **PPPoA**, **RFC 1483** or **ENET ENCAP**. |
| Multiplexing | Press [SPACE BAR] to select the method of multiplexing used by your ISP. Choices are **VC-based** or **LLC-based**. |
| VPI # | Enter the Virtual Path Identifier (VPI) assigned to you. |
| VCI # | Enter the Virtual Channel Identifier (VCI) assigned to you. |
| ATM QoS Type | Press [SPACE BAR] and select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR** (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications. |
| Peak Cell Rate (PCR) | This is the maximum rate at which the sender can send cells. Type the PCR. |
| Sustain Cell Rate (SCR)= 0 | Sustained Cell Rate is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-traffic. Type the SCR; it must be less than the PCR. |
| Maximum Burst Size (MBS)= 0 | Refers to the maximum number of cells that can be sent at the peak rate. Type the MBS. The MBS must be less than 65535. |
| My Login | Configure the **My Login** and **My Password** fields for PPPoA and PPPoE encapsulation only. Enter the login name that your ISP gives you. If you are using PPPoE encapsulation**,** then this field must be of the form user@domain where domain identifies your PPPoE service name. |
| My Password | Enter the password associated with the login name above. |
| ENET ENCAP Gateway | Enter the gateway IP address supplied by your ISP when you are using **ENET ENCAP** encapsulation. |
| Idle Timeout | This value specifies the number of idle seconds that elapse before the Prestige automatically disconnects the PPPoE session. |
| IP Address Assignment | Press [SPACE BAR] to select **Static** or **Dynamic** address assignment. |
| IP Address | Enter the IP address supplied by your ISP if applicable. |
| Network Address Translation | Press [SPACE BAR] to select **None**, **SUA Only** or **Full Feature**. Please see the NAT chapter for more details on the SUA (Single User Account) feature. |
| Address Mapping Set | Type the numbers of mapping sets (1-8) to use with NAT. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

If all your settings are correct your Prestige should connect automatically to the Internet. If the connection fails, note the error message that you receive on the screen and take the appropriate troubleshooting steps.

# CHAPTER 24
# Remote Node Configuration

This chapter covers remote node configuration.

## 24.1 Remote Node Setup Overview

This section describes the protocol-independent parameters for a remote node. A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. When you use menu 4 to set up Internet access, you are configuring one of the remote nodes.

You first choose a remote node in **Menu 11- Remote Node Setup**. You can then edit that node's profile in menu 11.1, as well as configure specific settings in three submenus: edit IP and bridge options in menu 11.3; edit ATM options in menu 11.6; and edit filter sets in menu 11.5.

## 24.2 Remote Node Setup

This section describes the protocol-independent parameters for a remote node.

### 24.2.1 Remote Node Profile

To configure a remote node, follow these steps:

1. From the main menu, enter 11 to display **Menu 11 - Remote Node Setup.**
2. When menu 11 appears, as shown in the following figure, type the number of the remote node that you want to configure.

**Figure 124** Menu 11 Remote Node Setup

```
                Menu 11 - Remote Node Setup
          1. MyISP (ISP, SUA)
          2. _________
          3. _________
          4. _________
          5. _________
          6. _________
          7. _________
          8. _________

                   Enter Node # to Edit:
```

## 24.2.2 Encapsulation and Multiplexing Scenarios

For Internet access you should use the encapsulation and multiplexing methods used by your ISP. Consult your telephone company for information on encapsulation and multiplexing methods for LAN-to-LAN applications, for example between a branch office and corporate headquarters. There must be prior agreement on encapsulation and multiplexing methods because they cannot be automatically determined. What method(s) you use also depends on how many VCs you have and how many different network protocols you need. The extra overhead that ENET ENCAP encapsulation entails makes it a poor choice in a LAN-to-LAN application. Here are some examples of more suitable combinations in such an application.

### 24.2.2.1 Scenario 1: One VC, Multiple Protocols

**PPPoA** (RFC-2364) encapsulation with **VC-based** multiplexing is the best combination because no extra protocol identifying headers are needed. The **PPP** protocol already contains this information.

### 24.2.2.2 Scenario 2: One VC, One Protocol (IP)

Selecting **RFC-1483** encapsulation with **VC-based** multiplexing requires the least amount of overhead (0 octets). However, if there is a potential need for multiple protocol support in the future, it may be safer to select **PPPoA** encapsulation instead of **RFC-1483**, so you do not need to reconfigure either computer later.

### 24.2.2.3 Scenario 3: Multiple VCs

If you have an equal number (or more) of VCs than the number of protocols, then select **RFC-1483** encapsulation and **VC-based** multiplexing.

**Figure 125** Menu 11.1 Remote Node Profile

```
                Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP                  Route= IP
Active= Yes                           Bridge= No
Encapsulation= RFC 1483               Edit IP/Bridge= No
Multiplexing= LLC-based               Edit ATM Options= No
Service Name= N/A                     Edit Advance Options= N/A
Incoming:                             Telco Option:
  Rem Login= N/A                        Allocated Budget(min)= N/A
  Rem Password= N/A                     Period(hr)= N/A
Outgoing:                               Schedule Sets= N/A
  My Login= N/A                         Nailed-Up Connection= N/A
  My Password= N/A                    Session Options:
  Authen= N/A                           Edit Filter Sets= No
                                          Idle Timeout(sec)= N/A
Press ENTER to Confirm or ESC to Cancel:
```

In **Menu 11.1 – Remote Node Profile**, fill in the fields as described in the following table.

**Table 84** Menu 11.1 Remote Node Profile

| FIELD | DESCRIPTION |
|---|---|
| Rem Node Name | Type a unique, descriptive name of up to eight characters for this node. |
| Active | Press [SPACE BAR] and then [ENTER] to select **Yes** to activate or **No** to deactivate this node. Inactive nodes are displayed with a minus sign –" in SMT menu 11. |
| Encapsulation | **PPPoA** refers to RFC-2364 (PPP Encapsulation over ATM Adaptation Layer 5).<br>If RFC-1483 (Multiprotocol Encapsulation over ATM Adaptation Layer 5) of **ENET ENCAP** are selected,<br>then the **Rem Login**, **Rem Password**, **My Login**, **My Password** and **Authen** fields are not applicable (**N/A**). |
| Multiplexing | Press [SPACE BAR] and then [ENTER] to select the method of multiplexing that your ISP uses, either **VC-based** or **LLC-based**. |
| Service Name | When using **PPPoE** encapsulation, type the name of your PPPoE service here. |
| Incoming: | |
| Rem Login | Type the login name that this remote node will use to call your Prestige. The login name and the **Rem Password** will be used to authenticate this node. |
| Rem Password | Type the password used when this remote node calls your Prestige. |
| Outgoing: | |
| My Login | Type the login name assigned by your ISP when the Prestige calls this remote node. |
| My Password | Type the password assigned by your ISP when the Prestige calls this remote node. |
| Authen | This field sets the authentication protocol used for outgoing calls. Options for this field are: |
| | **CHAP**/**PAP** – Your Prestige will accept either **CHAP** or **PAP** when requested by this remote node. |
| | **CHAP** – accept **CHAP** (Challenge Handshake Authentication Protocol) only. |

**Table 84** Menu 11.1 Remote Node Profile (continued)

| FIELD | DESCRIPTION |
|---|---|
| | **PAP** – accept PAP (Password Authentication Protocol) only. |
| Route | This field determines the protocol used in routing. Options are **IP** and **None.** |
| Bridge | When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. Select **Yes** to enable and **No** to disable. |
| Edit IP/Bridge | Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options**. |
| Edit ATM Options | Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.6 – Remote Node ATM Layer Options**. |
| Edit Advance Options | This field is only available when you select **PPPoE** in the **Encapsulation** field.<br>Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.8 – Advance Setup Options**. |
| Telco Option | |
| Allocated Budget (min) | This sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control. |
| Period (hr) | This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period (hr)** is 1 (hour). |
| Schedule Sets | This field is only applicable for **PPPoE** and **PPPoA** encapsulation. You can apply up to four schedule sets here. For more details please refer to Chapter 37 on page 338. |
| Nailed up Connection | This field is only applicable for **PPPoE** and **PPPoA** encapsulation. This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section. |
| Session Options | |
| Edit Filter Sets | Use [SPACE BAR] to choose **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See Chapter 29 on page 272 for more details. |
| Idle Timeout (sec) | Type the number of seconds (0-9999) that can elapse when the Prestige is idle (there is no traffic going to the remote node), before the Prestige automatically disconnects the remote node. 0 means that the session will not timeout. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

## 24.2.3 Outgoing Authentication Protocol

For obvious reasons, you should employ the strongest authentication protocol possible. However, some vendors' implementation includes specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If the peer disconnects right after a successful authentication, make sure that you specify the correct authentication protocol when connecting to such an implementation.

## 24.3 Remote Node Network Layer Options

For the TCP/IP parameters, perform the following steps to edit **Menu 11.3 – Remote Node Network Layer Options** as shown next.

1. In menu 11.1, make sure **IP** is among the protocols in the **Route** field.
2. Move the cursor to the **Edit IP/Bridge** field, press [SPACE BAR] to select **Yes,** then press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options.**

**Figure 126** Menu 11.3 Remote Node Network Layer Options

```
            Menu 11.3 - Remote Node Network Layer Options
IP Options:                          Bridge Options:
  IP Address Assignment = Static       Ethernet Addr Timeout(min)= N/A
  Rem IP Addr = 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= SUA Only
    Address Mapping Set= N/A
  Metric= 2
  Private= No
  RIP Direction= None
    Version= RIP-1
  Multicast= None
  IP Policies=

            Enter here to CONFIRM or ESC to CANCEL:
```

The next table explains fields in **Menu 11.3 – Remote Node Network Layer Options**.

**Table 85** Menu 11.3 Remote Node Network Layer Options

| FIELD | DESCRIPTION |
|---|---|
| IP Address Assignment | Press [SPACE BAR] and then [ENTER] to select **Dynamic** if the remote node is using a dynamically assigned IP address or **Static** if it is using a static (fixed) IP address. You will only be able to configure this in the ISP node (also the one you configure in menu 4), all other nodes are set to **Static**. |
| Rem IP Addr | This is the IP address you entered in the previous menu. |
| Rem Subnet Mask | Type the subnet mask assigned to the remote node. |
| My WAN Addr | Some implementations, especially UNIX derivatives, require separate IP network numbers for the WAN and LAN links and each end to have a unique address within the WAN network number. In that case, type the IP address assigned to the WAN port of your Prestige.<br>NOTE: Refers to local Prestige address, not the remote router address. |
| NAT | Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your Prestige. |
| | Select **SUA Only** if you have just one public WAN IP address for your Prestige. The SMT uses Address Mapping Set 255 (seeFigure 144 on page 257).<br>Select **None** to disable NAT. |

