ChoiceNet™ Administrator's Guide

Livingston Enterprises, Inc.
4464 Willow Rd
Pleasanton, CA 94588
(510) 426-0770
(800) 458-9966

January 1997

950-1190A

Copyright and Trademarks

The names Livingston, PortMaster, ComOS, RADIUS, ChoiceNet, PMconsole, IRX, True Digital, RAMP, and Total Access. Sure and Simple. are trademarks of Livingston Enterprises, Inc. All other marks are the property of their respective owners.

Disclaimer

Livingston Enterprises, Inc. makes no express or implied representations or warranties with respect to the contents or use of this manual, and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Livingston Enterprises, Inc. further reserves the right to revise this manual and to make changes to its content at any time, without obligation to notify any person or entity of such revisions or changes.

Contents

Figures

Tables

Preface

About This Guide

The *ChoiceNet™ Administrator's Guide* provides complete installation and configuration instructions for the Livingston Enterprises, Inc. ChoiceNet Server software release 1.0.

ChoiceNet can be used with the Livingston PortMaster™ family of products running ComOS™ release 3.5 or later. To install and configure these products, see "Related Documentation" on page xii.

This guide is designed to be used by qualified system administrators and network managers. Knowledge of UNIX and basic networking concepts is required to successfully install ChoiceNet. If you use ChoiceNet with the Remote Authentication Dial-In User Service (RADIUS™), you must be familiar with RADIUS installation, configuration, and use.

Preview of This Guide

The *ChoiceNet Administrator's Guide* includes the following chapters and appendixes:

Chapter 1, "Introducing ChoiceNet," provides an overview of ChoiceNet features.

Chapter 2, "Configuring a ChoiceNet Server," provides step-by-step installation and configuration instructions for ChoiceNet servers.

Chapter 3, "Configuring a ChoiceNet Client," provides step-by-step configuration instructions for ChoiceNet clients (PortMasters).

Chapter 4, "Installing User Notification," describes how to install notification pop-ups on user computers.

Chapter 5, "Using ChoiceNet," provides an overview of packet filters, describes how to construct filters for ChoiceNet, describes how to use site lists, and provides examples of ChoiceNet use.

Appendix A, "Troubleshooting," describes what to look for if you encounter problems and suggests possible solutions.

Appendix B, "Defining Filter Rules," describes the parameters and syntax used to define rules for filters.

Appendix C, "Port Assignments," lists the assignment between well-known TCP and UDP services and well-known ports.

Appendix D, "Preconfiguration Worksheets," provides blank worksheets to collect server and client information you will need before installing and configuring ChoiceNet.

Related Documentation

The following manuals are available from Livingston. These manuals are included with most Livingston products; if they were not shipped with your unit, contact Livingston for ordering information.

The manuals are also provided as PDF and PostScript files on the *PortMaster Software CD* shipped with your PortMaster.

- *RADIUS Administrator's Guide*

  This guide provides complete installation and configuration instructions for Livingston RADIUS software.

- Installation guides

  These guides contain complete hardware installation instructions. An installation guide is available for each PortMaster product line—IRX™, Office Router, Communications Server, and Integrated Access Server.

- *Configuration Guide for PortMaster Products*

  This guide provides an overview of PortMaster hardware, networking concepts, and configuration of PortMaster products.

- *Command Line Administrator's Guide*

  This guide provides the complete description and syntax of each command in the ComOS command set.

- *PMconsole for Windows Administrator's Guide*

This guide covers PMconsole™ Administration Software for Microsoft Windows, a graphical tool for configuring the PortMaster. The majority of the material in this guide also applies to the UNIX version of PMconsole.

Additional References

RFCs

Use any World Wide Web browser to find a Request for Comments (RFC) online.

RFC 768, *User Datagram Protocol*

RFC 791, *Internet Protocol*

RFC 792, *Internet Control Message Protocol*

RFC 793, *Transmission Control Protocol*

RFC 1035, *Domain Names—Implementation and Specification*

RFC 1700, *Assigned Numbers*

RFC 2058, *Remote Authentication Dial In User Service*

Books

Building Internet Firewalls. D. Brent Chapman and Elizabeth D. Zwicky. Sebastopol, CA: O'Reilly & Associates, Inc., 1995. (ISBN 1-56592-124-0)

DNS and BIND. Paul Albitz and Cricket Liu. Sebastopol, CA: O'Reilly & Associates, Inc., 1992. (ISBN 1-56592-010-4)

Firewalls and Internet Security: Repelling the Wily Hacker. William R. Cheswick and Steven M. Bellovin. Reading, MA: Addison-Wesley, 1994. (ISBN 0-201-63357-4)

Document Conventions

The following conventions are used in this guide:

Convention	Use	Examples
Bold font	Indicates a user entry—a command, menu option, button, or key—or the name of a file, directory, or utility, except in code samples.	• Enter **version** to display the version number. • Press **Enter**. • Open the **permit_list** file.
Italic font	Identifies a command-line placeholder. Replace with a real name or value.	• **set** *Ether0* **address** *Ipaddress* • Replace *Area* with the name of the OSPF area.
Square brackets ([])	Enclose optional keywords and values in command syntax.	• **set nameserver** [**2**] *Ipaddress* • **set** *S0* **destination** *Ipaddress* [*Ipmask*]
Vertical bar (|)	Separates two or more possible options in command syntax.	• **set** *S0* | *W1* **ospf on** | **off** • **set** *S0* **host default** | **prompt** | *Ipaddress*

Contacting Livingston Technical Support

The PortMaster comes with a 1-year hardware warranty.

To obtain technical support, contact Livingston Enterprises Monday through Friday between the hours of 6 a.m. and 5 p.m. (GMT -8). Please record your Livingston ComOS version number and report it to the technical support staff.

- By voice, dial (800) 458-9966 within the USA (including Hawaii), Canada, and the Caribbean, or +1 (510) 426-0770 from elsewhere.
- By FAX, dial +1 (510) 426-8951.
- By electronic mail (email), send mail to **support@livingston.com**.
- Using the World Wide Web, see **http://www.livingston.com/**.

You can schedule 1-hour software installation appointments in advance by calling the technical support telephone number listed above.

New releases and upgrades of Livingston software are available by anonymous FTP from **ftp.livingston.com**.

Subscribing to Livingston Mailing Lists

Livingston maintains the following Internet mailing lists for PortMaster users:

- **portmaster-users**—a discussion of general and specific PortMaster issues, including configuration and troubleshooting suggestions. To subscribe, send email to **majordomo@livingston.com** with **subscribe portmaster-users** in the body of the message.

  The mailing list is also available in a daily digest format. To receive the digest, send email to **majordomo@livingston.com** with **subscribe portmaster-users-digest** in the body of the message.

- **portmaster-radius**—a discussion of general and specific RADIUS issues, including configuration and troubleshooting suggestions. To subscribe, send email to **majordomo@livingston.com** with **subscribe portmaster-radius** in the body of the message.

  The mailing list is also available in a daily digest format. To receive the digest, send email to **majordomo@livingston.com** with **subscribe portmaster-radius-digest** in the body of the message.

- **portmaster-announce**—announcements of new PortMaster products and software releases. To subscribe, send email to **majordomo@livingston.com** with **subscribe portmaster-announce** in the body of the message. All announcements to this list also go to the portmaster-users list. You do not need to subscribe to both lists.

Introducing ChoiceNet 1

ChoiceNet is a client/server packet-filtering application created by Livingston. ChoiceNet provides a mechanism to filter network traffic on dial-up remote access, synchronous leased line, or asynchronous connections. Filter information is stored in a central location known as the **ChoiceNet server**.

ChoiceNet **clients** can be one or more PortMaster 2 Communications Servers, PortMaster IRX Routers, PortMaster Office Routers, PortMaster 3 Integrated Access Servers, or PortMaster FireWall IRX Routers. ChoiceNet clients communicate with the ChoiceNet server to determine user access.

ChoiceNet can use filter names specified by the Remote Authentication Dial-In User Service (RADIUS) user record.

This chapter includes the following topics:

Overview of ChoiceNet Features

ChoiceNet provides the following features:

- **Custom Access.** The ChoiceNet server uses **site lists** to control access to specific hosts, Web sites, and Internet addresses. With ChoiceNet, a single filter rule can specify an entire list of hosts or IP addresses. Internet service providers (ISPs) can fine-tune access to their customers' specific needs. For example, a school district can select only child-oriented sites for student access. Corporations can limit employee access to external sites to enhance employee productivity.

- **Simplified Management.** In large networks without a ChoiceNet server, filters must be scattered throughout the network on different communications servers or routers. ChoiceNet enables all filters to be stored on one host. Storing filters on the ChoiceNet server frees memory on the PortMasters for other uses. Central storage eliminates the need for updating filter tables on many individual clients. You can easily add new site lists and filters or modify existing information on the server.
- **Tight Security.** ChoiceNet filtering enables system administrators to restrict internal network access by establishing TCP and UDP sessions only as defined in a rule set. Any traffic not permitted in the rule set is denied. External access to internal networks can be denied entirely or constrained to specific subnets.
- **Flexibility.** ChoiceNet enables both inbound and outbound traffic filtering for each interface and user. Each interface, whether synchronous, asynchronous, or Ethernet, can have a customized set of rules. ChoiceNet filters IP traffic by comparing TCP, UDP, and ICMP packets against the filter rules.
- **Logging Capabilities.** The ChoiceNet server can log all ChoiceNet activities to the console or a file. You can use **syslog** to analyze information collected in the file for troubleshooting.

ChoiceNet server software is available for the following operating systems:

- AIX 4.1
- Alpha Digital UNIX 3.0
- BSD/OS 2.0
- HP-UX 10.01
- IRX 5.2
- Linux 1.2.13 (ELF)
- Solaris 2.5.1
- Solaris x86 2.5.1
- SunOS 4.1.4

ChoiceNet Functions

The two main functions of ChoiceNet are centralized site lists and centralized filter management.

Centralized Site Lists

ChoiceNet enables you to write filter rules to specify a site list in place of an IP address. You can replace either a source or destination IP address in a rule—but not both in the same rule. Each site list is a text file that contains the hostnames or IP addresses of hosts for which access is controlled. The rule can permit or deny access by hosts on the list or to hosts on the list.

You store the site lists on the ChoiceNet server. The number of lists that you can add to this directory is unlimited.

Centralized Filter Management

When filters are stored locally in the nonvolatile configuration memory on each router or communications server, the amount of memory available on these devices limits the number of rules in each filter and the number of filters defined. For example, most PortMasters have 1MB of nonvolatile memory, which limits local storage to no more than 150 packet filters.

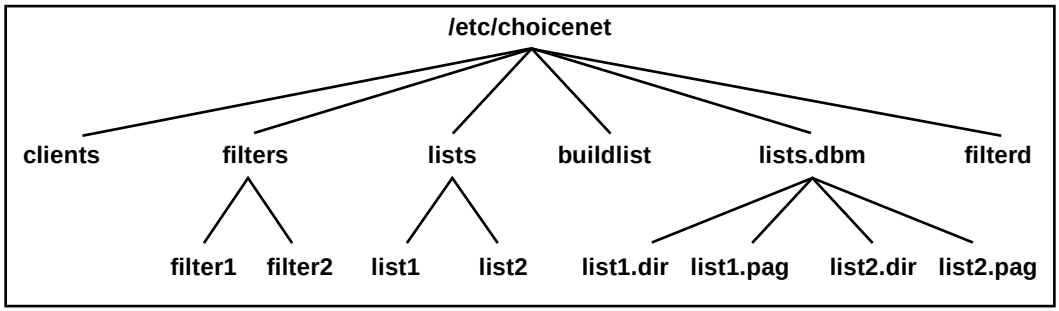
In contrast, ChoiceNet enables you to centralize the storage of an unlimited number of user-specific filters on the server. When a user dials in to the network, if the appropriate filter does not reside locally on the client, the client sends a request to the ChoiceNet server to look up the filter. If the name of the filter assigned to the interface matches a filter defined on the ChoiceNet server, the filter is downloaded to the client. This feature simplifies filter management and reduces the memory required on the client.

ChoiceNet can download filters from the server dynamically—on demand—to asynchronous and synchronous interfaces. To apply filters to an Ethernet interface, however, you must store the filters locally on the client. ChoiceNet cannot load filters dynamically for an Ethernet interface.

ChoiceNet Directory Structure

ChoiceNet server files are stored by default in a directory named **/etc/choicenet**. This directory contains files and subdirectories organized as shown in Figure 1-1.

