Management Setup

Introduction

By default, the router may be configured and managed with any Telnet client or Web browser running on any operating system. There is no requirement for additional software or utilities. However, for some specific environments, you may want to change the server port numbers for the built-in Telnet or HTTP server, create access lists to protect the router, or reject system administrator login from the Internet.

Configuration

Click **Management Setup**. The following setup page will be displayed.

Management Access Control

Enable remote firmware upgrade(FTP): Check to allow firmware upgrade from the Internet.

Allow management from the Internet: Check to allow system administrators to login from the Internet. The default is not allowed.

Disable PING from the Internet: Check to reject all PING packets from the Internet. The default is allowed.

Access List

You may specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks may be entered.

IP: Specifies an IP address allowed to login to the router.

Subnet Mask: Specifies a subnet mask allowed to login to the router.

Port Setup

Default Ports: Check to use standard port numbers for the Telnet and HTTP servers.

User Defined Ports: Check to specify user-defined port numbers for the Telnet and HTTP servers.

SNMP Setup

Enable SNMP Agent: Check to enable built-in SNMP agent.

Get Community: Specify a string to identify the management communities for the SNMP GET command.

Set Community: Specify a string to identify the management communities for the SNMP SET command.

Manager Host IP: Specify the IP address of the SNMP manager station.

Trap Community: Specify a string to identify the management communities for the SNMP TRAP notifications.

Notification Host IP: Specify the IP address which the station wants to receive the TRAP notifications.

Trap Timeout: Specify a time out for traps message queue.