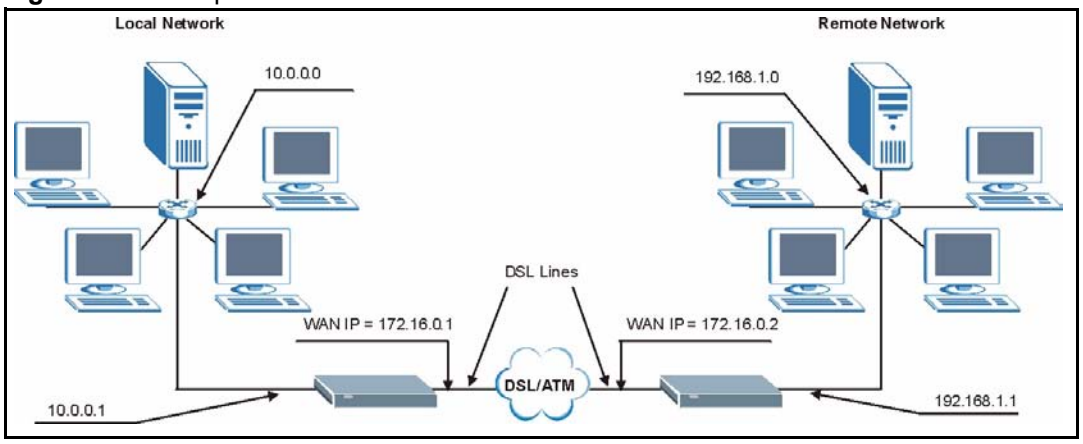
**Table 85** Menu 11.3 Remote Node Network Layer Options (continued)

| FIELD | DESCRIPTION |
|---|---|
| Address Mapping Set | When **Full Feature** is selected in the **NAT** field, configure address mapping sets in menu 15.1. Select one of the NAT server sets (2-10) in menu 15.2 (see Chapter 27 on page 254 for details) and type that number here.<br>When **SUA Only** is selected in the NAT field, the SMT uses NAT server set 1 in menu 15.2 (see Chapter 27 on page 254 for details). |
| Metric | The metric represents the cost of transmission for routing purposes. IP routing uses hop count as the cost measurement, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number. |
| Private | This determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts. |
| RIP Direction | Press [SPACE BAR] and then [ENTER] to select the RIP Direction. Options are **Both**, **In Only**, **Out Only** or **None**. |
| Version | Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**. |
| Multicast | **IGMP-v1** sets IGMP to version 1, **IGMP-v2** sets IGMP to version 2 and **None** disables IGMP. |
| IP Policies | You can apply up to four IP Policy sets (from 12) by typing in their numbers separated by commas. Configure the filter sets in menu 25 first (see Chapter 36 on page 328) and then apply them here. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

## 24.3.1 My WAN Addr Sample IP Addresses

The following figure uses sample IP addresses to help you understand the field of **My WAN Addr** in menu 11.3. **My WAN Addr** indicates the local Prestige WAN IP (172.16.0.1 in the following figure) while **Rem IP Addr** indicates the peer WAN IP (172.16.0.2 in the following figure).

**Figure 127** Sample IP Addresses for a TCP/IP LAN-to-LAN Connection




## 24.4 Remote Node Filter

Move the cursor to the **Edit Filter Sets** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.5 – Remote Node Filter**.

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige and also to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by comma, for example, 1, 5, 9, 12, in each filter field.

Note that spaces are accepted in this field. The Prestige has a prepackaged filter set, NetBIOS_WAN, that blocks NetBIOS packets. Include this in the call filter sets if you want to prevent NetBIOS packets from triggering calls to a remote node.

**Figure 128** Menu 11.5 Remote Node Filter (RFC 1483 or ENET Encapsulation)

```
            Menu 11.5 - Remote Node Filter
                     Input Filter Sets:
                       protocol filters=
                         device filters=
                     Output Filter Sets:
                       protocol filters=
                         device filters=

            Enter here to CONFIRM or ESC to CANCEL:
```

**Figure 129** Menu 11.5 Remote Node Filter (PPPoA or PPPoE Encapsulation)

```
                    Menu 11.5 - Remote Node Filter
                Input Filter Sets:
                  protocol filters=
                    device filters=
                Output Filter Sets:
                  protocol filters=
                    device filters=
                Call Filter Sets:
                  protocol filters=
                    device filters=

                 Enter here to CONFIRM or ESC to CANCEL:
```

# 24.5 Editing ATM Layer Options

Follow the steps shown next to edit **Menu 11.6 – Remote Node ATM Layer Options**.

In menu 11.1, move the cursor to the **Edit ATM Options** field and then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.6 – Remote Node ATM Layer Options**.

There are two versions of menu 11.6 for the Prestige, depending on whether you chose **VC-based**/**LLC-based** multiplexing and **PPP** encapsulation in menu 11.1.

## 24.5.1 VC-based Multiplexing (non-PPP Encapsulation)

For **VC-based** multiplexing, by prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. Separate VPI and VCI numbers must be specified for each protocol.

**Figure 130** Menu 11.6 for VC-based Multiplexing

```
          Menu 11.6 - Remote Node ATM Layer Options
          VPI/VCI (VC-Multiplexing)

VC Options for IP:            VC Options for Bridge:
  VPI #= 8                      VPI #= 1
  VCI #= 35                     VCI #= 36
  ATM QoS Type= UBR             ATM QoS Type= N/A
  Peak Cell Rate (PCR)= 0       Peak Cell Rate (PCR)= N/A
  Sustain Cell Rate (SCR)= 0    Sustain Cell Rate (SCR)= N/A
  Maximum Burst Size (MBS)= 0   Maximum Burst Size (MBR)= N/A

             Enter here to CONFIRM or ESC to CANCEL:
```

## 24.5.2 LLC-based Multiplexing or PPP Encapsulation

For **LLC-based** multiplexing or **PPP** encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header.

**Figure 131** Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation

```
            Menu 11.6 - Remote Node ATM Layer Options
            VPI/VCI (LLC-Multiplexing or PPP-Encapsulation)
                                  VPI #= 0
                                  VCI #= 38
                                  ATM QoS Type= UBR
                                  Peak Cell Rate (PCR)= 0
                                  Sustain Cell Rate (SCR)= 0
                                  Maximum Burst Size (MBS)= 0

            ENTER here to CONFIRM or ESC to CANCEL:
```

In this case, only one set of VPI and VCI numbers need be specified for all protocols. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (1 to 31 is reserved for local management of ATM traffic).

## 24.5.3 Advance Setup Options

In menu 11.1, select **PPPoE** in the **Encapsulation** field.

**Figure 132** Menu 11.1 Remote Node Profile

```
                  Menu 11.1 - Remote Node Profile
Rem Node Name= MyISP                  Route= IP
Active= Yes                           Bridge= No
Encapsulation= PPPoE                Edit IP/Bridge= No
Multiplexing= LLC-based               Edit ATM Options= No
Service Name=                         Edit Advance Options= Yes
Incoming:                             Telco Option:
  Rem Login=                            Allocated Budget(min)= 0
  Rem Password= ********                Period(hr)= 0
Outgoing:                               Schedule Sets=
  My Login= ?                           Nailed-Up Connection= No
  My Password= ?                      Session Options:
  Authen= CHAP/PAP                      Edit Filter Sets= No
                                        Idle Timeout(sec)= 0

                Press ENTER to Confirm or ESC to Cancel:
```

Move the cursor to the **Edit Advance Options** field, press [SPACE BAR] to select **Yes,** then press [ENTER] to display **Menu 11.8 – Advance Setup Options**.

**Figure 133** Menu 11.8 Advance Setup Options

```
                        Menu 11.8 - Advance Setup Options

                    PPPoE pass-through= No

                    Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 86** Menu 11.8 Advance Setup Options

| FIELD | DESCRIPTION |
|---|---|
| PPPoE pass-through | Press [SPACE BAR] to select **Yes** and press [ENTER] to enable PPPoE pass through. In addition to the Prestige's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the Prestige. Each host can have a separate account and a public WAN IP address.<br>PPPoE pass through is an alternative to NAT for applications where NAT is not appropriate.<br>Press [SPACE BAR] to select **No** and press [ENTER] to disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

# CHAPTER 25
# Static Route Setup

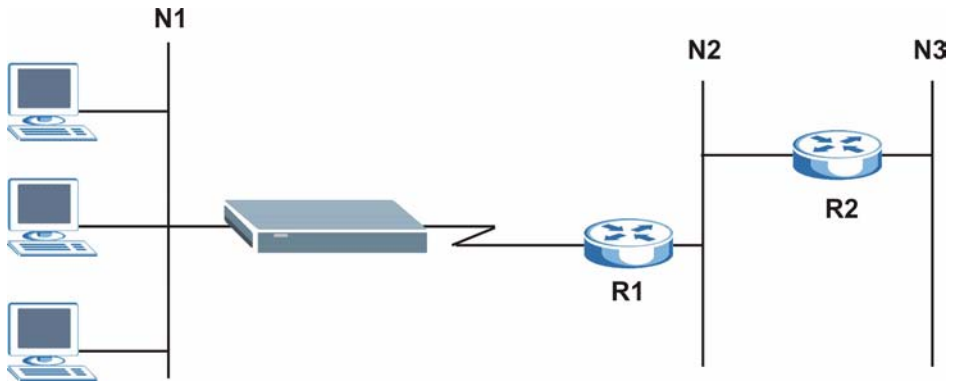
This chapter shows how to setup IP static routes.

## 25.1 IP Static Route Overview

Static routes tell the Prestige routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

Each remote node specifies only the network to which the gateway is directly connected and the Prestige has no knowledge of the networks beyond. For instance, the Prestige knows about network N2 in the following figure through remote node Router 1. However, the Prestige is unable to route a packet to network N3 because it does not know that there is a route through remote node Router 1 (via Router 2). The static routes allow you to tell the Prestige about the networks beyond the remote nodes.

**Figure 134** Sample Static Routing Topology




## 25.2 Configuration

To configure an IP static route, use **Menu 12 – Static Route Setup** (shown next).

**Figure 135** Menu 12 Static Route Setup

```
                    Menu 12 - Static Route Setup

               1. IP Static Route

               3. Bridge Static Route

                       Please enter selection:
```

From menu 12, select 1 to open **Menu 12.1 — IP Static Route Setup** (shown next).

**Figure 136** Menu 12.1 IP Static Route Setup

```
                        Menu 12.1 - IP Static Route Setup
                    1. _________
                    2. _________
                    3. _________
                    4. _________
                    5. _________
                    6. _________
                    7. _________
                    8. _________
                    9. _________
                    10. _________
                    11. _________
                    12. _________
                    13. _________
                    14. _________
                    15. _________
                    16. _________

                Enter selection number:
```

Now, type the route number of a static route you want to configure.

**Figure 137** Menu12.1.1 Edit IP Static Route

```
            Menu 12.1.1 - Edit IP Static Route
                        Route #: 1
                        Route Name= ?
                        Active= No
                        Destination IP Address= ?
                        IP Subnet Mask= ?
                        Gateway IP Address= ?
                        Metric= 2
                        Private= No

             Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields for **Menu 12.1.1 – Edit IP Static Route Setup**.

**Table 87** Menu12.1.1 Edit IP Static Route

| FIELD | DESCRIPTION |
|---|---|
| Route # | This is the index number of the static route that you chose in menu 12.1. |
| Route Name | Type a descriptive name for this route. This is for identification purpose only. |
| Active | This field allows you to activate/deactivate this static route. |
| Destination IP Address | This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. |
| IP Subnet Mask | Type the subnet mask for this destination. |
| Gateway IP Address | Type the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. |
| Metric | Metric represents the cost of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number. |
| Private | This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and is not included in RIP broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

# CHAPTER 26
# Bridging Setup

This chapter shows you how to configure the bridging parameters of your Prestige.

## 26.1 Bridging in General

Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does it on the network layer (IP) address. Bridging allows the Prestige to transport packets of network layer protocols that it does not route, for example, SNA, from one network to another. The caveat is that, compared to routing, bridging generates more traffic for the same network layer protocol, and it also demands more CPU cycles and memory.

For efficiency reasons, do *not* turn on bridging unless you need to support protocols other than IP on your network. For IP, enable the routing if you need it; do not bridge what the Prestige can route.

## 26.2 Bridge Ethernet Setup

Basically, all non-local packets are bridged to the WAN. Your Prestige does not support IPX.

### 26.2.1 Remote Node Bridging Setup

Follow the procedure in another section to configure the protocol-independent parameters in **Menu 11.1 – Remote Node Profile**. For bridging-related parameters, you need to configure **Menu 11.3 – Remote Node Network Layer Options**.