Figure 1-1 ChoiceNet Directory Structure



The ChoiceNet server process, **filterd**, uses the **clients** file, filters, site lists, user notification, and activity logging.

- **filterd Process.** The **filterd** process runs on a UNIX host. It can be started from **/etc/rc.local** or manually executed. It listens on UDP port 1647 for requests from clients to download a filter or to verify whether a host is a member of a site list.
- **Clients File.** The **clients** file is used for communication between the ChoiceNet server and its clients. It contains the names or IP addresses of ChoiceNet clients and their **shared secrets**. The **filterd** process consults this file to verify the validity of the ChoiceNet clients sharing the secret with the server.
- **ChoiceNet Filters.** You define filters, or rule sets, to specify permissions for site access and network services. Although the filters can reside locally on the client, ChoiceNet enables you to store filters in the **filters** directory on the central ChoiceNet server. Filters are then dynamically downloaded to the client when requested.
  - **Rules for Filters.** A ChoiceNet filter contains a list of rules. A ChoiceNet client executes the rules from the top down as they are presented in the filter text file.
  - **Port Services.** The Internet Assigned Numbers Authority (IANA) specifies the association between TCP and UDP network services and port numbers on IP networks—**well-known services** and **well-known port numbers**.

ChoiceNet controls access to these network services for source and destination hosts by comparing the port number or service requested with a port number specified in a filter rule. See Appendix C, "Port Assignments," for more information.

- **Site Lists.** You create and store site lists in the **lists** directory on the ChoiceNet server. Filter rules can use these lists instead of source or destination host addresses to evaluate access requests.

  The **buildlist** utility resolves all hostnames in the **lists** directory into IP addresses using the Domain Name System (DNS). The utility places this information in database files in the **lists.dbm** directory. The actual names of the files created in the **/etc/choicenet/lists.dbm** directory can vary depending on your operating system.

  The ChoiceNet server uses this database for faster searching when the PortMaster requests the server to determine whether a site is in a list specified in a filter rule.

- **User Notification.** When a filter denies access to a site or network service, it can send a notification to the source host, displaying a pop-up notification window to PC or Macintosh dial-up users.

- **Activity Logging.** The **filterd** process logs its activity to **syslog**. You can instruct **filterd** to log activity to a file—see "Starting ChoiceNet" on page 2-7.

How ChoiceNet Operates

You can use ChoiceNet with or without the RADIUS protocol.

ChoiceNet Filtering with RADIUS

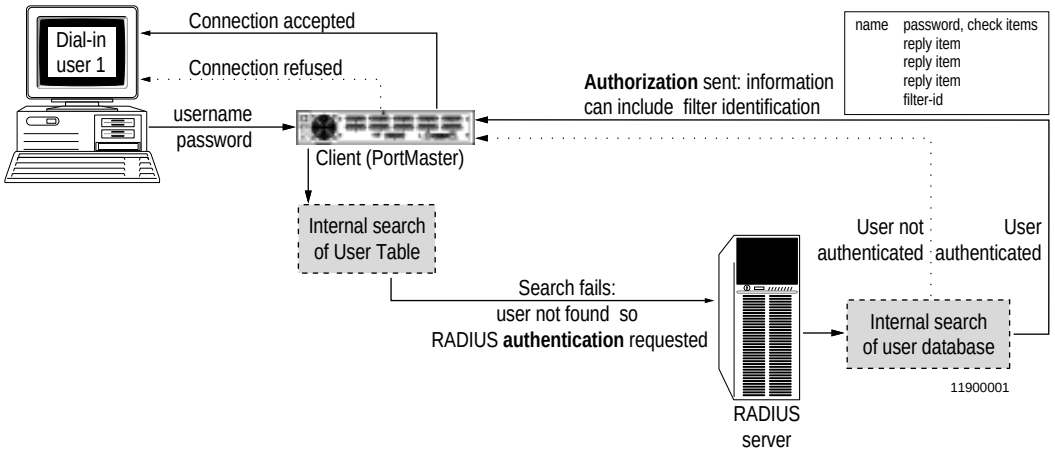
If a **User Table** entry or a RADIUS *Filter-Id* specifies a filter that is not in the **Filter Table** on the PortMaster, the PortMaster sends a request to the ChoiceNet server to download the filter.

A ChoiceNet filter rule can specify a site or address list instead of either a source or destination address. If the rest of the rule matches, the PortMaster determines from the ChoiceNet server whether the site is on that list. The PortMaster then takes the action required by the rule based on the server's response. The PortMaster caches the response for future use.

Example

In Figure 1-2, a dial-in user logs in to a PortMaster. The PortMaster first searches its User Table for the dial-in user. If the user is found in the User Table, the user is authenticated for the User Table.

Figure 1-2 RADIUS Authentication and Authorization

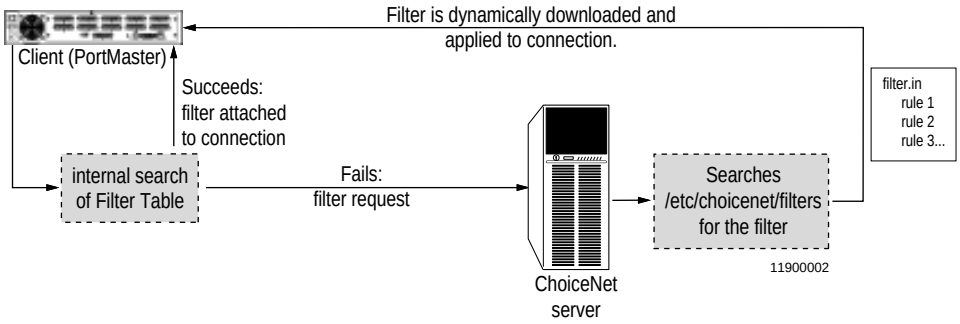


If the user is not found in the User Table, the PortMaster requests the RADIUS server to **authenticate** the user. The RADIUS server searches its user database. If it does not find the **user entry** for the dial-in user, or if the password for the user does not match, the RADIUS server sends a message to the PortMaster to reject the connection.

If the user is authenticated, the RADIUS server sends information to the PortMaster that **authorizes** the connection. This information consists of the **reply items** from the user entry that tell the PortMaster how to configure the connection. One of the reply items is the *Filter-Id* that associates a filter with the user. For example, if the *Filter-Id* is **wwwok**, then the input filter for the user is **wwwok.in** and the output filter is **wwwok.out**.

In Figure 1-3, the dial-in user has successfully connected. The PortMaster searches the Filter Table for the filters specified by *Filter-Id* in the user entry. If the filters are present in the Filter Table, then they are applied to the connection.

Figure 1-3 ChoiceNet Downloads a Filter to the PortMaster.

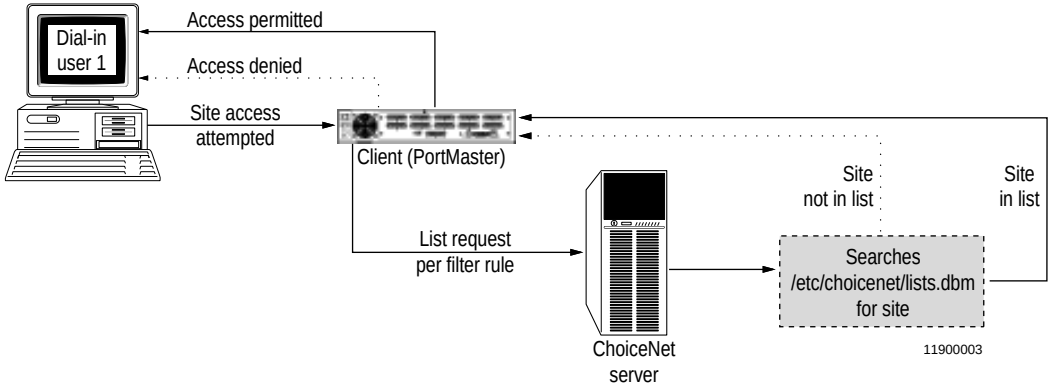


If a filter is not found in the Filter Table, the PortMaster sends a request to the ChoiceNet server to download the filter. The ChoiceNet server searches the **/etc/choicenet/filters** directory. If it finds the filter, the server downloads the filter to the PortMaster, where it is applied to the connection. This operation is called a **dynamic filter download**.

In Figure 1-4, the connected user attempts to access a particular site or service. The PortMaster compares the access request against the input filter rules. If the request matches a rule, the PortMaster takes the action—permit or deny—specified in the rule.

If a rule specifies a site list, the PortMaster sends a request to the ChoiceNet server to determine whether the site is on that list. This operation is called a **site list look-up**. The PortMaster caches the answer for future use.

Figure 1-4 Site Found or Not Found



The ChoiceNet server searches the **/etc/choicenet/lists.dbm** directory and notifies the PortMaster of the results. If the site is not in the list, then the rule does not match. If the site is in the list, the rule is matched and its action—permit or deny—is taken.

ChoiceNet Filtering without RADIUS

ChoiceNet operates exactly the same without RADIUS as it does with RADIUS, with the following exception:

- Filter names are found in the PortMaster User Table entry rather than in the *Filter-Id* reply item of a RADIUS user entry.

ChoiceNet Installation and Configuration

Table 1-1 provides a quick overview of the tasks required to install and configure ChoiceNet.

Table 1-1 Overview of ChoiceNet Installation and Configuration Tasks

Task	Instructions
1. Select a host to use as the ChoiceNet server.	See "Getting Started" on page 2-1.
2. Install the ChoiceNet server software on the host.	See "Installing ChoiceNet Server Software" on page 2-2.
3. Configure client information on the ChoiceNet server.	See "Configuring Client Information on the ChoiceNet Server" on page 2-5.
4. Start ChoiceNet.	See "Starting ChoiceNet" on page 2-7.
5. Configure the PortMaster as a ChoiceNet client.	See Chapter 3, "Configuring a ChoiceNet Client."
6. Optionally, install user notification files on users' computers (PC and Macintosh only).[1]	See Chapter 4, "Installing User Notification."
7. Construct site lists on the ChoiceNet server in **/etc/choicenet/lists**.[2]	See "Constructing Site Lists" on page 5-1.
8. Create filters on the ChoiceNet server in **/etc/choicenet/filters**.[2]	See "Constructing ChoiceNet Filters" on page 5-7.

1. If you do not install the user notification files, users will not know why they are denied access.

2. You do not have to use both features of ChoiceNet—site lists and centrally stored filters—but you must use one or the other.

Configuring a ChoiceNet Server 2

This chapter includes the following topics:

To configure ChoiceNet client information on a PortMaster, see Chapter 3, "Configuring a ChoiceNet Client."

To install access-denied notification windows on users' computers, see Chapter 4, "Installing User Notification."

Getting Started

Select a UNIX host with the following characteristics to use as the ChoiceNet server:

- Secure physical location
- Root access limited to the security officer or system administrator
- Limited number of user accounts, preferably none

If you are using RADIUS, the UNIX host where the RADIUS server resides is a good choice.

You must configure a shared secret on the ChoiceNet server for each client. The shared secret is an authentication key of up to 15 printable, nonspace, ASCII characters. It is stored as clear text in the **/etc/choicenet/clients** file on the ChoiceNet server and in the nonvolatile memory of the PortMaster. Each PortMaster can share a different secret with the ChoiceNet server, or multiple PortMasters can share the same secret. See "Configuring Client Information on the ChoiceNet Server" on page 2-5 for more information.

If you plan to use the ChoiceNet server with a RADIUS server, install and configure the RADIUS server first. See the *RADIUS Administrator's Guide* for instructions.

Livingston suggests that the host for the ChoiceNet server meet the following conditions:

- The host is accessible from outside your local network.
- The host does not run any public network services such as email, FTP, HTTP, or Telnet.

Appendix D, "Preconfiguration Worksheets," has blank worksheets you can use to collect server and client information you will need to install and configure ChoiceNet.

Installing ChoiceNet Server Software

Use one of the following installation methods:

- Install ChoiceNet server software with the **pminstall** utility shipped on the *PortMaster Software CD*.
- Install ChoiceNet server software without **pminstall**.

Note – Always use the latest version of **pminstall**, available by anonymous FTP from **ftp://ftp.livingston.com/pub/le/software**.

Installing with pminstall

To install ChoiceNet using **pminstall**, complete the following steps:

1. **Log in to the selected ChoiceNet server as root.**
2. **Mount the CD using the instructions in the CD booklet.**
3. **Install the PortMaster software by one of the following methods:**
   - Run **/cdrom/unix/setup**.
   - Follow the instructions in the CD booklet.
4. **Enter the /usr/portmaster/pminstall command at the UNIX prompt.**

The following list of choices appears:

```
% /usr/portmaster/pminstall

1. PortMaster Internet Address Setup
2. Host Installation
3. PortMaster Upgrade
4. Host Upgrade
5. Install RADIUS
6. Install ChoiceNet
7. Exit

Please select an option from above:
```

5. **Choose the Install ChoiceNet option to install all ChoiceNet files.**
   - The server prompts you for a directory name:

```
Directory to install ChoiceNet (/etc/choicenet):
```

6. **Provide directory information for ChoiceNet files by one of the following methods:**
   - Enter the appropriate directory.
   - Select the default directory (shown in parentheses) by pressing the **Return** or **Enter** key.
7. **When ChoiceNet installation is complete, select the Exit option to quit pminstall.**
8. **Go to "Configuring Client Information on the ChoiceNet Server" on page 2-5.**

Installing without pminstall

To install a ChoiceNet server without **pminstall**, complete the following steps:

1. **Log in to the selected ChoiceNet server as root.**
2. **Mount the CD on the /cdrom directory using the instructions in the CD booklet.**
3. **If you are running the Network Information Service (NIS) or NIS+, add the following line to the services NIS map on your NIS master and push the maps:**

```
choicenet      1647/udp      filterd
```

Note – Use the **make** *mapname* command on the NIS master to push the maps. This action updates the NIS database to include recently entered information. For details, consult your UNIX system documentation.

4. **If you are not running NIS or NIS+, add the following line to the /etc/services file:**

```
choicenet      1647/udp      filterd
```

5. **As root, enter the following commands on the ChoiceNet server:**

```
umask   022
mkdir   /etc/choicenet
chmod   700 /etc/choicenet
```

All ChoiceNet files are stored in the **/etc/choicenet** directory.

The **umask** and **chmod** commands affect the **choicenet** directory permissions; root access is required for read, write, and execute privileges.

6. **Copy all files in the /cdrom/unix/choicenet directory to the /etc/choicenet directory:**

```
cp   -r   /cdrom/unix/choicenet/*      /etc/choicenet
```

The **choicenet** directory contains the four subdirectories **clients**, **filters**, **lists**, and **lists.dbm**, and the file **logfile**.

7. **Copy the filterd file to the /etc/choicenet directory or to another directory such as /usr/sbin:**

```
cp   /cdrom/unix/platform/filterd      /etc/choicenet/filterd
```

   Replace *platform* with the name of your operating system—for example, **sun4_4.1**.

8. **Copy the buildlist utility to /etc/choicenet/buildlist:**

```
cp   /cdrom/unix/platform/buildlist      /etc/choicenet/buildlist
```

   Replace *platform* with the name of your operating system—for example, **sun4_4.1**.

9. **Go to "Configuring Client Information on the ChoiceNet Server" on page 2-5.**

Configuring Client Information on the ChoiceNet Server

The **/etc/choicenet/clients** file is a flat text file that stores information about ChoiceNet clients, including each client's name or IP address and its shared secret.

1. **To add a client, edit the text file and enter the client's name or IP address and the shared secret.**

   Shared secrets must consist of 15 or fewer printable, nonspace, ASCII characters. Control characters must not be used. You can add any number of clients to this file.

   Lines starting with the number sign (#) are ignored as comments.

   Examples of client names and shared secrets are displayed in Figure 2-1.

Figure 2-1 Example Client Names and Shared Secrets

```
#Client Name      Shared Secret
#-------------------------------------------------
portmaster1       wP40cQ0
portmaster2       A3X445A
192.168.1.2       wer369st
192.168.200.23    3jk3l5d&%vdpw89
```

2. **Verify that only root users have read and write access to the clients file.**

   As root, enter the following commands on the ChoiceNet server:

```
umask   077
chmod   600 /etc/choicenet/clients
```

   This is an important security precaution because the **clients** file contains the shared secrets for ChoiceNet clients. Figure 2-2 shows the correct permission setting for the **clients** file.

Figure 2-2 Example Permission Setting for the **clients** File

```
-rw------- 1 root daemon 802 Jul 15 00:21 clients
```

3. **Go to "Starting ChoiceNet" on page 2-7.**

Starting ChoiceNet

1. **Enter the following command to start the ChoiceNet server:**

```
/etc/choicenet/filterd
```

You can use **filterd** with any of the options shown in Table 2-1.

Table 2-1 **filterd** Options

Option	Purpose
-d	Specifies an alternate directory for ChoiceNet configuration files: **filterd -d** *directory* & The default directory is **/etc/choicenet**.
-x	Displays all ChoiceNet activities for troubleshooting.
-l *FileName*	Records ChoiceNet activities in *FileName*.
-v	Displays the ChoiceNet version. Always include the output of the **-v** option when reporting a problem to Livingston Technical Support.

2. **To start the filterd daemon each time the ChoiceNet server is booted, modify the /etc/rc.local file as shown in Figure 2-3.**

filterd is a standalone process; it must not be run from **/etc/inetd.conf**.

Figure 2-3 Modification of **/etc/rc.local** file to Start **filterd** on Reboot

```
#
# Start ChoiceNet
#
if [ -f /etc/choicenet/filterd ]; then
        echo "ChoiceNet"
        /etc/choicenet/filterd
fi
```

The name of the appropriate file might be different depending on your system. On some systems the file is named **/etc/rc2.d/S99choicenet.** Consult your UNIX system documentation for more information.

3. **Go to Chapter 3, "Configuring a ChoiceNet Client."**

Restarting the filterd Process

The **filterd** process automatically detects changes in the **clients** file and the **filters** directory. However, if you need to stop and restart the **filterd** process, perform the following procedure.

Note – The syntax for the **ps** command can vary depending on your operating system. Consult your system documentation for more information.

1. **Determine the UNIX process:**

```
ps -ax | grep filterd
```

2. **USe the kill command to stop the process:**

```
kill ProcessID
```

ProcessID is taken from the output of **ps** in step 1.

3. **Restart the process:**

```
/etc/filterd
```

Configuring a ChoiceNet Client 3

This chapter covers configuration of the PortMaster as a ChoiceNet client. The following items must be configured on each client:

- IP address of the primary ChoiceNet server
- ChoiceNet shared secret

Note – You must also add the PortMaster hostname or address and shared secret to the **/etc/choicenet/clients** file on the ChoiceNet server. See "Configuring Client Information on the ChoiceNet Server" on page 2-5.

You can configure ChoiceNet clients using either of the following interfaces:

Configuring a Client with the Command Line Interface

To configure the PortMaster using the command line interface, complete the following steps:

1. **Enter the IP address of the ChoiceNet server:**

```
Command> set choicenet Ipaddress
```

2. **Enter the secret shared by the PortMaster and ChoiceNet server:**

```
Command> set choicenet-secret String
```

The shared secret is a case-sensitive string of up to 15 printable, nonspace, ASCII characters. Control characters must not be used. If you specify a secret longer than 15 characters, ComOS will display an error message.

This is the same shared secret entered in the **clients** file on the ChoiceNet server (see page 2-5).

3. **If you are using ChoiceNet to download filters to the PortMaster on demand, set the number of concurrent PMconsole connections to the maximum:**

```
Command> set maximum pmconsole 10
```

The ChoiceNet server loads filters dynamically to the PortMaster using the PMconsole protocol on TCP port 1643 on the PortMaster. If you do not set the PMconsole connections to the maximum value, your own PMconsole connection might block ChoiceNet from downloading filters into the PortMaster.

Note – If you are using site lists only and not using dynamically loaded filters, you do not need to increase the number of PMconsole connections available to the PortMaster.

4. **Save your changes:**

```
Command> save all
```

5. **Go to Chapter 4, "Installing User Notification."**

   If you have no PC or Macintosh users, go instead to Chapter 5, "Using ChoiceNet," to construct site lists and create filters.

For more information on using the command line interface, refer to the *Command Line Administrator's Guide*.

Example

Suppose your ChoiceNet server has an IP address of 192.168.200.23. You have set the shared secret as 3jk3l5d&%vdpw89 on the server. Figure 3-1 shows the command sequence you enter on the PortMaster for these parameters.

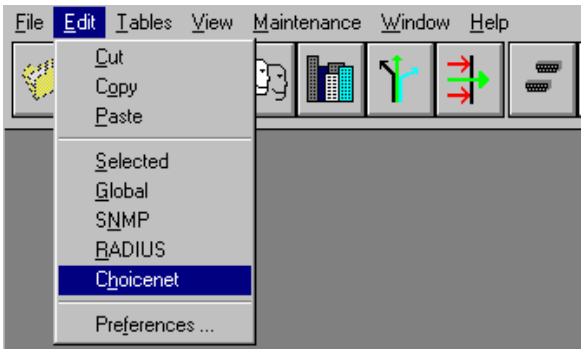
Figure 3-1 Example PortMaster Configuration Commands

```
Command> set choicenet 192.168.200.23
Command> set choicenet-secret 3jk3l5d&%vdpw89
Command> save all
```

Configuring a Client with PMconsole

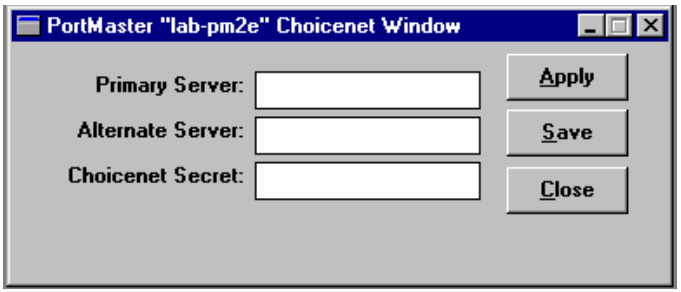
To configure the PortMaster using PMconsole, complete the following steps:

1. **Choose ChoiceNet from the Edit menu:**



The ChoiceNet window shown in Figure 3-2 appears.

Figure 3-2 ChoiceNet Window



2. **In the ChoiceNet Window, enter the IP address of the ChoiceNet server in the Primary Server field.**
3. **Enter the secret shared by the ChoiceNet client and ChoiceNet server.**

   For security reasons, the secret is not displayed in the dialog box.

   The shared secret is case-sensitive, and must consist of 15 or fewer printable, nonspace, ASCII characters. Control characters must not be used.
4. **Click the Save button to save the ChoiceNet settings.**
5. **Click the Done button to leave the window.**
6. **Go to Chapter 4, "Installing User Notification."**

   If you have no PC or Macintosh users, go instead to Chapter 5, "Using ChoiceNet," to construct site lists and create filters.

For more information on using PMconsole, refer to the *Configuration Guide for PortMaster Products* and the *PMconsole for Windows Administrator's Guide*.

Installing User Notification 4

ChoiceNet can notify users when it denies them access to a service or site. A pop-up window appears and displays the following message:

> Access denied; ChoiceNet by Livingston

The users must be on PCs or Macintoshes. You must load the software that produces this pop-up notification on each user's computer. You must use the **notify** keyword at the end of a deny rule in a filter to cause the pop-up to appear.

If the user is on a UNIX computer, a deny notification is sent to the **syslog** daemon.

This chapter includes the following topics:

Pop-Up Installation on a PC

To install the pop-up on a PC from the CD-ROM, complete **one** of the following procedures:

Procedure A

1. **Copy the /cdrom/unix/choicenet/notifier/pcpopup/choicene.exe file to the user's start-up directory.**
2. **Copy the /cdrom/unix/choicenet/notifier/pcpopup/choicen.ini file to the user's start-up directory.**
3. **Modify the choicen.ini file as desired to display a pop-up message different from the default.**
4. **Restart the PC.**

Procedure B

1. **Copy /cdrom/unix/choicenet/notifier/pcpopup/choicene.exe to C:\windows on the user's PC, and run choicene.exe to launch the pop-up.**
2. **Modify the choicen.ini file as desired to display a pop-up message different from the default.**

Pop-Up Installation on a Macintosh

To install the pop-up on a Macintosh from the CD-ROM, complete the following steps:

1. **Copy the /cdrom/unix/choicenet/notifier/macpopup file to the Macintosh desktop.**
2. **Double-click the icon to launch the pop-up.**

Using ChoiceNet 5

With a ChoiceNet server you can create lists of sites to provide custom access for dial-in and network users. You can create filters that use one or more of these lists to permit or deny user access.