1. To setup **Menu 11.3 – Remote Node Network Layer Options** shown in the next figure, follow these steps:
2. In menu 11.1, make sure the **Bridge** field is set to **Yes**.

**Figure 138** Menu 11.1 Remote Node Profile

```
                Menu 11.1 - Remote Node Profile
  Rem Node Name= ?                      Route= IP
  Active= Yes                           Bridge= Yes
  Encapsulation= ENET ENCAP             Edit IP/Bridge= No
  Multiplexing= VC-based                Edit ATM Options= No
  Service Name= N/A                     Edit Advance Options= N/A
  Incoming:                             Telco Option:
    Rem Login= N/A                        Allocated Budget(min)= N/A
    Rem Password= N/A                     Period(hr)= N/A
  Outgoing:                               Schedule Sets= N/A
    My Login= N/A                         Nailed-Up Connection= N/A
    My Password= N/A                    Session Options:
    Authen= N/A                           Edit Filter Sets= No
                                          Idle Timeout(sec)= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

**3** Move the cursor to the **Edit IP/Bridge** field, then press [SPACE BAR] to set the value to **Yes** and press [ENTER] to edit **Menu 11.3 – Remote Node Network Layer Options**.

**Figure 139** Menu 11.3 Remote Node Network Layer Options

```
            Menu 11.3 - Remote Node Network Layer Options
 IP Options:                          Bridge Options:
   IP Address Assignment= Static        Ethernet Addr Timeout (min)= 0
   Rem IP Addr: 0.0.0.0
   Rem Subnet Mask= 0.0.0.0
   My WAN Addr= 0.0.0.0
   NAT= Full Feature
     Address Mapping Set=2
   Metric= 2
   Private= No
   RIP Direction= Both
     Version= RIP-2B
   Multicast= IGMP-v2
   IP Policies=

            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 88** Remote Node Network Layer Options: Bridge Fields

| FIELD | DESCRIPTION |
|---|---|
| Bridge (menu 11.1) | Make sure this field is set to **Yes**. |
| Edit IP/Bridge (menu 11.1) | Press [SPACE BAR] to select **Yes** and press [ENTER] to display menu 11.3. |
| Ethernet Addr Timeout (min.) (menu 11.3) | Type the time (in minutes) for the Prestige to retain the Ethernet Address information in its internal tables while the line is down. If this information is retained, your Prestige will not have to recompile the tables when the line comes back up. |

## 26.2.2 Bridge Static Route Setup

Similar to network layer static routes, a bridging static route tells the Prestige the route to a node before a connection is established. You configure bridge static routes in menu 12.3.1 (go to menu 12, choose option 3, then choose a static route to edit) as shown next.

**Figure 140** Menu 12.3.1 Edit Bridge Static Route

```
Menu 12.3.1 - Edit Bridge Static Route
Route #: 1
Route Name=
Active= No
Ether Address= ?
IP Address=
Gateway Node= 1

Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the **Edit Bridge Static Route** menu.

**Table 89** Menu 12.3.1 Edit Bridge Static Route

| FIELD | DESCRIPTION |
|---|---|
| Route # | This is the route index number you typed in **Menu 12.3 – Bridge Static Route Setup**. |
| Route Name | Type a name for the bridge static route for identification purposes. |
| Active | Indicates whether the static route is active (**Yes**) or not (**No**). |
| Ether Address | Type the MAC address of the destination computer that you want to bridge the packets to. |
| IP Address | If available, type the IP address of the destination computer that you want to bridge the packets to. |
| Gateway Node | Press [SPACE BAR] and then [ENTER] to select the number of the remote node (one to eight) that is the gateway of this static route. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

# CHAPTER 27
# Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

## 27.1 Using NAT

You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the Prestige.

### 27.1.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See Section 27.3 on page 256 or a detailed description of the NAT set for SUA. The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.

- Choose **SUA Only** if you have just one public WAN IP address for your Prestige.
- Choose **Full Feature** if you have multiple public WAN IP addresses for your Prestige.

## 27.2 Applying NAT

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

**Figure 141** Menu 4 Applying NAT for Internet Access

```
            Menu 4 - Internet Access Setup
                        ISP's Name= MyISP
                        Encapsulation= RFC 1483
                        Multiplexing= LLC-based
                        VPI #= 8
                        VCI #= 35
                        ATM QoS Type= UBR
                          Peak Cell Rate (PCR)= 0
                          Sustain Cell Rate (SCR)= 0
                          Maximum Burst Size (MBS)= 0
                        My Login= N/A
                        My Password= N/A
                        ENET ENCAP Gateway= N/A
                        IP Address Assignment= Static
                          IP Address= 0.0.0.0
                        Network Address Translation= SUA Only
                          Address Mapping Set= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

The following figure shows how you apply NAT to the remote node in menu 11.1.

1. Enter 11 from the main menu.
2. When menu 11 appears, as shown in the following figure, type the number of the remote node that you want to configure.
3. Move the cursor to the **Edit IP/Bridge** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options.**

**Figure 142** Applying NAT in Menus 4 & 11.3

```
            Menu 11.3 - Remote Node Network Layer Options
IP Options:                          Bridge Options:
  IP Address Assignment = Static       Ethernet Addr Timeout(min)= N/A
  Rem IP Addr = 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= SUA Only
    Address Mapping Set= N/A
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= None
  IP Policies=

            Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the options for Network Address Translation.

**Table 90** Applying NAT in Menus 4 & 11.3

| FIELD | DESCRIPTION |
|---|---|
| NAT | Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your Prestige. The SMT uses the address mapping set that you configure and enter in the **Address Mapping Set** field (seeFigure 144 on page 257). |
| | Select **None** to disable NAT. |
| | When you select **SUA Only**, the SMT uses Address Mapping Set 255 (seeFigure 145 on page 257). Choose **SUA Only** if you have just one public WAN IP address for your Prestige. |

# 27.3 NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see the web configurator NAT chapter for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

**Figure 143** Menu 15 NAT Setup

```
              Menu 15 - NAT Setup

                    1. Address Mapping Sets

                    2. NAT Server Sets

              Enter Menu Selection Number:
```

## 27.3.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 — Address Mapping Sets**.

**Figure 144** Menu 15.1 Address Mapping Sets

```
            Menu 15.1 - Address Mapping Sets
                     1.
                     2.
                     3.
                     4.
                     5.
                     6.
                     7.
                     8.
                   255. SUA (read only)

            Enter Menu Selection Number:
```

### 27.3.1.1 SUA Address Mapping Set

Enter 255 to display the next screen (see also Section 27.1.1 on page 254). The fields in this menu cannot be changed.

**Figure 145** Menu 15.1.255 SUA Address Mapping Rules

```
            Menu 15.1.255 - Address Mapping Rules
 Set Name=
Idx  Local Start IP   Local End IP     Global Start IP  Global End IP  Type
---  ---------------  ---------------  ---------------  -------------  ----
 1.  0.0.0.0          255.255.255.255  0.0.0.0                          M-1
 2.                                 0.0.0.0                         Server
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

              Press ENTER to Confirm or ESC to Cancel:
```

The following table explains the fields in this menu.

Menu 15.1.255 is read-only.

**Table 91** SUA Address Mapping Rules

| FIELD | DESCRIPTION |
|---|---|
| Set Name | This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create. |
| Idx | This is the index or rule number. |
| Local Start IP | **Local Start IP** is the starting local IP address (ILA). |

**Table 91** SUA Address Mapping Rules (continued)

| FIELD | DESCRIPTION |
|---|---|
| Local End IP | **Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255. |
| Global Start IP | This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**. |
| Global End IP | This is the ending global IP address (IGA). |
| Type | These are the mapping types. Server allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

### 27.3.1.2 User-Defined Address Mapping Sets

Now let's look at option 1 in menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

**Figure 146** Menu 15.1.1 First Set

```
            Menu 15.1.1 - Address Mapping Rules
 Set Name= NAT_SET
Idx  Local Start IP   Local End IP     Global Start IP  Global End IP   Type
---  ---------------  ---------------  ---------------  --------=-----  ---
 1.
 2
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

            Action= Edit          Select Rule=

            Press ENTER to Confirm or ESC to Cancel:
```

If the **Set Name** field is left blank, the entire set will be deleted.

The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

### 27.3.1.3 Ordering Your Rules

Ordering your rules is important because the Prestige applies the rules in the order that you specify. When a rule matches the current packet, the Prestige takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

**Table 92** Menu 15.1.1 First Set

| FIELD | DESCRIPTION |
|---|---|
| Set Name | Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted. |
| Action | The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item. |
| Select Rule | When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question. |

You must press **[ENTER]** at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

An End IP address must be numerically greater than its corresponding IP Start address.

**Figure 147** Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

```
              Menu 15.1.1.1 Address Mapping Rule
                   Type= One-to-One
                   Local IP:
                     Start=
                     End  = N/A
                   Global IP:
                     Start=
                     End  = N/A
                   Server Mapping Set= N/A

              Press ENTER to Confirm or ESC to Cancel:
```

The following table explains the fields in this menu.

**Table 93** Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

| FIELD | DESCRIPTION |
|---|---|
| Type | Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in the web configurator NAT chapter. Server allows you to specify multiple servers of different types behind NAT to this computer. |
| Local IP | Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**. |
| Start | This is the starting local IP address (ILA). |
| End | This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types. |
| Global IP | |
| Start | This is the starting inside global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server.** |
| End | This is the ending inside global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**. |
| Server Mapping Set | Only available when **Type** is set to **Server**. Type a number from 1 to 10 to choose a server set from menu 15.2. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

## 27.4 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.
2. Enter 2 to display **Menu 15.2 - NAT Server Sets** as shown next.

**Figure 148** Menu 15.2 NAT Server Setup

```
            Menu 15.2 - NAT Server Sets
                    1. Server Set 1 (Used for SUA Only)
                    2. Server Set 2
                    3. Server Set 3
                    4. Server Set 4
                    5. Server Set 5
                    6. Server Set 6
                    7. Server Set 7
                    8. Server Set 8
                    9. Server Set 9
                   10. Server Set 10

                     Enter Set Number to Edit:
```

3. Enter 1 to go to **Menu 15.2.1 NAT Server Setup** as follows.

**Figure 149** Menu 15.2.1 NAT Server Setup

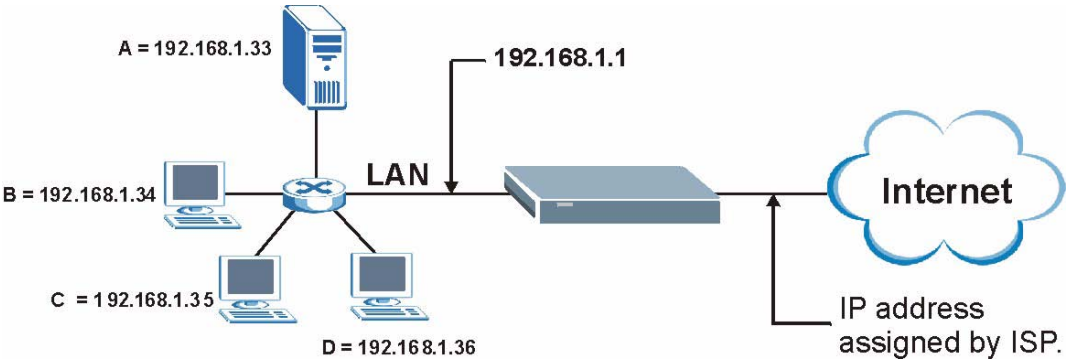
```
          Menu 15.2 - NAT Server Setup
 Rule    Start Port No.    End Port No.    IP Address
-------------------------------------------------------
   1.     Default           Default         0.0.0.0
   2.       21                21            192.168.1.33
   3.       0                 0             0.0.0.0
   4.       0                 0             0.0.0.0
   5.       0                 0             0.0.0.0
   6.       0                 0             0.0.0.0
   7.       0                 0             0.0.0.0
   8.       0                 0             0.0.0.0
   9.       0                 0             0.0.0.0
  10.       0                 0             0.0.0.0
  11.       0                 0             0.0.0.0
  12.       0                 0             0.0.0.0

          Press ENTER to Confirm or ESC to Cancel:
```

4 Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.

5 Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

6 Press [ENTER] at the "`Press ENTER to confirm ...`" prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

**Figure 150** Multiple Servers Behind NAT Example




## 27.5 General NAT Examples

The following are some examples of NAT configuration.

### 27.5.1 Example 1: Internet Access Only

In the following Internet access example, you only need one rule where your ILAs (Inside Local addresses) all map to one dynamic IGA (Inside Global Address) assigned by your ISP.

**Figure 151** NAT Example 1

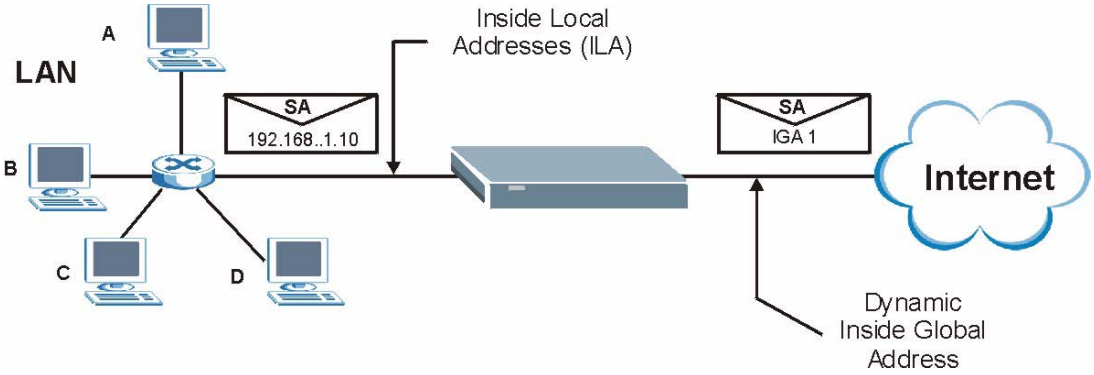


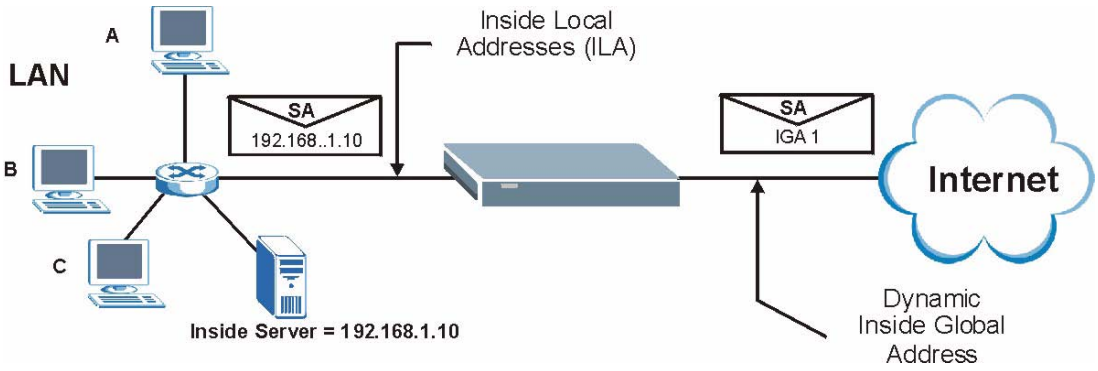

**Figure 152** Menu 4 Internet Access & NAT Example

```
          Menu 4 - Internet Access Setup
ISP's Name= MyISP
Encapsulation= RFC 1483
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Static
  IP Address= 0.0.0.0
Network Address Translation= SUA Only
  Address Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:
```

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the **Many-to-One** mapping discussed in Section 27.5 on page 261. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

### 27.5.2 Example 2: Internet Access with an Inside Server

**Figure 153** NAT Example 2




In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

**Figure 154** Menu 15.2.1 Specifying an Inside Server

```
        Menu 15.2.1 - NAT Server Setup (Used for SUA Only)
 Rule    Start Port No.    End Port No.    IP Address
-------------------------------------------------------
   1.     Default           Default         192.168.1.10
   2.       0                 0             0.0.0.0
   3.       0                 0             0.0.0.0
   4.       0                 0             0.0.0.0
   5.       0                 0             0.0.0.0
   6.       0                 0             0.0.0.0
   7.       0                 0             0.0.0.0
   8.       0                 0             0.0.0.0
   9.       0                 0             0.0.0.0
  10.       0                 0             0.0.0.0
  11.       0                 0             0.0.0.0
  12.       0                 0             0.0.0.0

          Press ENTER to Confirm or ESC to Cancel:
```

## 27.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two unidirectional as follows.

Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

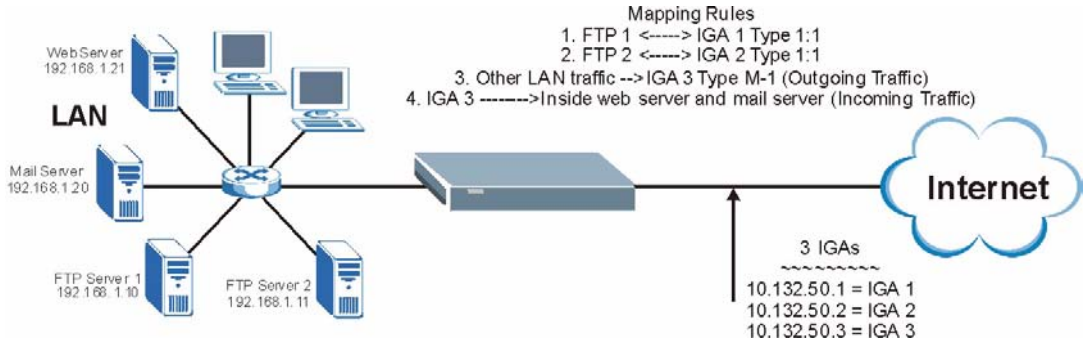
Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

**Figure 155** NAT Example 3




In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets.** Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) inFigure 156 on page 265.

1. Enter 15 from the main menu.
2. Enter 1 to configure the Address Mapping Sets.
3. Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
4. Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (SeeFigure 157 on page 265).
5. Repeat the previous step for rules 2 to 4 as outlined above.

When finished, menu 15.1.1 should look like as shown inFigure 158 on page 266.

**Figure 156** Example 3: Menu 11.3

```
            Menu 11.3 - Remote Node Network Layer Options
IP Options:                          Bridge Options:
  IP Address Assignment= Static        Ethernet Addr Timeout (min)= 0
  Rem IP Addr: 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= Full Feature
    Address Mapping Set= 2
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies=

            Press ENTER to Confirm or ESC to Cancel:
```

The following figures show how to configure the first rule

**Figure 157** Example 3: Menu 15.1.1.1

```
             Menu 15.1.1.1 Address Mapping Rule
                  Type= One-to-One
                  Local IP:
                    Start= 192.168.1.10
                    End  = N/A
                  Global IP:
                    Start= 10.132.50.1
                    End  = N/A
                  Server Mapping Set= N/A

              Press ENTER to Confirm or ESC to Cancel:
```

**Figure 158** Example 3: Final Menu 15.1.1

```
            Menu 15.1.1 - Address Mapping Rules
Set Name= Example3
Idx  Local Start IP   Local End IP   Global Start IP  Global End IP    Type
---  ---------------  -------------  ---------------  --------------   ----
 1. 192.168.1.10                      10.132.50.1                       1-1
 2  192.168.1.11                      10.132.50.2                       1-1
 3. 0.0.0.0          255.255.255.255  10.132.50.3                       M-1
 4.                                  10.132.50.3                      Server
 5.
 6.
 7.
 8.
 9.
10.

            Action= Edit          Select Rule=

            Press ENTER to Confirm or ESC to Cancel:
```

Now configure the IGA3 to map to our web server and mail server on the LAN.

1. Enter 15 from the main menu.
2. Enter 2 in **Menu 15 - NAT Setup**.
3. Enter 1 in **Menu 15.2 - NAT Server Sets** to see the following menu. Configure it as shown.

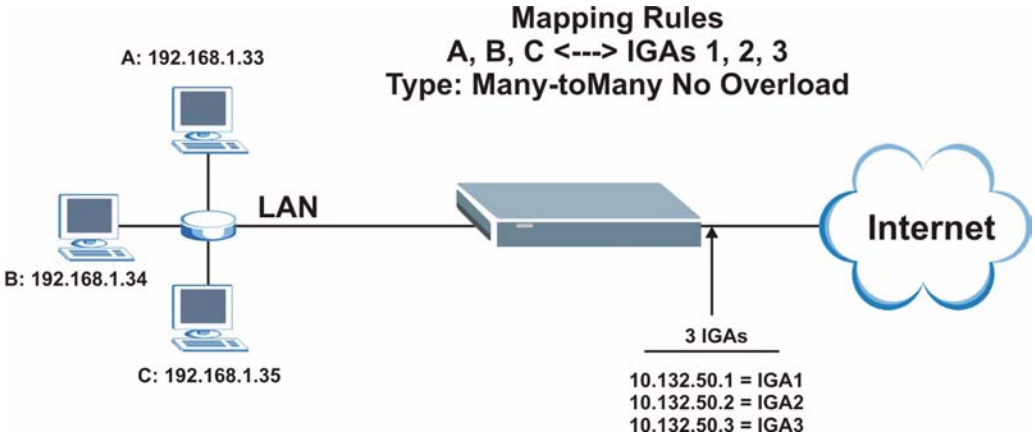
**Figure 159** Example 3: Menu 15.2.1

```
               Menu 15.2.1 - NAT Server Setup
        Rule   Start Port No.   End Port No.   IP Address
        ------------------------------------------------
           1.    Default          Default        0.0.0.0
           2.      80               80           192.168.1.21
           3.      25               25           192.168.1.20
           4.      0                0            0.0.0.0
           5.      0                0            0.0.0.0
           6.      0                0            0.0.0.0
           7.      0                0            0.0.0.0
           8.      0                0            0.0.0.0
           9.      0                0            0.0.0.0
          10.      0                0            0.0.0.0
          11.      0                0            0.0.0.0
          12.      0                0            0.0.0.0

              Press ENTER to Confirm or ESC to Cancel:
```

## 27.5.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-to-Many No Overload** mapping as port numbers do *not* change for **Many-to-Many No Overload** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

**Figure 160** NAT Example 4




Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using **One-to-One** and **Many-to-Many No Overload** mapping types.

Follow the steps outlined in example 3 to configure these two menus as follows.

**Figure 161** Example 4: Menu 15.1.1.1 Address Mapping Rule

```
            Menu 15.1.1.1 Address Mapping Rule
                 Type= Many-to-Many No Overload
                 Local IP:
                   Start= 192.168.1.10
                   End  = 192.168.1.12
                 Global IP:
                   Start= 10.132.50.1
                   End  = 10.132.50.3
                 Server Mapping Set= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

**Figure 162** Example 4: Menu 15.1.1 Address Mapping Rules

```
              Menu 15.1.1 - Address Mapping Rules
  Set Name= Example4
 Idx  Local Start IP   Local End IP   Global Start IP  Global End IP    Type
 ---  ---------------  ------------   ---------------  ---------------  ----
  1.  192.168.1.10     192.168.1.12   10.132.50.1      10.132.50.3      M:M
NO OV
  2.
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.
                    Action= Edit          Select Rule=

               Press ENTER to Confirm or ESC to Cancel:
```

# CHAPTER 28
# Enabling the Firewall

This chapter shows you how to get started with the Prestige firewall.