ChoiceNet lets you centralize the storage of packet filters. Packet filters can control inbound or outbound traffic for each interface and user. You can apply filters to users, locations, or interfaces as either input or output filters. You can filter packets for TCP, UDP, and ICMP protocols.

This chapter includes the following topics:

For more information on filters, refer to the *Configuration Guide for PortMaster Products*.

Constructing Site Lists

This section describes how to construct site lists to customize user access, and provides several examples that explain how to use them.

ChoiceNet site lists are simple text files that you create and store in the **/etc/choicenet/lists** directory on the ChoiceNet server. The filename is the list name and consists of up to 15 printable, nonspace, ASCII characters. ChoiceNet lists can be created or modified at any time.

The site list contains the IP address—in dotted decimal notation—or the hostname of sites. Any number of sites can be included in a list. The site list file must have only one hostname or IP address per line. A simple site list appears in Figure 5-1.

Figure 5-1 Example Contents of **wwwok**, a Simple ChoiceNet Site List

```
homeserver.edu.com
www.site1.com
www.site2.com
www.site3.com
192.168.247.55
172.16.240.3
serverx.edu.com
```

Grouping Sites in a List

Group sites in a list according to the purpose of the list.

Preventing Access. If you want to prevent access to certain sites by network or dial-in users, you can place those sites together in one list. You can give this list any name, as long as the name meets the naming requirements—for example, **deny_list** or **no_go**.

Allowing Access. If you want to specify certain sites that users are expressly permitted to access, you can place those sites together in another list. You can give this list any name, as long as it meets the naming requirements—for example, **wwwok** or **permit_list**.

Using a Site List in a Filter Rule

To use a list in a filter rule, prefix the list name with an equal sign (=) as shown in Figure 5-2. See "Constructing ChoiceNet Filters" on page 5-7 and Appendix B, "Defining Filter Rules," for information about filter rules. You can use a site list for either the source or destination address in a rule, but not for both addresses in the same rule.

Figure 5-2 Example Filter Rule Using a Site List

```
permit 172.16.0.0/16 =wwwok tcp dst eq 80
```

Resolving Site Names to IP Addresses

When a connected user attempts to access a site, the PortMaster evaluates the request against the applied filter, starting at the first rule and continuing until it finds a rule that matches. If the rule includes a site list, the PortMaster determines from the ChoiceNet server whether the requested site is in the site list.

You must run the ChoiceNet **buildlist** utility if you add or change any lists in the **/etc/choicenet/lists** directory. This utility resolves any site names included in the lists to their IP addresses and constructs a DBM database of the resolved addresses. The structure of a DBM database enables the server to find IP addresses quickly.

To resolve the names for a specific list, run the utility on the server as follows:

```
/etc/choicenet/buildlist ListName
```

To resolve the names for all lists that have changed since the last time **buildlist** was run, run the utility as follows:

```
/etc/choicenet/buildlist
```

The ChoiceNet server uses the Domain Name System (DNS) for the Internet and the Network Information Service (NIS) for intranets to resolve names to addresses when you run **/etc/choicenet/buildlist**. The utility formulates a query for each name in a list in the **/etc/choicenet/lists** directory and sends the queries to a local domain name server. The name server translates the names to addresses and returns those to the ChoiceNet server. More information on DNS can be found in *DNS and BIND in a Nutshell* by Albitz and Liu.

The utility creates a DBM database in the **/etc/choicenet/lists.dbm** directory. Depending on your system, the database will consist of one of the following:

- Two files, ***ListName*.dir** and ***ListName*.pag**, for each *ListName* in the **/etc/choicenet/lists** directory
- One file, ***ListName*.db**, for each *ListName* in the **/etc/choicenet/lists** directory

Note – If name resolution fails and you want to rebuild the list, the DBM file(s) for the list must first be deleted.

Example: Resolving Lists

Suppose your **/etc/choicenet/lists** directory contains the lists shown in Figure 5-3.

Figure 5-3 Sample Contents of the **/etc/choicenet/lists** Directory

-rw-------	**1**	**root**	**other**	**200**	**Jan 30**	**11:59**	**wwwok**
-rw-------	**1**	**root**	**other**	**105**	**Jan 30**	**12:14**	**deny_list**

In this example, assume that on your system **buildlist** generates **.dir** and **.pag** DBM files instead of **.db** DBM files. The first time you run **buildlist**, it generates the files shown in Figure 5-4.

Figure 5-4 Sample Contents of the **/etc/choicenet/lists.dbm** Directory

-rw-------	**1**	**root**	**other**	**0**	**Jan 30**	**12:25**	**wwwok.dir**
-rw-------	**1**	**root**	**other**	**2048**	**Jan 30**	**12:25**	**wwwok.pag**
-rw-------	**1**	**root**	**other**	**0**	**Jan 30**	**12:25**	**deny_list.dir**
-rw-------	**1**	**root**	**other**	**1024**	**Jan 30**	**12:25**	**deny_list.pag**

A few days later, suppose you modify the **deny_list** file and add two new lists, **no_go** and **permit_list**, as shown in Figure 5-5.

Figure 5-5 Sample Modified Contents of the **/etc/choicenet/lists** Directory

-rw-------	**1**	**root**	**other**	**200**	**Jan 30**	**11:59**	**wwwok**
-rw-------	**1**	**root**	**other**	**200**	**Feb 4**	**08:24**	**deny_list**
-rw-------	**1**	**root**	**other**	**95**	**Feb 4**	**08:56**	**no_go**
-rw-------	**1**	**root**	**other**	**190**	**Feb 4**	**09:08**	**permit_list**

When you run **buildlist** now, it updates and generates the files as shown in Figure 5-6.

Figure 5-6 Sample Modified Contents of the **/etc/choicenet/lists.dbm** Directory

-rw-------	**1**	**root**	**other**	**0**	**Jan 30**	**12:25**	**wwwok.dir**
-rw-------	**1**	**root**	**other**	**2048**	**Jan 30**	**12:25**	**wwwok.pag**
-rw-------	**1**	**root**	**other**	**0**	**Feb 4**	**12:25**	**deny_list.dir**
-rw-------	**1**	**root**	**other**	**2048**	**Feb 4**	**12:25**	**deny_list.pag**
-rw-------	**1**	**root**	**other**	**0**	**Feb 4**	**12:25**	**no_go.dir**
-rw-------	**1**	**root**	**other**	**1024**	**Feb 4**	**12:25**	**no_go.pag**
-rw-------	**1**	**root**	**other**	**0**	**Feb 4**	**12:25**	**permit_list.dir**
-rw-------	**1**	**root**	**other**	**2048**	**Feb 4**	**12:25**	**permit_list.pag**

The files **wwwok.dir** and **wwwok.pag** are not updated because their modification dates (Figure 5-4) are more recent than that of the **wwwok** file (Figure 5-5). The modification date of the **deny_list** file (Figure 5-5) is more recent than that of the files **deny_list.dir** and **deny_list.pag** (Figure 5-4), so **buildlist** updates these files. The other two files are new, so **buildlist** generates directory files to resolve the included names.

Introduction to Packet Filters

Packet filters can limit certain kinds of internetwork communications by permitting or denying the passage of packets through network interfaces. By placing well-written rules in the appropriate sequence within a filter, you can control access to specific hosts, networks, and network services.

Packet filtering analyzes the header information contained in each packet sent or received through an interface. The header information is evaluated against a set of rules, which either allow the packet to pass freely through the interface or cause the packet to be discarded without being forwarded.

ChoiceNet passes the packet to permit access to a service or site, and discards a packet to deny access to a service or site. This process reduces network traffic and provides more immediate feedback to a user attempting unauthorized access.

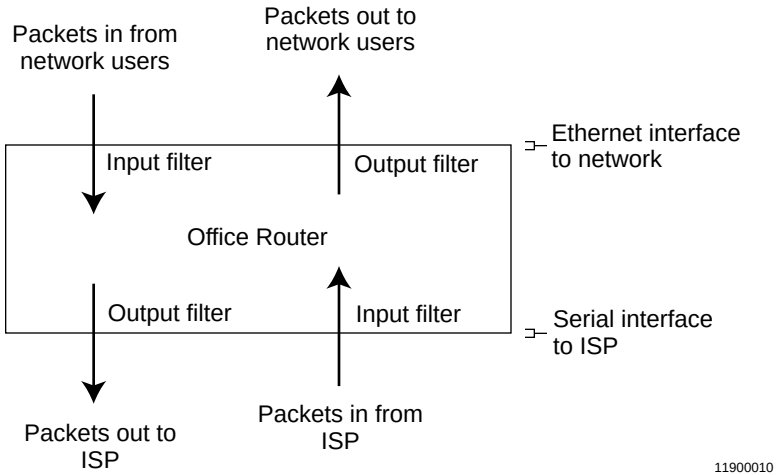
Each interface, whether synchronous, asynchronous, or Ethernet, can have a customized set of rules. For dial-in and dial-out interfaces, packet filters are enabled when a connection becomes active on the port (the port status on the PortMaster transitions to ESTABLISHED). For an Ethernet interface, filters are enabled as soon as the name of the input or output filter is applied to the interface.

Input and Output Filters

You can apply input filters, output filters, both input and output filters, or no filters to a user, location, or interface. The terms **input** and **output** are defined relative to the PortMaster.

Use an input filter to filter packets coming into a PortMaster on an interface. Use an output filter to filter packets going out of a PortMaster on an interface. Figure 5-7 shows examples of how to apply input and output filters for a network using an Office Router to access the Internet through an Internet service provider (ISP).

Figure 5-7 Examples of Input Filters and Output Filters



Filtering Methods

Packets can be filtered according to the following attributes:

- **Source and Destination Address.** A rule can evaluate either the source or destination address of a packet—or both. You can set the number of significant bits used in IP address comparisons to filter by a specific host, subnet, or network, or by a group of hosts whose addresses are within a bit-aligned boundary. Either the source or destination—but not both—can refer to a ChoiceNet site list.
- **Source and Destination Port.** Rules can use the source and destination port numbers to control access to certain network services. The rules evaluate whether the port number is less than, equal to, or greater than a specified value.

- **Protocol.** Rules can permit or deny TCP, UDP, or ICMP packets.
- **Established Session.** Rules can use the status of TCP connections. Network users can open connections to external networks without allowing external users access to the local network.

Constructing ChoiceNet Filters

You can create or modify ChoiceNet filters at any time, independent of any active packet filters. To use centralized storage and dynamic downloading for ChoiceNet filters, place the filters in the **/etc/choicenet/filters** directory on the ChoiceNet server. Each filter consists of a text file with the same name as the filter.

You can define input and output filters for Ethernet interfaces, hardwired serial ports, users, and locations. When ChoiceNet is used with RADIUS (the typical application), you can specify filters in user entries on the RADIUS server.

You can associate filters with network users configured for dial-in SLIP or PPP access. When the user makes a PPP or SLIP connection, the designated filters are applied to the interface used.

You can associate location filters to dial-out locations using SLIP or PPP connections. When the connection is established to a remote site, the designated filters are applied to the interface used.

Because filters are very flexible, you must carefully evaluate the types of traffic that a specific filter permits or denies through an interface. If possible, test filters to verify that the filter is operating as you intended. The **log** keyword is very useful when you are testing and refining filters.

Note – Any packet that is not explicitly permitted by a filter rule is denied. However, an empty filter permits everything. If you create a filter and apply it without defining any rules, the filter will permit all packets.

Filtering Guidelines

When creating filters for use with ChoiceNet, follow these guidelines:

- **Use Input and Output Filters Appropriately.** Both an input filter and an output filter can be applied to each user, each location, and each network interface. Having both input and output filters can decrease the number of rules needed and make it easier to design and apply your access policy.
- **Write Rules as Simply as Possible.** While each filter can have any number of rules, fewer rules are better. Each rule needs to include only as much information as is necessary for that filter. For example, if a rule is not based on specific source and destination addresses, those can be omitted.
- **Place Rules in the Proper Order.** Rules are loaded by ChoiceNet in order. If you create the filter with PMconsole or by editing a text file, the rules are processed in order of appearance. If you create the filter from the command line interface, the rules are processed according to their rule number.

  Placing rules in the order you want them evaluated eliminates ambiguity about how a packet is handled. The first rule that matches the packet is applied. If the rule is a **permit** statement, the packet is passed. If the first matching rule is a **deny** statement, the packet is discarded. If the packet does not match any of the rules, the packet is discarded.