## 28.1 Remote Management and the Firewall

When SMT menu 24.11 is configured to allow management and the firewall is enabled:

- The firewall blocks remote management from the WAN unless you configure a firewall rule to allow it.
- The firewall allows remote management from the LAN.

## 28.2 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your Prestige has to offer. For this reason, it is recommended that you configure your firewall using the web configurator, see the following chapters for instructions. SMT screens allow you to activate the firewall and view firewall logs.

## 28.3 Enabling the Firewall

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next**.**

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Additional rules may be configured using the web configurator.

**Figure 163** Menu 21.2 Firewall Setup

```
        Menu 21.2 - Firewall Setup
The firewall protects against Denial of Service (DOS) attacks when
it is active. The default Policy sets
    1. allow all sessions originating from the LAN to the WAN and
    2. deny all sessions originating from the WAN to the LAN
You may define additional Policy rules or modify existing ones but
please exercise extreme caution in doing so
    Active: Yes
    LAN-to-WAN Set Name: ACL Default Set
    WAN-to-LAN Set Name: ACL Default Set
Please configure the Firewall function through Web Configurator.

          Press ENTER to Confirm or ESC to Cancel:
```

Use the web configurator or the command interpreter to configure the firewall rules

# CHAPTER 29
# Filter Configuration

This chapter shows you how to create and apply filters.

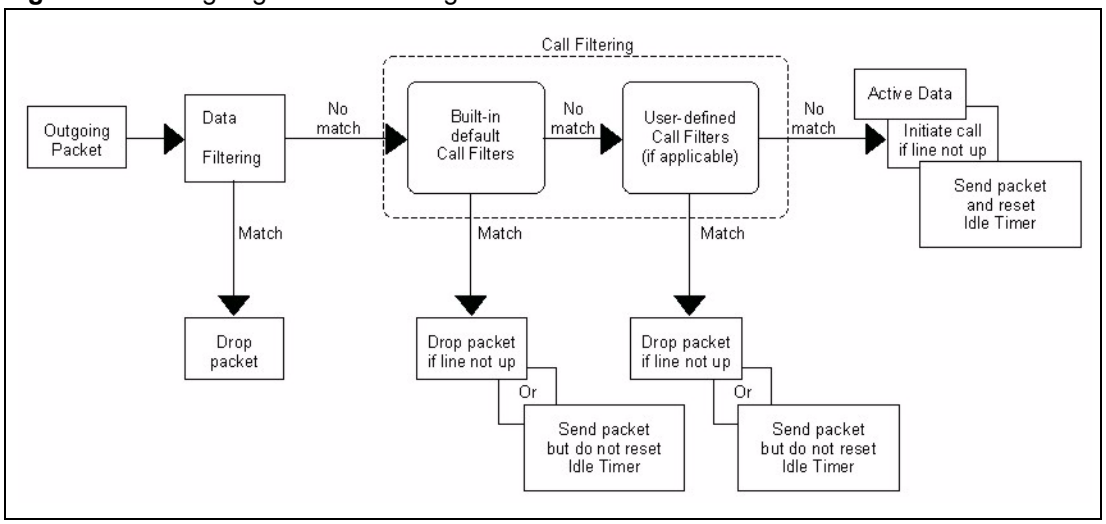
## 29.1 About Filtering

Your Prestige uses filters to decide whether or not to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call.

Outgoing packets must undergo data filtering before they encounter call filtering. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your Prestige has built-in call filters that prevent administrative, for example, RIP packets from triggering calls. These filters are always enabled and not accessible to you. Your Prestige applies the built-in filters first and then the user-defined call filters, if applicable, as shown next.

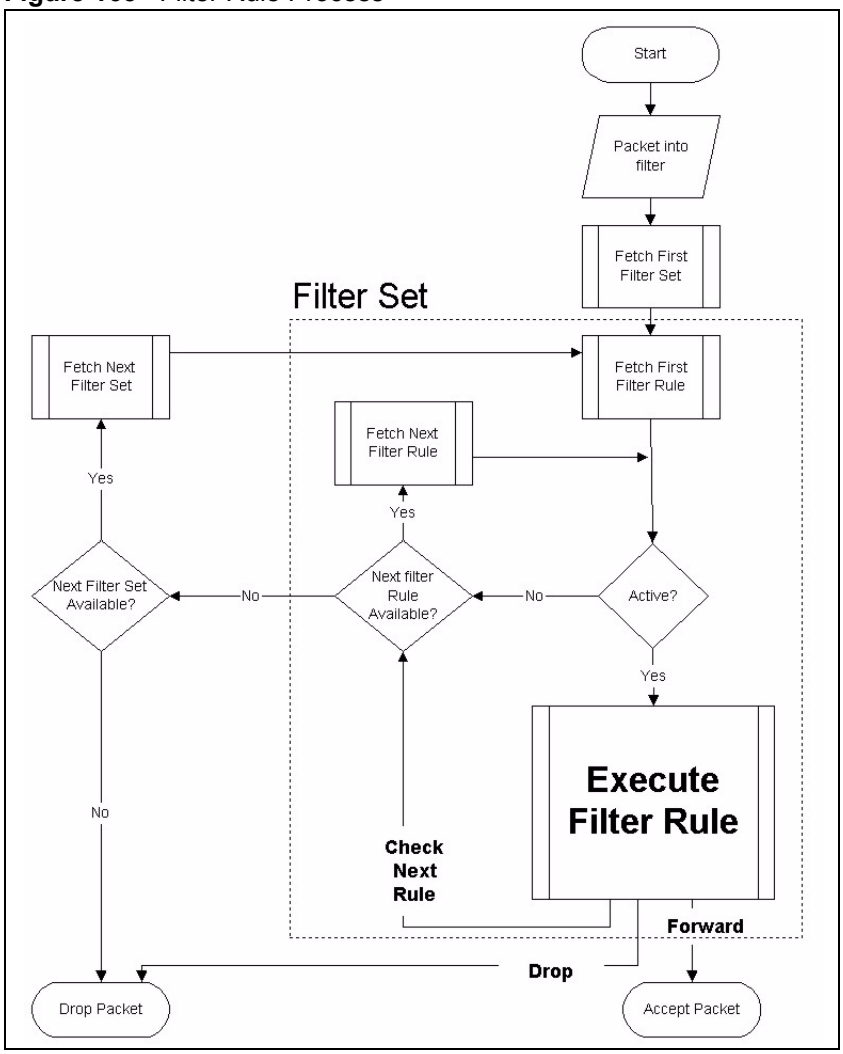
**Figure 164** Outgoing Packet Filtering Process




Two sets of factory filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule.

**Figure 165** Filter Rule Process




You can apply up to four filter sets to a particular port to block various types of packets. Because each filter set can have up to six rules, you can have a maximum of 24 rules active for a single port.

For incoming packets, your Prestige applies data filters only. Packets are processed depending on whether a match is found. The following sections describe how to configure filter sets.

## 29.1.1 The Filter Structure of the Prestige

A filter set consists of one or more filter rules. Usually, you would group related rules, for example, all the rules for NetBIOS, into a single set and give it a descriptive name. You can configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

## 29.2 Configuring a Filter Set for the Prestige

To configure a filter set, follow the steps shown next.

1. Enter 21 in the main menu to display **Menu 21 – Filter and Firewall Setup**.
2. Enter 1 to display **Menu 21.1 – Filter Set Configuration** as shown next.

**Figure 166** Menu 21 Filter Set Configuration

```
            Menu 21.1 - Filter Set Configuration
Filter
 Set #        Comments                Set #        Comments
 ------  ------------------           ------  ------------------
   1      ________________              7      ________________
   2      ________________              8      ________________
   3      ________________              9      ________________
   4      ________________             10      ________________
   5      ________________             11      ________________
   6      ________________             12      ________________

            Enter Filter Set Number to Configure= 0

            Edit Comments= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

3. Type the filter set to configure (no. 1 to 12) and press [ENTER].
4. Type a descriptive name or comment in the **Edit Comments** field and press [ENTER].
5. Press [ENTER] at the message "**Press ENTER to confirm…**" to display **Menu 21.1.1 – Filter Rules Summary** (that is, if you selected filter set 1 in menu 21.1).

**Figure 167** NetBIOS_WAN Filter Rules Summary

```
            Menu 21.1.2 - Filter Rules Summary
 # A Type                      Filter Rules                              M m n
 - - ---- ------------------------------------------------------------- - -
- -
 1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137                          N D N
 2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138                          N D N
 3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139                          N D N
 4 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137                         N D N
 5 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138                         N D N
 6 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139                         N D F

            Enter Filter Rule Number (1-6) to Configure:
```

**Figure 168** NetBIOS_LAN Filter Rules Summary

```
             Menu 21.1.3 - Filter Rules Summary
 # A Type                       Filter Rules                           M m n
 - - ---- ------------------------------------------------------------ - - -
1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53                  N D F
 2 N
 3 N
 4 N
 5 N
 6 N
             Enter Filter Rule Number (1-6) to Configure:
```

**Figure 169** IGMP Filter Rules Summary

```
             Menu 21.1.4 - Filter Rules Summary
 # A Type                       Filter Rules                           M m n
 - - ---- ------------------------------------------------------------ - - -
 1 Y Gen Off=0, Len=3, Mask=ffffff, Value=01005e                       N D F
 2 N
 3 N
 4 N
 5 N
 6 N

             Enter Filter Rule Number (1-6) to Configure:
```

## 29.3 Filter Rules Summary Menus

The following tables briefly describe the abbreviations used in menus 21.1.1 and 21.1.2.

**Table 94** Abbreviations Used in the Filter Rules Summary Menu

| FIELD | DESCRIPTION |
|---|---|
| # | The filter rule number: 1 to 6. |
| A | Active: "Y" means the rule is active. "N" means the rule is inactive. |
| Type | The type of filter rule: "GEN" for Generic, "IP" for TCP/IP. |
| Filter Rules | These parameters are displayed here. |
| M | More.<br>"Y" means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete.<br>"N" means there are no more rules to check. You can specify an action to be taken for instance, forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked. |

**Table 94** Abbreviations Used in the Filter Rules Summary Menu (continued)

| FIELD | DESCRIPTION |
|---|---|
| m | Action Matched.<br>"F" means to forward the packet immediately and skip checking the remaining rules.<br>"D" means to drop the packet.<br>"N"means to check the next rule. |
| n | Action Not Matched.<br>"F" means to forward the packet immediately and skip checking the remaining rules.<br>"D" means to drop the packet.<br>"N" means to check the next rule. |

The protocol dependent filter rules abbreviation are listed as follows:

**Table 95** Rule Abbreviations Used

| FILTER TYPE | DESCRIPTION |
|---|---|
| IP | |
| Pr | Protocol |
| SA | Source Address |
| SP | Source Port Number |
| DA | Destination Address |
| DP | Destination Port Number |
| GEN | |
| Off | Offset |
| Len | Length |

## 29.4 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.x – Filter Rules Summary** and press [ENTER] to open menu 21.1.x.1 for the rule.

There are two types of filter rules: **TCP/IP** and **Generic**. Depending on the type of rule, the parameters for each type will be different. Use [SPACE BAR] to select the type of rule that you want to create in the **Filter Type** field and press [ENTER] to open the respective menu.

To speed up filtering, all rules in a filter set must be of the same class, for instance, protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filters field or vice versa, the Prestige will warn you and will not allow you to save.

## 29.4.1 TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select TCP/IP Filter Rule from the **Filter Type** field and press [ENTER] to open **Menu 21.1.x.1 – TCP/IP Filter Rule**, as shown next.

**Figure 170** Menu 21.1.x.1 TCP/IP Filter Rule