  In addition, specify packets that represent the highest volume of traffic early in the list of rules, where possible. Give careful consideration to which services and sites are permitted or denied for which users or interfaces.

Creating Filters for the ChoiceNet Server

ChoiceNet filters are simple text files that the system administrator creates in the **/etc/choicenet/filters** directory. The filename is the filter name and consists of up to 15 printable, nonspace ASCII characters.

RADIUS requires that filter names must end with **.in** for input filters and with **.out** for output filters. However, you must omit the suffix from the filter name in the *Filter-Id* reply item in the RADIUS user entry. The PortMaster appends **.in** for the input filter and **.out** for the output filter when it applies the filter to the user.

The filter file contains the rules to be followed when the filter is applied. You define the rules with keywords and values as described in Appendix B, "Defining Filter Rules."

You can add comments to the filter by beginning each comment line with a number sign (#). Comments can be useful as the number of filters you administer increases.

Consider the example filter **net.in**. Figure 5-8 shows the contents of this simple filter with seven rules as stored in **/etc/choicenet/filters/net.in**.

Figure 5-8 Simple ChoiceNet Filter

```
#
#These are comment lines you can use to describe
#what this filter does or who it is for.
#
permit tcp estab
permit udp dst eq 53
permit tcp dst eq 53
permit tcp dst eq smtp
permit 0.0.0.0/0 =wwwok tcp dst eq 80
deny tcp dst eq 80 log notify
permit 0.0.0.0/0 =mailbox tcp dst eq 110
```

Table 5-1 describes each rule of the **net.in** filter.

Table 5-1 Description of Simple Filter

Rule	Description
1	Permits established TCP connections.
2	Permits DNS using UDP from any host to any host.
3	Permits DNS using TCP from any host to any host.
4	Permits outgoing email traffic (SMTP).
5	Permits Web access via HTTP to the addresses in the site list **wwwok**.
6	Displays a notification pop-up window on the user's machine when the user attempts to access via HTTP a Web site not specified in **wwwok**.
7	Permits access to hosts in the site list **mailbox** using Post Office Protocol (POP3) to pick up email.

Using the RADIUS Filter-Id Reply Item

When a ChoiceNet server is used with RADIUS, the ChoiceNet filters are associated with individual users in the RADIUS user entry. Each entry consists of a username, check items to authenticate the user, and reply items that provide information about the user and specify what that user can do. *Filter-Id* is a reply item that identifies the filter to be associated with that user. In the user entry shown in Figure 5-9, an input filter named **user.in** and an output filter named **user.out** will be applied to user *bob* when he connects.

Figure 5-9 RADIUS User Entry Specifying a Filter

```
bob     Password = "ge55gep"
        Service-Type = Framed-User,
        Framed-Protocol = PPP,
        Framed-MTU = 1500,
        Filter-Id = "user"
```

Do not specify the **.in** and **.out** suffixes in *Filter-Id*. When a user attempts access, the PortMaster appends the appropriate suffix to the filter name provided by RADIUS.

The PortMaster first looks for each filter in its local Filter Table. If it does not find the filter there, and a ChoiceNet server has been set, the PortMaster sends a request to the ChoiceNet server to download the filter.

Example 1: Limiting Child Access with ChoiceNet

An ISP can use ChoiceNet to offer special services to its subscribers. The ISP can customize access to sites or services for groups of subscribers that share similar interests. One group might be interested in access only to the Web, another in access to role-playing games, another only in sites that are church-related, and another only in sites that relate to business and economics.

This example shows how an ISP might offer a custom service for individual subscribers to provide access only to Web sites suitable for children (Figure 5-10). In this example, the ISP takes advantage of **Yahooligans**, a service available from Yahoo, Inc., and distributed with ChoiceNet. Yahooligans is a guided service for the Web designed specifically for children ages 8 through 13.

Figure 5-10 ISP Providing Custom Access for an Individual Subscriber

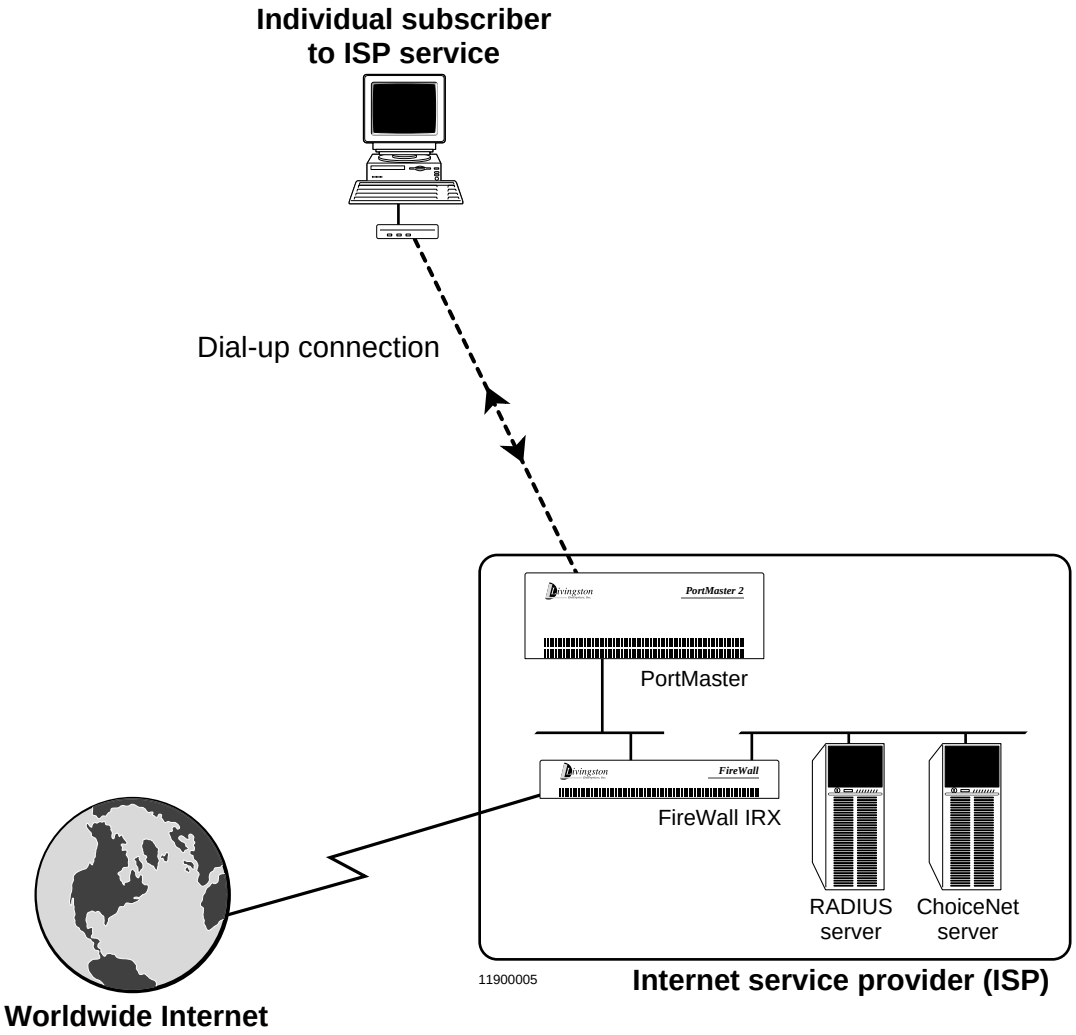


Figure 5-11 shows an example of a preconfiguration worksheet containing all the information needed to configure ChoiceNet for this example. Appendix D, "Preconfiguration Worksheets," has blank worksheets you can use to collect information before installing and configuring ChoiceNet.

Figure 5-11 Preconfiguration Worksheet for Example 1

Preconfiguration Worksheet	
PortMaster name	pm3.edu.net
PortMaster IP address	192.168.200.28
Shared secret	j42xlp3PQ56x
ChoiceNet server IP address	192.168.200.23
Names or addresses of sites to be placed in site list	www.nba.com www.stanford.edu www.abctelevision.com www.aetv.com
Site list name	yahooligans
Filter name	kids.in
Other filter requirements	Notify users when access is denied Permit established TCP sessions Permit ping Permit Domain Name Service look-up

Follow these steps to configure ChoiceNet to limit child access (Example 1):

1. **Establish the ChoiceNet service in the /etc/services file on the ChoiceNet server:**

```
choicenet      1647/udp      filterd
```

2. **On the ChoiceNet server in the /etc/choicenet/clients text file, do one of the following, but not both:**

- Define a ChoiceNet client name and shared secret:

```
#Client Name      Shared Secret
#-----------------------------------------
pm3.edu.net       j42xlp3PQ56x
```

- Define a ChoiceNet client IP address and shared secret:

```
#Client Name      Shared Secret
#-----------------------------------------
192.168.200.28    j42xlp3PQ56x
```

3. **On the PortMaster, specify the address of the ChoiceNet server and define the shared secret:**

```
Command> set choicenet 192.168.200.23
Command> set choicenet-secret j42xlp3PQ56x
Command> save all
```

4. **Create the /etc/choicenet/lists/yahooligans file on the ChoiceNet server:**

```
www.nba.com
www.stanford.edu
www.abctelevision.com
www.aetv.com
```

The list contains the Yahooligans-provided sites, one per line. The list is much abbreviated in this example.

5. **Resolve the names in the yahooligans list:**

```
/etc/choicenet/buildlist yahooligans
```

6. **Create the /etc/choicenet/filters/kids.in filter on the ChoiceNet server for the custom Yahooligans access:**

```
permit tcp estab
permit udp dst eq 53
permit tcp dst eq 53
permit 0.0.0.0/16 =yahooligans tcp dst eq 80
permit icmp
deny log notify
```

7. **Install the user notification pop-up on each user's PC or Macintosh, if desired.**

   Refer to Chapter 4, "Installing User Notification."

8. **Associate the kids.in filter with individual users on the RADIUS server.**

   To associate the filter with user *joey* for example, define the *Filter-Id* reply item in *joey*'s RADIUS user entry as the filter name, stripped of the suffix **.in**:

```
joey        Auth-Type = System
            Service-Type = Framed-User,
            Framed-Protocol = PPP,
            Framed-Address = 255.255.255.254,
            Framed-Routing = None,
            Framed-MTU = 1500,
            Filter-Id = "kids"
```

   When *joey* dials in to the PortMaster, RADIUS will apply the **kids.in** input filter on the interface coming into the PortMaster from the user.

9. **Start the filter daemon using the following command:**

```
/etc/choicenet/filterd
```