```
                Menu 21.1.1.1 - TCP/IP Filter Rule

           Filter #: 1,1
           Filter Type= TCP/IP Filter Rule
           Active= No
           IP Protocol= 0     IP Source Route= No
           Destination: IP Addr=
                        IP Mask=
                        Port #=
                        Port # Comp= None
                Source: IP Addr=
                        IP Mask=
                        Port #=
                        Port # Comp= None
           TCP Estab= N/A
           More= No            Log= None
           Action Matched= Check Next Rule
           Action Not Matched= Check Next Rule

           Press ENTER to Confirm or ESC to Cancel:
```

The following table describes how to configure your TCP/IP filter rule.

**Table 96** Menu 21.1.x.1 TCP/IP Filter Rule

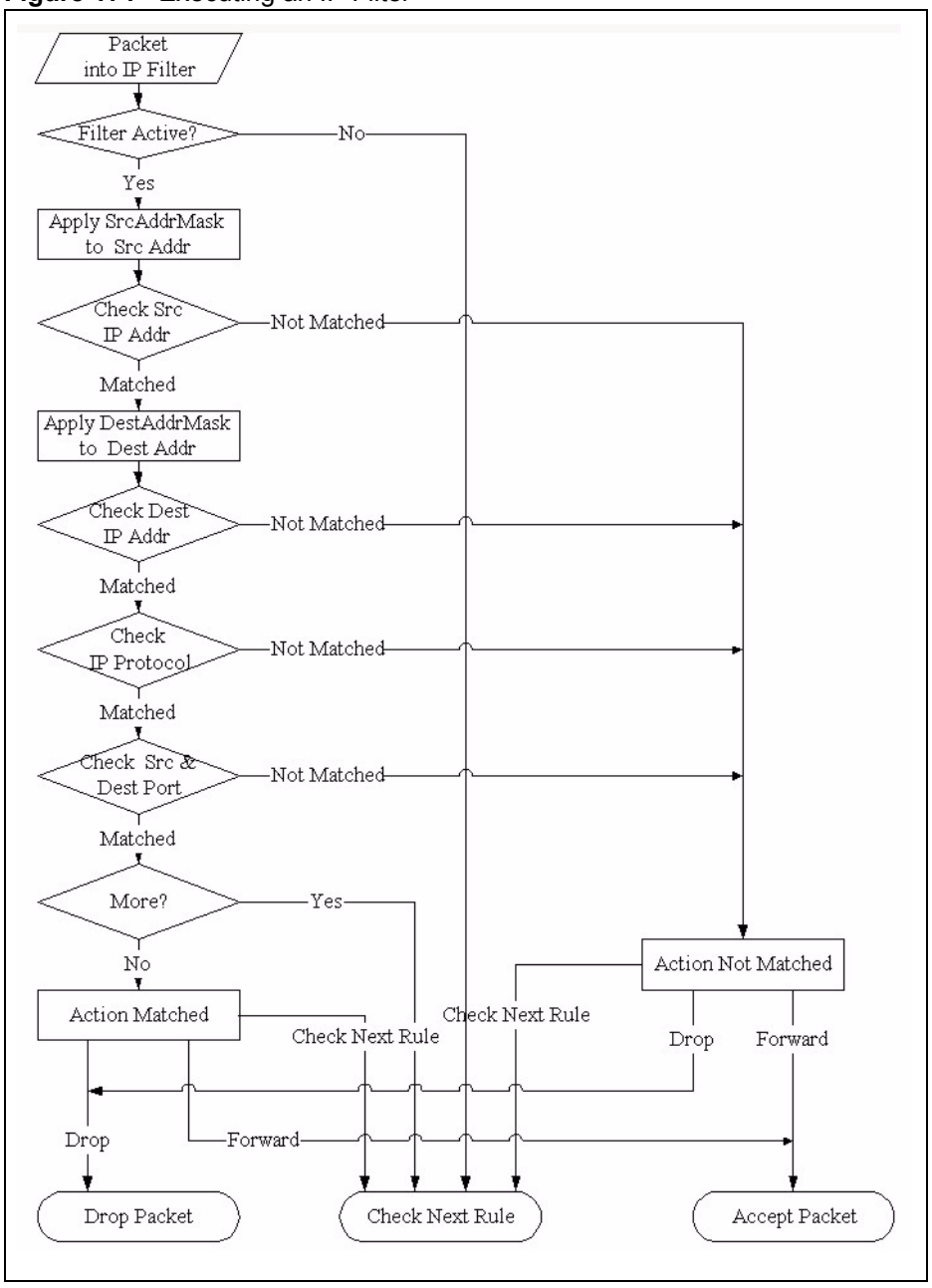
| FIELD | DESCRIPTION |
|---|---|
| Filter # | This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set. |
| Filter Type | Use [SPACE BAR] and then [ENTER] to choose a rule. Parameters displayed for each type will be different. Choices are **TCP/IP Filter Rule** or **Generic Filter Rule**. |
| Active | Select **Yes** to activate or **No** to deactivate the filter rule. |
| IP Protocol | This is the upper layer protocol, for example, TCP is 6, UDP is 17 and ICMP is 1. The value must be between 0 and 255. A value of 0 matches ANY protocol. |
| IP Source Route | IP Source Route is an optional header that dictates the route an IP packet takes from its source to its destination. If **Yes**, the rule applies to any packet with an IP source route. The majority of IP packets do not have source route. |
| Destination: | |
| IP Addr | Type the destination IP address of the packet you want to filter. This field is ignored if it is 0.0.0.0. |
| IP Mask | Type the IP mask to apply to the **Destination: IP Addr** field. |

**Table 96** Menu 21.1.x.1 TCP/IP Filter Rule (continued)

| FIELD | DESCRIPTION |
|---|---|
| Port # | Type the destination port of the packets you want to filter. The field range is 0 to 65535. A 0 field is ignored. |
| Port # Comp | Select the comparison to apply to the destination port in the packet against the value given in **Destination: Port #.** Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**. |
| Source: | |
| IP Addr | Type the source IP Address of the packet you want to filter. A 0.0.0.0 field is ignored. |
| IP Mask | Type the IP mask to apply to the **Source: IP Addr** field. |
| Port # | Type the source port of the packets you want to filter. The range of this field is 0 to 65535. A 0 field is ignored. |
| Port # Comp | Select the comparison to apply to the source port in the packet against the value given in **Source: Port #** field. Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**. |
| TCP Estab | This applies only when the IP Protocol field is 6, TCP. If **Yes**, the rule matches packets that want to establish TCP connection(s) (SYN=1 and ACK=0); else it is ignored. |
| More | If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields.<br>If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be N/A. |
| Log | Select the logging option from the following:<br>**None** – No packets will be logged.<br>**Action Matched** – Only packets that match the rule parameters will be logged.<br>**Action Not Matched** – Only packets that do not match the rule parameters will be logged.<br>**Both** – All packets will be logged. |
| Action Matched | Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**. |
| Action Not Matched | Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

The following figure illustrates the logic flow of an IP filter.

**Figure 171** Executing an IP Filter




## 29.4.2 Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the Prestige treats a packet as a byte stream as opposed to an IP packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The Prestige applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** fields are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule select an empty filter set in menu 21, for example 5. Select **Generic Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.1.5.1 – Generic Filter Rule**, as shown in the following figure.

**Figure 172** Menu 21.1.5.1 Generic Filter Rule

```
Menu 21.1.5.1 - Generic Filter Rule

Filter #: 5,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No            Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:
```

The next table describes the fields in the **Generic Filter Rule** menu.

**Table 97** Menu 21.1.5.1 Generic Filter Rule

| FIELD | DESCRIPTION |
|---|---|
| Filter # | This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third rule of that set. |
| Filter Type | Press [SPACE BAR] and then [ENTER] to select a type of rule. Parameters displayed below each type will be different. Choices are **Generic Filter Rule** or **TCP/IP Filter Rule**. |
| Active | Select **Yes** to turn on or **No** to turn off the filter rule. |
| Offset | Type the starting byte of the data portion in the packet that you want to compare. The range for this field is from 0 to 255. |
| Length | Type the byte count of the data portion in the packet that you want to compare. The range for this field is 0 to 8. |
| Mask | Type the mask (in Hexadecimal) to apply to the data portion before comparison. |
| Value | Type the value (in Hexadecimal) to compare with the data portion. |
| More | If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields.<br>If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**. |

**Table 97** Menu 21.1.5.1 Generic Filter Rule (continued)

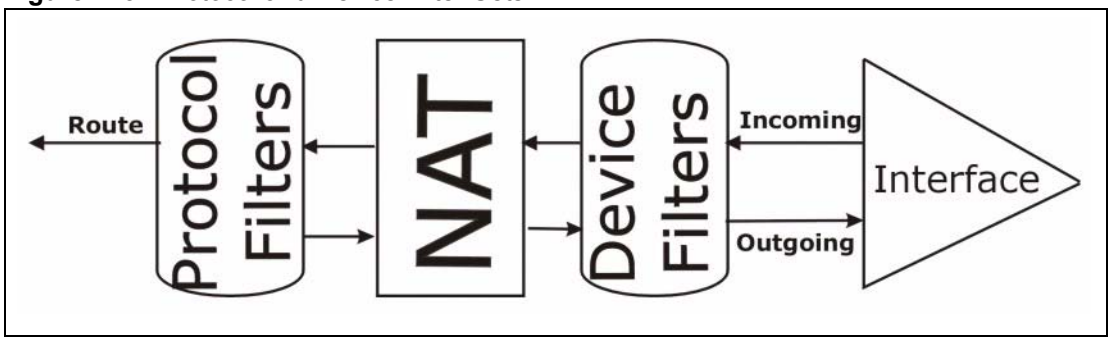
| FIELD | DESCRIPTION |
|---|---|
| Log | Select the logging option from the following:<br>**None** – No packets will be logged.<br>**Action Matched** – Only matching packets and rules will be logged.<br>**Action Not Matched** – Only packets that do not match the rule parameters will be logged.<br>**Both** – All packets will be logged. |
| Action Matched | Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**. |
| Action Not Matched | Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

## 29.5 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** Device rules and Protocol Filter (**TCP/IP**) rules. Generic Filter rules act on the raw data from/to LAN and WAN. Protocol Filter rules act on IP packets.

When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the Prestige applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic (or device) filters are applied to the raw packets that appear on the wire. They are applied at the point where the Prestige is receiving and sending the packets; for instance, the interface. The interface can be an Ethernet, or any other hardware port. The following figure illustrates this.

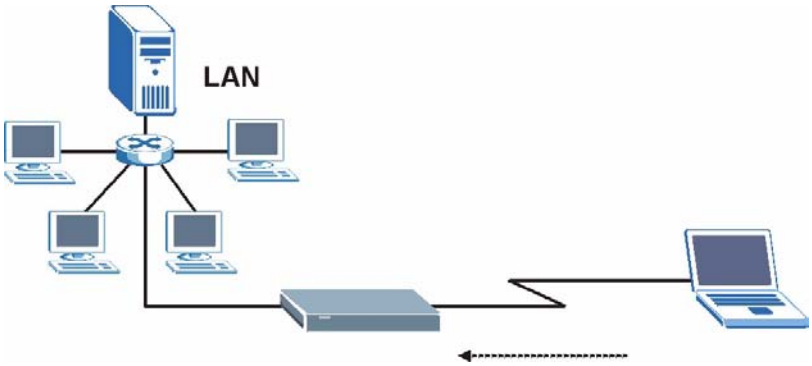
**Figure 173** Protocol and Device Filter Sets




## 29.6 Example Filter

Let's look at an example to block outside users from telnetting into the Prestige.

**Figure 174** Sample Telnet Filter




1. Enter 1 in the menu 21 to display **Menu 21.1 — Filter Set Configuration**.
2. Enter the index number of the filter set you want to configure (in this case 6).
3. Type a descriptive name or comment in the **Edit Comments** field (for example, TELNET_WAN) and press [ENTER].
4. Press [ENTER] at the message "`Press [ENTER] to confirm or [ESC] to cancel...`" to open **Menu 21.1.6 — Filter Rules Summary**.
5. Type 1 to configure the first filter rule. Make the entries in this menu as shown next.

When you press [ENTER] to confirm, the following screen appears. Note that there is only one filter rule in this set.

**Figure 175** Menu 21.1.6.1 Sample Filter