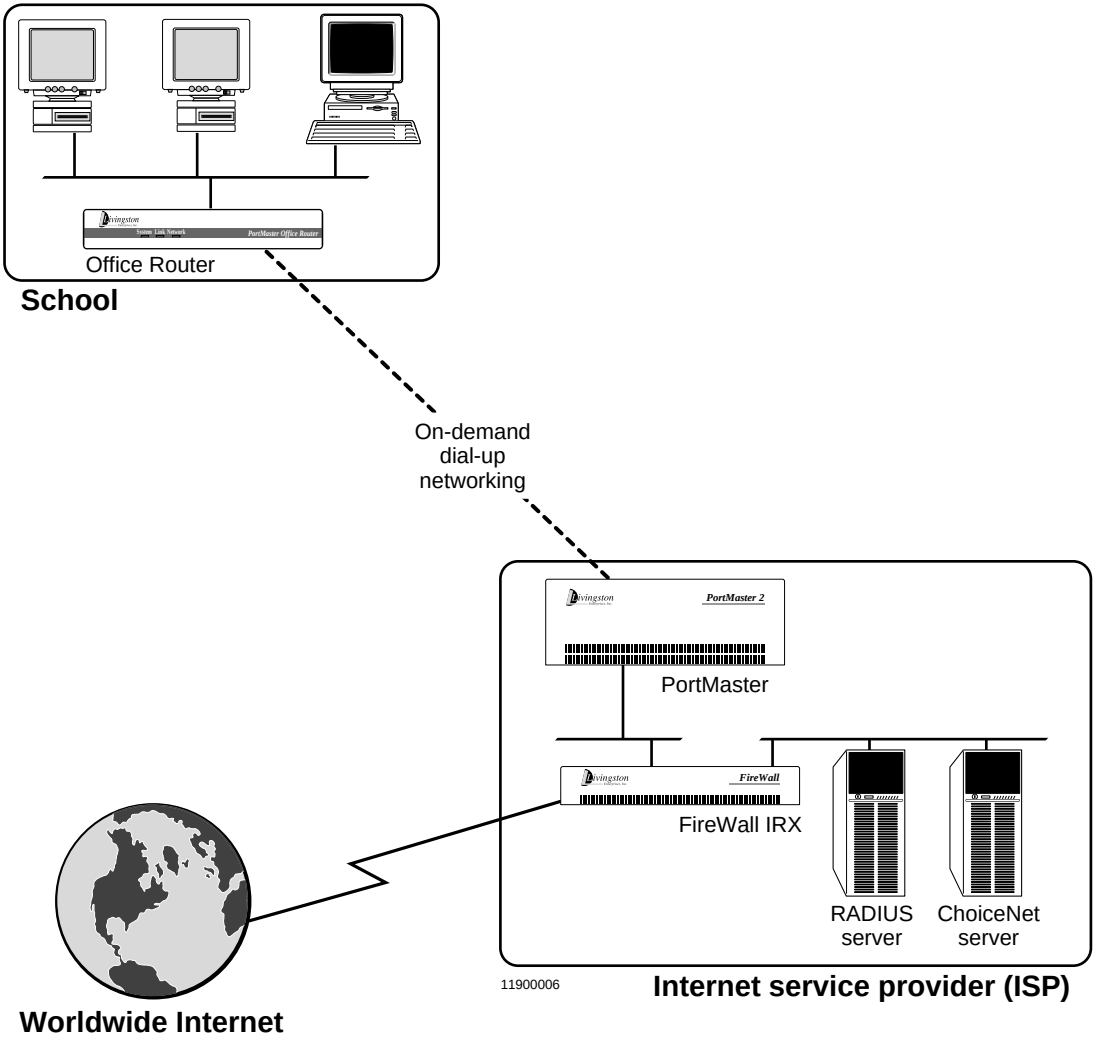
With this ChoiceNet filter in place, subscribers to the Yahooligans service can gain Web access to only the sites that are specified in the **yahooligans** list. The subscribers can only use DNS, HTTP, and ICMP services.

When a subscriber to this service attempts to connect to a site that is not listed in the **yahooligans** list, or tries to access a service not listed, such as FTP, the **notify** keyword in the rule opens a pop-up window on the subscriber's computer to inform the subscriber that access is denied. Because of the **log** keyword in the rule, the failed access attempt is also logged to the **auth.notice** facility of the client's loghost.

Example 2: Limiting Student Access with ChoiceNet

In this example, an ISP also uses the Yahooligans service to provide custom access to the Web. A school needs Web access for its students, but wants to ensure that they only access sites suitable for children (Figure 5-12). The ISP uses a filter to specify the **yahooligans** site list and deny students access to sites not in the list.

Figure 5-12 ISP Providing Custom Access for a School

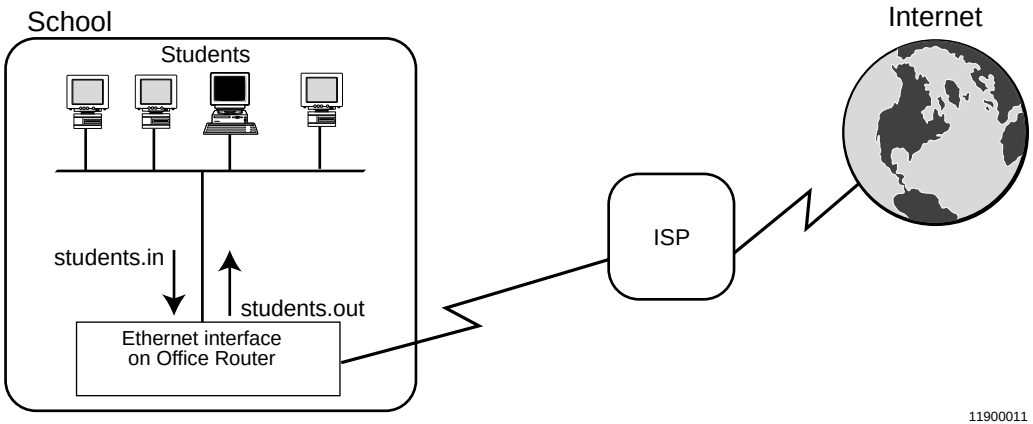


ChoiceNet cannot download filters dynamically on the interface used to reach the ChoiceNet server. In this example, the school uses on-demand dial-up networking to connect to the ISP and the ChoiceNet server. If the filter is applied on an interface at the school, the ISP cannot use the centralized filter storage feature of ChoiceNet. In this case, the filter must be stored in the Filter Table on the school's Office Router.

The ISP can apply filters at one or more interfaces to limit access by students at the school. Figure 5-13, Figure 5-14, and Figure 5-15 show several alternative methods.

School's Ethernet Interface. Figure 5-13 shows an input filter **students.in** and an output filter **students.out** applied on the Ethernet interface of the school's Office Router. The **students.in** filter evaluates packets coming into the Office Router from students on the school network. The **students.out** filter evaluates packets going out from the Office Router to students on the school network.

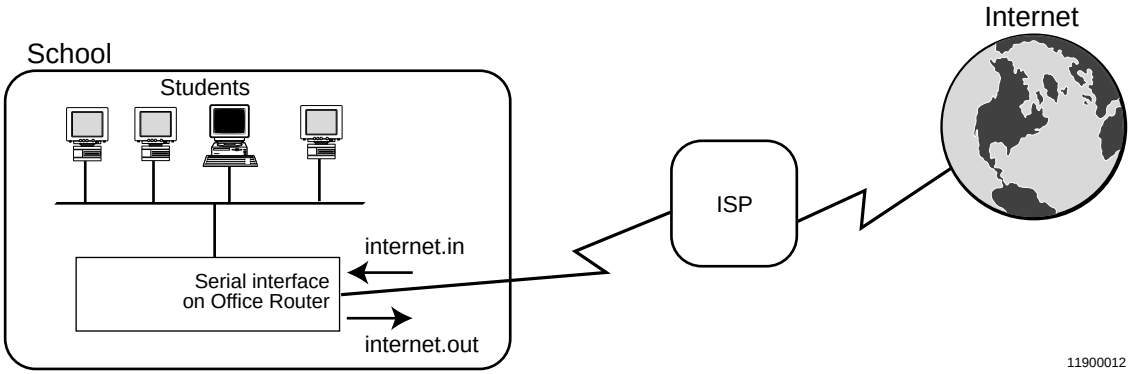
Figure 5-13 Filters Applied on the School's Office Router Ethernet Interface



School's Serial Interface. Figure 5-14 shows an input filter **internet.in** and an output filter **internet.out** applied on the serial interface of the school's Office Router. The **internet.in** filter evaluates packets coming into the Office Router from the Internet. The **internet.out** filter evaluates packets going out from the Office Router to the Internet.

This configuration cannot be used with a dynamically downloaded file, but can be used with a site list.

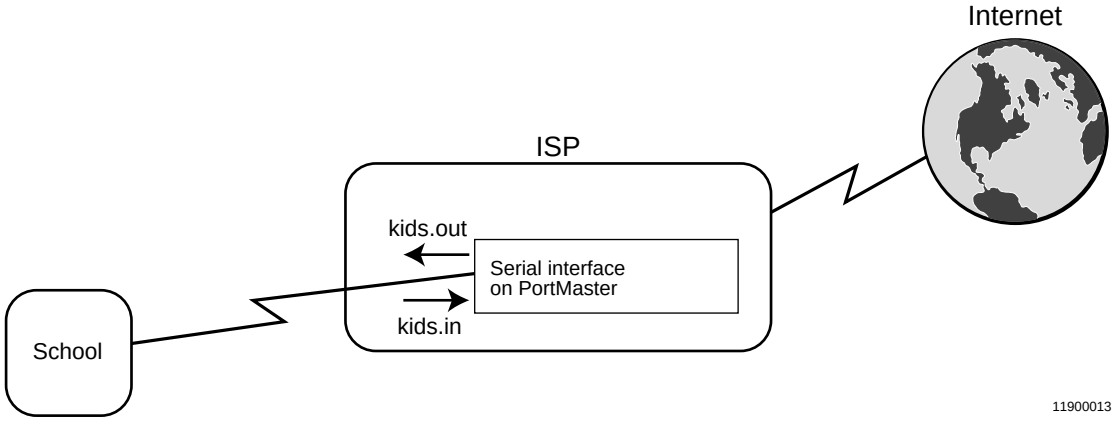
Figure 5-14 Filters Applied on the School's Office Router Serial Interface



ISP's Serial Interface. If the ISP is providing this service to a number of schools, storing the filters on the ChoiceNet server makes the filters easier to administer. Each filter can be stored on the ChoiceNet server and applied to an interface on the PortMaster at the ISP.

In Figure 5-15, the ISP has applied an input filter **kids.in** on the interface coming into the ISP's PortMaster from the school, and an output filter **kids.out** on the interface going out from its PortMaster to the school. The **kids.in** filter evaluates packets coming into the PortMaster from the school. The **kids.out** filter evaluates packets going out from the PortMaster to the school.

Figure 5-15 Filters Applied on the ISP's PortMaster Serial Interface



This example uses a variation of the method shown in Figure 5-15. Instead of both input and output filters, the example uses an input filter on the PortMaster interface from the school only. If a student requests access to sites not on the list, the filter denies the request packets from the student as the packets enter the ISP's PortMaster.

Figure 5-16 shows an example of a preconfiguration worksheet containing all the information needed to configure ChoiceNet for this example. Appendix D, "Preconfiguration Worksheets," has blank worksheets you can use to collect information before installing and configuring ChoiceNet.

Figure 5-16 Preconfiguration Worksheet for Example 2

Preconfiguration Worksheet	
PortMaster name	pm1.com.net
PortMaster IP address	192.168.225.3
Shared secret	56mjq312YTM
ChoiceNet server IP address	192.168.190.5
Names or addresses of sites to be placed in site list	www.nba.com www.stanford.edu www.abctelevision.com www.aetv.com
Site list name	yahooligans
Filter name	kids.in
Other filter requirements	Notify users when access is denied Permit established TCP sessions Permit ping Permit Domain Name Service look-up

Follow these steps to configure ChoiceNet to limit student access (Example 2):

1. **Add the ChoiceNet service in the /etc/services file on the ChoiceNet server:**

```
choicenet      1647/udp      filterd
```

2. **On the ChoiceNet server in the /etc/choicenet/clients text file, do one of the following, but not both:**

- Define a ChoiceNet client name and shared secret:

```
#Client Name      Shared Secret
#-----------------------------------------
pm1.com.net       56mjq312YTM
```

- Define a ChoiceNet client IP address and shared secret:

```
#Client Name      Shared Secret
#-----------------------------------------
192.168.225.3     56mjq312YTM
```

3. **On the PortMaster, specify the address of the ChoiceNet server and define the shared secret:**

```
Command> set choicenet 192.168.190.5
Command> set choicenet-secret 56mjq312YTM
Command> save all
```

4. **Create the /etc/choicenet/lists/yahooligans file on the ChoiceNet server:**

```
www.nba.com
www.stanford.edu
www.abctelevision.com
www.aetv.com
```

The list contains the Yahooligans-provided sites, one per line. The list is much abbreviated in this example.

5. **Resolve the names in the yahooligans list:**

```
/etc/choicenet/buildlist yahooligans
```

6. **Create the /etc/choicenet/filters/kids.in filter on the ChoiceNet server for the custom Yahooligans access:**

```
permit tcp estab
permit udp dst eq 53
permit tcp dst eq 53
permit 0.0.0.0/16 =yahooligans tcp dst eq 80
permit icmp
deny log notify
```

7. **Install the user notification pop-up on each user's PC or Macintosh, if desired.**

   Refer to Chapter 4, "Installing User Notification."

8. **Associate the kids.in filter with individual users on the RADIUS server.**

   To associate the filter with user *masumi*, for example, define the *Filter-Id* reply item in *masumi*'s RADIUS user entry as the filter name, stripped of the suffix **.in**:

```
masumi      Auth-Type = System
            Service-Type = Framed-User,
            Framed-Protocol = PPP,
            Framed-Address = 255.255.255.254,
            Framed-Routing = None,
            Framed-MTU = 1500,
            Filter-Id = "kids"
```

   When *masumi* dials in to the ISP's PortMaster, RADIUS will apply the **kids.in** input filter on the interface coming into the PortMaster from the school.

9. **Start the filter daemon using the following command:**

```
/etc/choicenet/filterd
```

With this ChoiceNet filter in place, students at the school service can gain Web access to only the sites that are specified in the **yahooligans** list. The students can use only DNS, HTTP, and ICMP services.

When a student attempts to connect to a site that is not listed in the **yahooligans** list, or tries to access a service not listed, such as FTP, the **notify** keyword in the rule opens a pop-up window on the student's computer to inform the student that access is denied. Because of the **log** keyword in the rule, the failed access attempt is also logged to the **auth.notice** facility of the ISP PortMaster's loghost.

Troubleshooting A

This appendix provides hints and tips for troubleshooting the ChoiceNet server. If the ChoiceNet server is being used with a RADIUS server, refer to the *RADIUS Administrator's Guide* first to verify that RADIUS is installed and configured properly.

This appendix includes the following topics:

Most problems occur because the server or the client was not configured correctly, or because a step was omitted during installation. Carefully check the instructions in Chapter 2, "Configuring a ChoiceNet Server," and Chapter 3, "Configuring a ChoiceNet Client," to ensure that ChoiceNet is installed and configured properly.

If you have not solved the problem after reviewing the instructions in Chapter 2 and Chapter 3, read the troubleshooting suggestions in this section.

Checking the filterd Daemon

On your ChoiceNet server, do the following:

1. **Use filterd -v to display the version number.**
2. **Make sure /etc/filterd is running.**
3. **Verify that the /etc/choicenet directory—or the directory specified with the -d option—contains the following files and directories: clients, filters, lists, and lists.dbm.**
4. **Use filterd -x to view incoming and outgoing packets from ChoiceNet.**

   This option displays all ChoiceNet server activity on the screen. Figure A-1 shows an example display of normal activity.

Figure A-1 Example Display of ChoiceNet Activity

```
Wed Dec 11 19:01:57 1996: [328] filterrecv: Request from host 95c69b01
code=20, id=1, length=32
Wed Dec 11 19:01:57 1996: [328] Filter-Name = "nogo"
Wed Dec 11 19:01:57 1996: [328] IP-Address = 192.31.7.130
Wed Dec 11 19:01:57 1996: [336] list nogo includes address 192.31.7.130
Wed Dec 11 19:01:57 1996: [336] IP address 192.31.7.130 found in list nogo
Wed Dec 11 19:01:58 1996: [336] sending info-accept of id 1 to 95c69b01
(149.198.155.1)
Wed Dec 11 19:02:44 1996: [328] filterrecv: Request from host 95c69b01
code=20, id=2, length=32
Wed Dec 11 19:02:44 1996: [328] Filter-Name = "nogo"
Wed Dec 11 19:02:44 1996: [328] IP-Address = 149.198.1.70
Wed Dec 11 19:02:44 1996: [337] list nogo does not include address
149.198.1.70
Wed Dec 11 19:02:44 1996: [337] IP Address 149.198.1.70 not found in list
nogo
Wed Dec 11 19:02:44 1996: [337] sending info-reject of id 2 to 95c69b01
(149.198.155.1)
Wed Dec 11 19:03:06 1996: [328] filterrecv: Request from host 95c69b01
code=20, id=3, length=32
Wed Dec 11 19:03:06 1996: [328] Filter-Name = "nogo"
Wed Dec 11 19:03:06 1996: [328] IP-Address = 192.9.9.100
Wed Dec 11 19:03:06 1996: [338] list nogo includes address 192.9.9.100
Wed Dec 11 19:03:06 1996: [338] IP address 192.9.9.100 found in list nogo
Wed Dec 11 19:03:07 1996: [338] sending info-accept of id 3 to 95c69b01
(149.198.155.1)
Wed Dec 11 19:03:40 1996: [328] filterrecv: Request from host 95c69b01
code=20, id=4, length=32
Wed Dec 11 19:03:40 1996: [328] Filter-Name = "nogo"
Wed Dec 11 19:03:40 1996: [328] IP-Address = 149.198.247.2
Wed Dec 11 19:03:40 1996: [339] list nogo does not include address
149.198.247.2
Wed Dec 11 19:03:40 1996: [339] IP Address 149.198.247.2 not found in list
nogo
Wed Dec 11 19:03:40 1996: [339] sending info-reject of id 4 to 95c69b01
(149.198.155.1)
```

Checking the PortMaster

1. **Verify that the ChoiceNet server is reachable from the client by one of the following methods:**

   – Use the **ping** command to send ICMP echo request packets to the ChoiceNet server address. The command displays a reply. Figure A-2 shows an example of a successful **ping** to a server at 192.168.200.23.

Figure A-2 Example **ping** Command

```
Command> ping 192.168.200.23
192.168.200.23 is alive
```

   – Use the **traceroute** command to trace the network route to the ChoiceNet server address. The command prints the addresses that send back ICMP Time Exceeded packets. Figure A-3 shows an example of a successful **traceroute** to a server at 192.168.200.23.

Figure A-3 Example **traceroute** Command

```
Command> traceroute 192.168.200.23
traceroute to (192.168.200.23), 30 hops max
1 192.168.200.3
2 192.168.156.40
3 192.168.200.25
```

   Refer to the *Command Line Administrator's Guide* for more information about these commands.

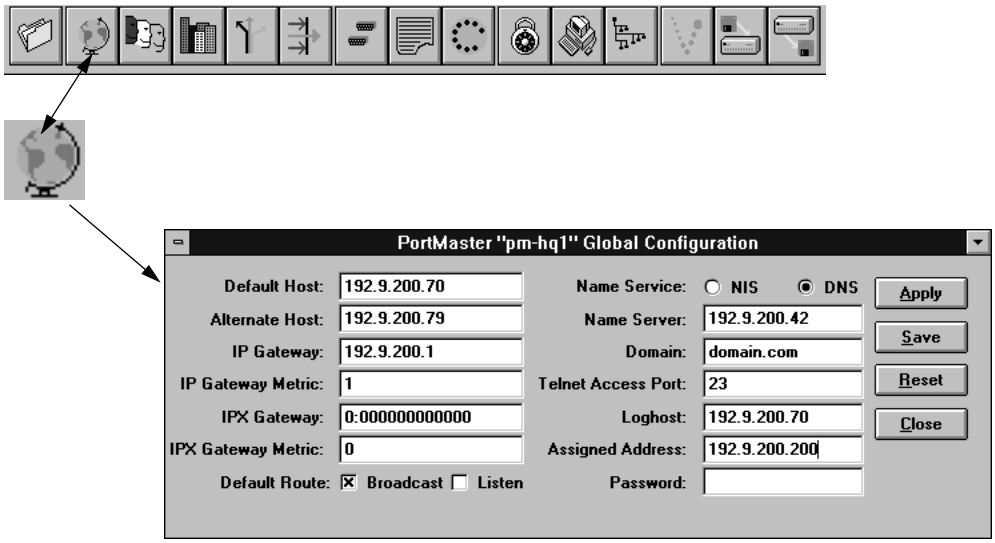
2. **Verify that the ChoiceNet server IP address is set on the client by one of the following methods:**

   – From the command line interface, display the global configuration parameters.

```
Command> show global
```

   – From PMconsole, click the **Global** button in the toolbar to bring up the Global Configuration window, as shown in Figure A-4.

Figure A-4 Opening the Global Configuration Window



3. **Verify that the secret set on the PortMaster matches the secret in the /etc/choicenet/clients file on the ChoiceNet server.**

   The PortMaster will not display the shared secret; however, you can set the secret again if you are not sure that it is set properly by one of the following methods:

   – Using the command line interface:

   ```
   Command> set choicenet-secret Password
   Command> save all
   ```

   – Using PMconsole. See "Configuring a Client with PMconsole" on page 3-3.

4. **Verify that any filters between the PortMaster and the ChoiceNet server are not blocking traffic between them.**

   You cannot use dynamic filters on the interface through which you access the ChoiceNet server.

Checking User Access

If ChoiceNet permits access to a site or service that should have been denied, or denies access that should have been permitted, examine the filter(s) and site list(s) involved.

1. **Run buildlist on the ChoiceNet server to verify that the lists are up-to-date:**

```
/etc/choicenet/buildlist
```

2. **Verify that the filter is written correctly, with the desired permissions or denials set.**

3. **Verify that the maximum number of PMconsole connections on the PortMaster is set:**

```
Command> set maximum pmconsole 10
Command> save all
```

   The **save all** command saves this setting in the nonvolatile memory of the PortMaster.

4. **Display and analyze all ChoiceNet activity by stopping and restarting filterd:**

   a. Use the **ps** command to find the process ID for **filterd**. The necessary command options vary with operating system. See "Restarting the filterd Process" on page 2-8 for an example. Refer to your system documentation for more information.

   b. Enter the **kill** command to stop **filterd**:

```
kill ProcessID
```

      ProcessID is taken from the output of **ps** in Step a.

   c. Restart **filterd** with the **-x** option:

```
/etc/choicenet/filterd -x
```

Defining Filter Rules B

The tables in this appendix describe the parameters and proper syntax to use when you define rules for filters. For more information on filtering, see the *Configuration Guide for PortMaster Products*.

This appendix includes the following topics:

Using a Site List Specifier

You can replace either the source or the destination host IP address with a ChoiceNet list specifier. You cannot replace both in the same rule. The filter looks up the specified site list on the ChoiceNet server.

Figure B-1 shows an example rule in which the source value *Ipaddress/NM* has been replaced with the **=***ListName* value. This rule permits users on the **internal_hosts** list to telnet to the host at 192.160.240.10.

Figure B-1 Example Rule Using a Source Site List

```
permit =internal_hosts 192.168.240.10 tcp dst eq 23
```

Figure B-2 shows an example rule in which the destination value *Ipaddress(dest)/NM* has been replaced with the *=ListName* value. This rule permits users from the source IP address 172.30.00/16 to access any Web sites on the **yahooligans** list.

Figure B-2 Example Rule Using a Destination Site List

```
permit 172.30.0.0/16 =yahooligans tcp dst eq 80
```

Filtering IP Packets

Use one of the three syntax forms presented in Table B-1 to define rules for filtering IP packets with the keywords and values described in Table B-2.

Table B-1 IP Rule Syntax

permit | **deny** [*Ipaddress*/*NM Ipaddress(dest)*/*NM*] [**log**] [**notify**]
or
permit | **deny** =*ListName Ipaddress(dest)*/*NM* [**log**] [**notify**]
or
permit | **deny** *Ipaddress*/*NM* =*ListName* [**log**] [**notify**]

You can use a hostname in a filter rule only if NIS or DNS is configured on the PortMaster, or if you are entering the filter with PMconsole.

Table B-2 IP Rule Keywords and Values

Keyword or Value	Description
permit	Permits the packet to pass through the interface.
deny	Stops the packet from passing through the interface. The packet is dropped, and an ICMP Host Unreachable message is sent to the source address.
Ipaddress	An IP address expressed in dotted decimal notation or as a hostname. The source IP address of the packet is compared with this value.

Table B-2 IP Rule Keywords and Values *(Continued)*

Keyword or Value	**Description**
Ipaddress(dest)	An IP address expressed in dotted decimal notation or as a hostname. The destination IP address of the packet is compared with this value.
/NM	The netmask that indicates the number of high-order bits of the source or destination IP address of the packet that must match an address in the filter. Any value between 0 and 32 inclusive, preceded by a slash (/), can be used; common mask values are /0—Matches all packets with any source address /16—Looks at high-order 16 bits of the address /24—Looks at high-order 24 bits of the address /32—Looks at the entire IP address
=	Identifies the following value as a site list specifier. There must not be a space between this identifier and the *ListName* value.
ListName	Specifies a list of source or destination sites in the **/etc/choicenet/lists** directory. The equal sign (=) identifier must immediately precede the value.
log	Packets matching the rule are logged by **syslog** to the loghost.
notify	Packets matching the rule are logged by **syslog** to the source of the packet. This keyword is used to cause a notification pop-up to appear on a user's computer.

Filtering TCP Packets

Use one of the three syntax forms presented in Table B-3 to define rules for filtering TCP packets with the keywords and values described in Table B-4.