```
            Menu 21.1.6.1 - TCP/IP Filter Rule

            Filter #: 6,1
            Filter Type= TCP/IP Filter Rule
            Active= Yes
            IP Protocol= 6      IP Source Route= No
            Destination: IP Addr= 0.0.0.0
            IP Mask= 0.0.0.0
            Port #= 23
            Port # Comp= Equal
                          Source: IP Addr= 0.0.0.0
            IP Mask= 0.0.0.0
            Port #=
            Port # Comp= Equal
            TCP Estab= No
            More= No              Log= None
            Action Matched= Drop
            Action Not Matched= Forward

            Press ENTER to Confirm or ESC to Cancel:
```

After you have created the filter set, you must apply it.

1. Enter 11 in the main menu to display menu 11 and type the remote node number to edit.

2 Go to the **Edit Filter Sets** field, press [SPACE BAR] to choose **Yes** and press [ENTER].

This brings you to menu 11.5. Apply the example filter set (for example, filter set 3) in this menu as shown in the next section.

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP**, **Pr = 6**) for destination telnet ports (**DP = 23**).

**M = N** means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

**Figure 176** Menu 21.1.6.1 Sample Filter Rules Summary

```
             Menu 21.1.6 - Filter Rules Summary
 # A Type                      Filter Rules                              M m n
 - - ---- ------------------------------------------------------------ - -
- -
 1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                           N D F
 2 N
 3 N
 4 N
 5 N
 6 N

             Enter Filter Rule Number (1-6) to Configure: 1
```

# 29.7 Applying Filters and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in menu 21 (but have not been applied) to filter traffic.

**Table 98** Filter Sets Table

| FILTER SETS | DESCRIPTION |
|---|---|
| Input Filter Sets: | Apply filters for incoming traffic. You may apply protocol or device filter rules. See earlier in this chapter for information on filters. |
| Output Filter Sets: | Apply filters for traffic leaving the Prestige. You may apply filter rules for protocol or device filters. See earlier in this section for information on types of filters. |
| Call Filter Sets: | Apply filters to decide if a packet should be allowed to trigger a call. |

### 29.7.1 Ethernet Traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and type the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by typing their numbers separated by commas, for example, 3, 4, 6, 11. The factory default filter set, `NetBIOS_LAN`, is inserted in the **protocol filters** field under **Input Filter Sets** in menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server.

**Figure 177** Filtering Ethernet Traffic

```
Menu 3.1 - LAN Port Filter Setup


Input Filter Sets:
protocol filters= 3
device filters=
Output Filter Sets:
protocol filters=
device filters=


Press ENTER to Confirm or ESC to Cancel:
```

### 29.7.2 Remote Node Filters

Go to menu 11.5 (shown next) and type the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by typing their numbers separated by commas. The factory default filter set, `NetBIOS_WAN`, is inserted in the **protocol filters** field under **Call Filter Sets** in menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP.

**Figure 178** Filtering Remote Node Traffic

```
Menu 11.5 - Remote Node Filter

          Input Filter Sets:
            protocol filters= 6
            device filters=
          Output Filter Sets:
            protocol filters= 2
            device filters=
          Call Filter Sets:
            Protocol filters=
            Device filters=


Enter here to CONFIRM or ESC to CANCEL:
```

Note that call filter sets are visible when you select PPPoA or PPPoE encapsulation.

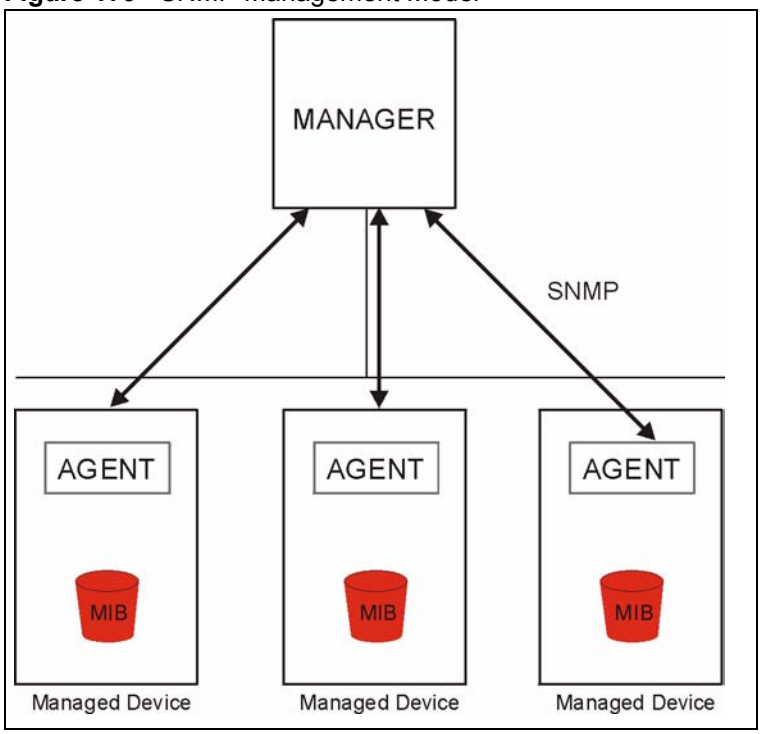
# CHAPTER 30
# SNMP Configuration

This chapter explains SNMP Configuration menu 22.

## 30.1 About SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1) and version two c (SNMPv2c). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

**Figure 179** SNMP Management Model




An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the Prestige). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include the number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

## 30.2 Supported MIBs

The Prestige supports RFC-1215 and MIB II as defined in RFC-1213 as well as ZyXEL private MIBs. The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

## 30.3 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 — SNMP Configuration** as shown next. The "community" for Get, Set and Trap fields is SNMP terminology for password.

**Figure 180** Menu 22 SNMP Configuration

```
              Menu 22 - SNMP Configuration

              SNMP:
                Get Community= public
                Set Community= public
                Trusted Host= 0.0.0.0
                Trap:
                  Community= public
                  Destination= 0.0.0.0

              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the SNMP configuration parameters.

**Table 99** Menu 22 SNMP Configuration

| FIELD | DESCRIPTION |
|---|---|
| SNMP: | |
| Get Community | Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station. |
| Set Community | Type the **Set** community, which is the password for incoming Set requests from the management station. |
| Trusted Host | If you enter a trusted host, your Prestige will only respond to SNMP messages from this address. A blank (default) field means your Prestige will respond to all SNMP messages it receives, regardless of source. |
| Trap: | |
| Community | Type the trap community, which is the password sent with each trap to the SNMP manager. |
| Destination | Type the IP address of the station to send your SNMP traps to. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

# 30.4 SNMP Traps

The Prestige will send traps to the SNMP manager when any one of the following events occurs:

**Table 100** SNMP Traps

| TRAP # | TRAP NAME | DESCRIPTION |
|---|---|---|
| 1 | coldStart (*defined in RFC-1215*) | A trap is sent after booting (power on). |
| 2 | warmStart (*defined in RFC-1215*) | A trap is sent after booting (software reboot). |
| 3 | linkDown (*defined in RFC-1215*) | A trap is sent with the port number when any of the links are down. See the following table. |
| 4 | linkUp (*defined in RFC-1215*) | A trap is sent with the port number. |

**Table 100** SNMP Traps (continued)

| TRAP # | TRAP NAME | DESCRIPTION |
|---|---|---|
| 5 | authenticationFailure (*defined in RFC-1215*) | A trap is sent to the manager when receiving any SNMP gets or sets requirements with wrong community (password). |
| 6 | whyReboot (defined in ZYXEL-MIB) | A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start). |
| 6a | For intentional reboot : | A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.). |

The port number is its interface index under the interface group.

**Table 101** Ports and Permanent Virtual Circuits

| PORT | PVC (PERMANENT VIRTUAL CIRCUIT) |
|---|---|
| 1 | Ethernet LAN |
| 2 | 1 |
| 3 | 2 |
| … | … |
| 13 | 12 |
| 14 | xDSL |

# CHAPTER 31
# System Security

This chapter describes how to configure the system security on the Prestige.

## 31.1 System Security

You can configure the system password.

### 31.1.1 System Password

Enter 23 in the main menu to display **Menu 23 – System Security**.

You should change the default password. If you forget your password you have to restore the default configuration file.

**Figure 181** Menu 23 – System Security

```
Menu 23 - System Security

      1. Change Password
      2. RADIUS Server
      4. IEEE802.1x

Enter Menu Selection Number:
```

### 31.1.2 Configuring External RADIUS Server

From **Menu 23- System Security**, enter 2 to display **Menu 23.2 - System Security-RADIAS Server**.

**Figure 182** Menu 23.2 System Security: RADIUS Server

```
            Menu 23.2 - System Security - RADIUS Server

                        Authentication Server:
                          Active= No
                          Server Address= 10.11.12.13
                          Port #= 1812
                          Shared Secret= ********
                        Accounting Server:
                          Active= No
                          Server Address= 10.11.12.13
                          Port #= 1813
                          Shared Secret= ********

            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 102** Menu 23.2 System Security: RADIUS Server

| FIELD | DESCRIPTION |
|---|---|
| Authentication Server | |
| Active | Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external authentication server. |
| Server Address | Enter the IP address of the external authentication server in dotted decimal notation. |
| Port | The default port of the RADIUS server for authentication is **1812**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Shared Secret | Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points.<br>The key is not sent over the network. This key must be the same on the external authentication server and Prestige. |
| Accounting Server | |
| Active | Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external accounting server. |
| Server Address | Enter the IP address of the external accounting server in dotted decimal notation. |
| Port | The default port of the RADIUS server for accounting is **1813**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Shared Secret | Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points.<br>The key is not sent over the network. This key must be the same on the external accounting server and Prestige. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

### 31.1.3 IEEE 802.1x

The IEEE 802.1x standards outline enhanced security methods for both the authentication of wireless stations and encryption key management.

Follow the steps below to enable EAP authentication on your Prestige.

1 From the main menu, enter 23 to display **Menu23 – System Security**.

**Figure 183** Menu 23 System Security

```
Menu 23 - System Security

       1. Change Password
       2. RADIUS Server
       4. IEEE802.1x


Enter Menu Selection Number:
```

2 Enter 4 to display **Menu 23.4 – System Security – IEEE 802.1x**.

**Figure 184** Menu 23.4 System Security: IEEE 802.1x

```
Menu 23.4 - System Security - IEEE 802.1x

      Wireless Port Control= No Authentication Required
      ReAuthentication Timer (in second)= N/A
      Idle Timeout (in second)= N/A
      Key Management Protocol= N/A
      Dynamic WEP Key Exchange= N/A
      PSK= N/A
      WPA Mixed Mode= N/A
      Data Privacy for Broadcast/Multicast packets= N/A
      WPA Broadcast/Multicast Key Update Timer= N/A
      Authentication Databases= N/A


Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 103** Menu 23.4 System Security: IEEE 802.1x

| FIELD | DESCRIPTION |
|---|---|
| Wireless Port Control | Press [SPACE BAR] and select a security mode for the wireless LAN access.<br>Select **No Authentication Required** to allow any wireless stations access to your wired network without entering usernames and passwords. This is the default setting.<br>Selecting **Authentication Required** means wireless stations have to enter usernames and passwords before access to the wired network is allowed.<br>Select **No Access Allowed** to block all wireless stations access to the wired network.<br>The following fields are not available when you select **No Authentication Required** or **No Access Allowed**. |
| ReAuthentica-tion Timer (in second) | Specify how often a client has to re-enter username and password to stay connected to the wired network.<br>This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Enter a time interval between 10 and 9999 (in seconds). The default time interval is **1800** seconds (or 30 minutes). |
| Idle Timeout (in second) | The Prestige automatically disconnects a client from the wired network after a period of inactivity. The client needs to enter the username and password again before access to the wired network is allowed.<br>This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (or 1 hour). |
| Key Management Protocol | Press [SPACE BAR] to select **802.1x**, **WPA** or **WPA-PSK** and press [ENTER]. |
| Dynamic WEP Key Exchange | This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Also set the **Authentication Databases** field to **RADIUS Only**. Local user database may not be used.<br>Select **Disable** to allow wireless stations to communicate with the access points without using Dynamic WEP Key Exchange.<br>Select **64-bit WEP** or **128-bit WEP** to enable data encryption.<br>Up to 32 stations can access the Prestige when you configure Dynamic WEP Key Exchange. This field is not available when you set **Key Management Protocol** to **WPA** or **WPA-PSK**. |
| PSK | Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) when you select **WPA-PSK** in the **Key Management Protocol** field. |
| WPA Mixed Mode | Select **Enable** to activate WPA mixed mode. Otherwise, select **Disable** and configure **Group Data Privacy** field. |
| Data Privacy for Broadcast/ Multicast packets | This field allows you to choose **TKIP** (recommended) or **WEP** for broadcast and multicast ("group") traffic if the **Key Management Protocol** is **WPA** and **WPA Mixed Mode** is disabled. **WEP** is used automatically if you have enabled **WPA Mixed Mode**.<br>All unicast traffic is automatically encrypted by **TKIP** when **WPA** or **WPA-PSK Key Management Protocol** is selected. |
| WPA Broadcast/ Multicast Key Update Timer | The **WPA Broadcast/Multicast Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Broadcast/Multicast Key Update Timer** is also supported in WPA-PSK mode. The Prestige default is 1800 seconds (30 minutes). |

**Table 103** Menu 23.4 System Security: IEEE 802.1x (continued)

| FIELD | DESCRIPTION |
|---|---|
| Authentication Databases | The authentication database contains wireless station login information. The local user database is the built-in database on the Prestige. The RADIUS is an external server. Use this field to decide which database the Prestige should use (first) to authenticate a wireless station.<br>Before you specify the priority, make sure you have set up the corresponding database correctly first.<br>When you configure **Key Management Protocol** to **WPA**, the **Authentication Databases** must be **RADIUS Only**. You can only use the **Local User Database** with **802.1x Key Management Protocol**.<br>Select **Local User Database Only** to have the Prestige just check the built-in user database on the Prestige for a wireless station's username and password.<br>Select **RADIUS Only** to have the Prestige just check the user database on the specified RADIUS server for a wireless station's username and password.<br>Select **Local first, then RADIUS** to have the Prestige first check the user database on the Prestige for a wireless station's username and password. If the user name is not found, the Prestige then checks the user database on the specified RADIUS server.<br>Select **RADIUS first, then Local** to have the Prestige first check the user database on the specified RADIUS server for a wireless station's username and password. If the Prestige cannot reach the RADIUS server, the Prestige then checks the local user database on the Prestige. When the user name is not found or password does not match in the RADIUS server, the Prestige will not check the local user database and the authentication fails. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the Prestige for authentication.

## 31.2 Creating User Accounts on the Prestige

By storing user profiles locally, your Prestige is able to authenticate wireless users without interacting with a network RADIUS server.

Follow the steps below to set up user profiles on your Prestige.

1 From the main menu, enter 14 to display **Menu 14 - Dial-in User Setup**.

**Figure 185** Menu 14 Dial-in User Setup

```
                          Menu 14 - Dial-in User Setup

1. ________          9. ________         17. ________         25. ________
2. ________         10. ________         18. ________         26. ________
3. ________         11. ________         19. ________         27. ________
4. ________         12. ________         20. ________         28. ________
5. ________         13. ________         21. ________         29. ________
6. ________         14. ________         22. ________         30. ________
7. ________         15. ________         23. ________         31. ________
8. ________         16. ________         24. ________         32. ________

                                  Enter Menu Selection Number:
```

**2** Type a number and press [ENTER] to edit the user profile.

**Figure 186** Menu 14.1 Edit Dial-in User

```
            Menu 14.1 - Edit Dial-in User

                  User Name= test
                  Active= Yes
                  Password= ********


            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 104** Menu 14.1 Edit Dial-in User

| FIELD | DESCRIPTION |
|---|---|
| User Name | Enter a username up to 31 alphanumeric characters long for this user profile. This field is case sensitive. |
| Active | Press [SPACE BAR] to select **Yes** and press [ENTER] to enable the user profile. |
| Password | Enter a password up to 31 characters long for this user profile. |
| When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel. | |

# CHAPTER 32
# System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

## 32.1 Overview

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu to open **Menu 24 – System Maintenance**, as shown in the following figure.

**Figure 187** Menu 24 System Maintenance

```
Menu 24 - System Maintenance

1.  System Status
2.  System Information and Console Port Speed
3.  Log and Trace
4.  Diagnostic
5.  Backup Configuration
6.  Restore Configuration
7.  Upload Firmware
8.  Command Interpreter Mode
9.  Call Control
10.  Time and Date Setting
11.  Remote Management

Enter Menu Selection Number:
```

## 32.2 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next. System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your DSL telephone line status, number of packets sent and received.

To get to System Status, type 24 to go to **Menu 24 — System Maintenance.** From this menu, type 1**. System Status**. There are two commands in **Menu 24.1 — System Maintenance — Status**. Entering 1 resets the counters; [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status** which are read-only and meant for diagnostic purposes.

**Figure 188** Menu 24.1 System Maintenance : Status

```
                  Menu 24.1 - System Maintenance - Status          23:08:47
                                                          Sat. Jan. 01, 2000

Node-Lnk Status      TxPkts      RxPkts      Errors  Tx B/s  Rx B/s     Up
Time
 1-ENET  N/A             0           0           0       0       0     0:00:00
 2       N/A             0           0           0       0       0     0:00:00
 3       N/A             0           0           0       0       0     0:00:00
 4       N/A             0           0           0       0       0     0:00:00
 5       N/A             0           0           0       0       0     0:00:00
 6       N/A             0           0           0       0       0     0:00:00
 7       N/A             0           0           0       0       0     0:00:00
 8       N/A             0           0           0       0       0     0:00:00

My WAN IP (from ISP): 0.0.0.0

    Ethernet:                                      WAN:
      Status: 100M/Full Duplex Tx Pkts: 5731         Line Status: Down
      Collisions: 0           Rx Pkts: 8314        Upstream Speed:     0 kbps
    CPU Load =   25.52%                          Downstream Speed:     0 kbps
                                 Press Command:
              COMMANDS: 1-Reset Counters  TAB-Next Page  ESC-Exit
```

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status**.

**Table 105** Menu 24.1 System Maintenance: Status

| FIELD | DESCRIPTION |
|---|---|
| Node-Lnk | This is the node index number and link type. Link types are: PPP, ENET, 1483. |
| Status | This shows the status of the remote node. |
| TxPkts | The number of transmitted packets to this remote node. |
| RxPkts | The number of received packets from this remote node. |
| Errors | The number of error packets on this connection. |
| Tx B/s | This shows the transmission rate in bytes per second. |
| Rx B/s | This shows the receiving rate in bytes per second. |
| Up Time | This is the time this channel has been connected to the current remote node. |
| My WAN IP (from ISP) | This is the IP address of the ISP remote node. |
| Ethernet | This shows statistics for the LAN. |
| Status | This shows the current status of the LAN. |
| Tx Pkts | This is the number of transmitted packets to the LAN. |
| Rx Pkts | This is the number of received packets from the LAN. |

**Table 105** Menu 24.1 System Maintenance: Status (continued)

| FIELD | DESCRIPTION |
|---|---|
| Collision | This is the number of collisions. |
| WAN | This shows statistics for the WAN. |
| Line Status | This shows the current status of the xDSL line, which can be Up or Down. |
| Upstream Speed | This shows the upstream transfer rate in kbps. |
| Downstream Speed | This shows the downstream transfer rate in kbps. |
| CPU Load | This specifies the percentage of CPU utilization. |

# 32.3 System Information

To get to the System Information:

1. Enter 24 to display **Menu 24 — System Maintenance**.
2. Enter 2 to display **Menu 24.2 — System Information and Console Port Speed**.

From this menu you have two choices as shown in the next figure:

**Figure 189** Menu 24.2 System Information and Console Port Speed

```
            Menu 24.2 - System Information and Console Port Speed

            1. System Information
            2. Console Port Speed

            Please enter selection:
```

## 32.3.1 System Information

Enter 1 in menu 24.2 to display the screen shown next.

**Figure 190** Menu 24.2.1 System Maintenance: Information

```
              Menu 24.2.1 - System Maintenance - Information

            Name:
            Routing: IP
            ZyNOS F/W Version: V3.40(ACC.0)| 04/26/2005
            ADSL Chipset Vendor: DMT FwVer: 3.0.11.11_A_TC, HwVer: T14F+
            Standard: Multi-Mode

            LAN
              Ethernet Address: 00:13:49:11:11:35
              IP Address: 192.168.1.1
              IP Mask: 255.255.255.0
              DHCP: Server


                  Press ESC or RETURN to Exit:
```

The following table describes the fields in this menu.

**Table 106** Menu 24.2.1 System Maintenance: Information

| FIELD | DESCRIPTION |
|---|---|
| Name | Displays the system name of your Prestige. This information can be changed in **Menu 1 – General Setup**. |
| Routing | Refers to the routing protocol used. |
| ZyNOS F/W Version | Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation. |
| ADSL Chipset Vendor | Displays the vendor of the ADSL chipset and DSL version. |
| Standard | This refers to the operational protocol the Prestige and the DSLAM (Digital Subscriber Line Access Multiplexer) are using. |
| LAN | |
| Ethernet Address | Refers to the Ethernet MAC (Media Access Control) of your Prestige. |
| IP Address | This is the IP address of the Prestige in dotted decimal notation. |
| IP Mask | This shows the subnet mask of the Prestige. |
| DHCP | This field shows the DHCP setting (None, Relay or Server) of the Prestige. |

## 32.3.2 Console Port Speed

**Note:** The console port is internal and reserved for technician use only.

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your Prestige supports 9600 (default), 19200, 38400, 57600 and 115200 bps. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

**Figure 191** Menu 24.2.2 System Maintenance : Change Console Port Speed

```
            Menu 24.2.2 - System Maintenance - Change Console Port Speed

                      Console Port Speed: 9600

            Press ENTER to Confirm or ESC to Cancel:
```

Once you change the Prestige console port speed, you must also set the speed parameter for the communication software you are using to connect to the Prestige.

# 32.4 Log and Trace

There are two logging facilities in the Prestige. The first is the error logs and trace records that are stored locally. The second is the syslog facility for message logging.

## 32.4.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

1. Type 24 in the main menu to display **Menu 24 – System Maintenance**.
2. From menu 24, type 3 to display **Menu 24.3 – System Maintenance – Log and Trace**.

**Figure 192** Menu 24.3 System Maintenance: Log and Trace

```
            Menu 24.3 - System Maintenance - Log and Trace

                   1. View Error Log
                   2. UNIX Syslog


            Please enter selection
```

3. Enter 1 from **Menu 24.3 — System Maintenance — Log and Trace** to display the error log in the system.

After the Prestige finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.