Table B-3 TCP Rule Syntax

permit | **deny** [*Ipaddress*/*NM Ipaddress(dest)*/*NM*] **tcp** [**src eq** | **lt** | **gt** *Tport*] [**dst eq** | **lt** | **gt** *Tport*] [**established**] [**log**] [**notify**]
or
permit | **deny** =*ListName Ipaddress(dest)*/*NM* **tcp** [**src eq** | **lt** | **gt** *Tport*] [**dst eq** | **lt** | **gt** *Tport*] [**established**] [**log**] [**notify**]
or
permit | **deny** *Ipaddress*/*NM* =*ListName* **tcp** [**src eq** | **lt** | **gt** *Tport*] [**dst eq** | **lt** | **gt** *Tport*] [**established**] [**log**] [**notify**]

You can use a hostname in a filter rule only if NIS or DNS is configured on the PortMaster, or if you are entering the filter with PMconsole.

Table B-4 TCP Rule Keywords and Values

Keyword or Value	Description
permit	Permits the packet to pass through the interface.
deny	Stops the packet from passing through the interface. The packet is dropped, and an ICMP Host Unreachable message is sent to the source address.
IPaddress	An IP address expressed in dotted decimal notation or as a hostname. The source IP address of the packet is compared with this value.
Ipaddress(dest)	An IP address expressed in dotted decimal notation or as a hostname. The destination IP address of the packet is compared with this value.

Table B-4 TCP Rule Keywords and Values *(Continued)*

Keyword or Value	Description
/NM	The netmask that indicates the number of high-order bits of the source or destination IP address of the packet that must match an address in the filter. Any value between 0 and 32 inclusive, preceded by a slash (/), can be used; common mask values are /0—Matches all packets with any source address /16—Looks at high-order 16 bits of the address /24—Looks at high-order 24 bits of the address /32—Looks at the entire IP address
=	Identifies the following value as a site list specifier. There must not be a space between this identifier and the *ListName* value.
ListName	Specifies a list of source or destination sites in the **/etc/choicenet/lists** directory. The equal sign (=) identifier must immediately precede the value.
tcp	Specifies that the filter looks for TCP packets. Supports filtering on source and destination port numbers as well as the established state of a connection.
src	The TCP source port number is compared with the port number in the rule.
eq	The comparison determines whether the port number in the packet is equal to the port number specified in the rule.
lt	The comparison determines whether the port number in the packet is less than the port number specified in the rule.
gt	The comparison determines whether the port number in the packet is greater than the port number specified in the rule.
Tport	The port number for the TCP/IP connection; an integer from 0 to 65535.

Table B-4 TCP Rule Keywords and Values *(Continued)*

Keyword or Value	Description
dst	The TCP destination port number is compared with the port number in the rule.
established	Determines whether the packet is for an established TCP network connection. Packets being sent to start new TCP connections do not match this rule.
log	Packets matching the rule are logged by **syslog** to the loghost.
notify	Packets matching the rule are logged by **syslog** to the source of the packet. This keyword is used to cause a notification pop-up to appear on a user's computer.

Filtering UDP Packets

Use one of the three syntax forms presented in Table B-5 to define rules for filtering UDP packets with the keywords and values described in Table B-6.

Table B-5 UDP Rule Syntax

permit | **deny** [*Ipaddress*/*NM Ipaddress(dest)*/*NM*] **udp** [**src eq** | **lt** | **gt** *Uport*] [**dst eq** | **lt** | **gt** *Uport*] [**log**] [**notify**]
or
permit | **deny** =*ListName Ipaddress(dest)*/*NM* **udp** [**src eq** | **lt** | **gt** *Uport*] [**dst eq** | **lt** | **gt** *Uport*] [**log**] [**notify**]
or
permit | **deny** *Ipaddress*/*NM* =*ListName* **udp** [**src eq** | **lt** | **gt** *Uport*] [**dst eq** | **lt** | **gt** *Uport*] [**log**] [**notify**]

You can use a hostname in a filter rule only if NIS or DNS is configured on the PortMaster, or if you are entering the filter with PMconsole.

Table B-6 UDP Rule Keywords and Values

Keyword or Value	Description
permit	Permits the packet to pass through the interface.
deny	Stops the packet from passing through the interface. The packet is dropped, and an ICMP Host Unreachable message is sent to the source address.
IPaddress	An IP address expressed in dotted decimal notation or as a hostname. The source IP address of the packet is compared with this value.
Ipaddress(dest)	An IP address expressed in dotted decimal notation or as a hostname. The destination IP address of the packet is compared with this value.
/*NM*	The netmask that indicates the number of high-order bits of the source or destination IP address of the packet that must match an address in the filter. Any value between 0 and 32 inclusive, preceded by a slash (/), can be used; common mask values are /0—Matches all packets with any source address /16—Looks at high-order 16 bits of the address /24—Looks at high-order 24 bits of the address /32—Looks at the entire IP address
=	Identifies the following value as a site list specifier. There must not be a space between this identifier and the *ListName* value.
ListName	Specifies a list of source or destination sites in the **/etc/choicenet/lists** directory. The equal sign (=) identifier must immediately precede the value.
udp	Specifies that the filter looks for UDP packets. Supports filtering on source and destination port numbers.

Table B-6 UDP Rule Keywords and Values *(Continued)*

Keyword or Value	Description
src	The TCP source port number is compared with the port number in the rule.
eq	The comparison determines whether the port number in the packet is equal to the port number specified in the rule.
lt	The comparison determines whether the port number in the packet is less than the port number specified in the rule.
gt	The comparison determines whether the port number in the packet is greater than the port number specified in the rule.
Uport	The port number for the UDP/IP connection; an integer from 0 to 65535.
dst	The TCP destination port number is compared with the port number in the rule.
log	Packets matching the rule are logged by **syslog** to the loghost.
notify	Packets matching the rule are logged by **syslog** to the source of the packet. This keyword is used to cause a notification pop-up to appear on a user's computer.

Filtering ICMP Packets

Use one of the three syntax forms presented in Table B-7 to define rules for filtering ICMP packets with the keywords and values described in Table B-8.

Table B-7 ICMP Rule Syntax

permit | **deny** [*Ipaddress*/*NM Ipaddress(dest)*/*NM*] **icmp** [**type** *Itype*] [**log**] [**notify**] or **permit** | **deny** =*ListName Ipaddress(dest)*/*NM* **icmp** [**type** *Itype*] [**log**] [**notify**] or **permit** | **deny** *Ipaddress*/*NM* =*ListName* **icmp** [**type** *Itype*] [**log**] [**notify**]

You can use a hostname in a filter rule only if NIS or DNS is configured on the PortMaster, or if you are entering the filter with PMconsole.

Table B-8 ICMP Rule Keywords and Values

Keyword or Value	Description
permit	Permits the packet to pass through the interface.
deny	Stops the packet from passing through the interface. The packet is dropped, and an ICMP Host Unreachable message is sent to the source address.
IPaddress	An IP address expressed in dotted decimal notation or as a hostname. The source IP address of the packet is compared with this value.
Ipaddress(dest)	An IP address expressed in dotted decimal notation or as a hostname. The destination IP address of the packet is compared with this value.

Table B-8 ICMP Rule Keywords and Values *(Continued)*

Keyword or Value	Description
/NM	The netmask that indicates the number of high-order bits of the source or destination IP address of the packet that must match an address in the filter. Any value between 0 and 32 inclusive, preceded by a slash (/), can be used; common mask values are /0—Matches all packets with any source address /16—Looks at high-order 16 bits of the address /24—Looks at high-order 24 bits of the address /32—Looks at the entire IP address
=	Identifies the following value as a site list specifier. There must not be a space between this identifier and the *ListName* value.
ListName	Specifies a list of source or destination sites in the **/etc/choicenet/lists** directory. The equal sign (=) identifier must immediately precede the value.
type	Compares the ICMP message type in the rule with the ICMP source message type.
Itype	Type of ICMP packet; an integer 0 or higher. ICMP message types are defined in RFC 1700, "Assigned Numbers." Message types 0, 3, 8, and 11 are the most commonly used.
log	Packets matching the rule are logged by **syslog** to the loghost.
notify	Packets matching the rule are logged by **syslog** to the source of the packet. This keyword is used to cause a notification pop-up to appear on a user's computer.

Port Assignments C

Table C-1 lists common port numbers—**well-known ports**—assigned to TCP and UDP services—**well-known services**—by IANA. A more complete list is available in RFC 1700, "Assigned Numbers."

ChoiceNet always uses the port numbers for comparison. Filters stored on the server cannot use the service name. On most hosts, you can find the port numbers in the **/etc/services** file.

If you are not using a filter that is dynamically downloaded from the ChoiceNet server, the filters are stored on the PortMaster. If you create the filter using PMconsole, you can specify a service name for comparison only if you have configured the Internet services and aliases database—the **/etc/services** file—on the host correctly. PMconsole uses NIS to look up the specified name and converts it to the assigned port number.

If you are configuring a filter on a PortMaster from the command line interface, you must use the port number. The PortMaster does not have the **/etc/services** file and cannot use NIS to get the equivalent information.

Table C-1 TCP and UDP Port Services

Service	Port	Protocol	Description
ftp-data	20	TCP	File Transfer Protocol (FTP) (default data)
ftp	21	TCP	FTP (control)
telnet	23	TCP	Telnet
smtp	25	TCP	Simple Mail Transfer Protocol (SMTP) (email)
nicname	43	TCP	**whois** Internet directory service
nicname	43	UDP	**whois** Internet directory service
domain	53	TCP	Domain Name System (DNS)
domain	53	UDP	DNS
tftp	69	UDP	Trivial File Transfer Protocol (TFTP)

Table C-1 TCP and UDP Port Services *(Continued)*

Service	Port	Protocol	Description
gopher	70	TCP	Gopher
gopher	70	UDP	Gopher
finger	79	TCP	Finger Protocol
finger	79	UDP	Finger Protocol
www-http	80	TCP	World Wide Web Hypertext Transfer Protocol (HTTP)
kerberos	88	TCP	Kerberos authentication
kerberos	88	UDP	Kerberos authentication
pop3	110	TCP	Post Office Protocol (POP) version 3
sunrpc	111	TCP	SUN Remote Procedure Call (RPC)
sunrpc	111	UDP	SUN RPC
auth	113	TCP	Authentication service
auth	113	UDP	Authentication service
nntp	119	TCP	Network News Transfer Protocol (NNTP)
ntp	123	TCP	Network Time Protocol (NTP)
ntp	123	UDP	NTP
snmp	161	TCP	Simple Network Management Protocol (SNMP)
snmp	161	UDP	SNMP
snmptrap	162	TCP	SNMP system management messages
snmptrap	162	UDP	SNMP system management messages
imap3	220	TCP	Interactive Mail Access Protocol (IMAP) version 3
imap3	220	UDP	IMAP version 3
exec	512	TCP	Remote process execution
login	513	TCP	Remote login
who	513	UDP	Remote **who** daemon (rwhod)

Table C-1 TCP and UDP Port Services *(Continued)*

Service	Port	Protocol	Description
cmd	514	TCP	Remote command (rsh)
syslog	514	UDP	System log facility
printer	515	TCP	Line printer daemon (LPD) spooler
talk	517	TCP	Terminal-to-terminal chat
talk	517	UDP	Terminal-to-terminal chat
ntalk	518	TCP	Newer version of Terminal-to-terminal chat
router	520	UDP	Routing Information Protocol (RIP)
uucp	540	TCP	UNIX-to-UNIX Copy Protocol (UUCP)
uucp	540	UDP	UUCP
uucp-rlogin	541	TCP	Variant of UUCP/TCP
uucp-rlogin	541	UDP	Variant of UUCP/IP
klogin	543	TCP	Kerberized login
klogin	543	UDP	Kerberized login
pmd	1642	TCP	PortMaster daemon **in.pmd**
pmconsole	1643	TCP	PortMaster Console Protocol
radius	1645	UDP	Remote Authentication Dial-In User Service (RADIUS)
radacct	1646	UDP	RADIUS accounting
choicenet	1647	UDP	ChoiceNet

Preconfiguration Worksheets *D*

You can use the worksheets in this appendix to record the information you need before you install and configure ChoiceNet.

Preconfiguration Worksheet	
PortMaster name	
PortMaster IP address	
Shared secret	
ChoiceNet server IP address	
Names or addresses of sites to be placed in site list	
Site list name	
Filter name	
Other filter requirements	

Preconfiguration Worksheet

PortMaster name	
PortMaster IP address	
Shared secret	
ChoiceNet server IP address	
Names or addresses of sites to be placed in site list	
Site list name	
Filter name	
Other filter requirements	

Index

F

I

M

N

O

P

R

S

T

U

W

Y