CHAPTER 6

Using IP Filters with Cisco 700 Series Routers

This chapter describes how to implement the Internet Protocol (IP) filtering supported by the Cisco 700 series routers. IP filtering can be used to maintain network security by controlling the data that is allowed to be sent between specified networks.

This chapter contains the following sections:

- IP Filtering Overview
- User Profiles and IP Filters
- Configuring IP Filters

Note This chapter assumes basic knowledge of Transmission Control Protocol (TCP)/IP and IP packet format. If you are not familiar with these topics, refer to the section "Internet Protocols" in the appendix "Internetworking Background."

IP Filtering Overview

This section is a short descriptive overview of how the Cisco 700 series routers implement IP filtering.

IP filtering is the prevention of certain IP packets from being forwarded either onto the LAN or onto the ISDN line. Which packets are filtered is defined using a software configuration.

User Profiles and IP Filters

This section describes how to use IP filters in user profiles.

Note If you are not familiar with user profiles, refer to the appendix "Using Profiles with Cisco 700 Series Routers."

Each user profile can be configured with both outgoing and incoming IP filters:

- Outgoing filters—Determine which IP packets are sent over the ISDN line to the remote device that is associated with the user profile.
- Incoming filters—Determine which IP packets are received over the ISDN line from the remote device associated with the user profile.

The implication of incoming and outgoing filters is that, although certain IP packets might be accepted over an ISDN connection from a remote device, they will not be forwarded to any local or remote devices unless a user profile (associated with one of the local or remote devices) contains an outgoing filter for that specific IP packet type.

Configuring IP Filters

The **set ip filter** command is used while in profile mode to configure IP filters for a specific remote device.

You can configure IP filters to block or accept IP packets based on the following IP packet fields:

- Packet type
- Source address
- Destination address

The following is an example of the **set ip filter** command:

```
765:2503> set ip filter tcpsyn out block
```

With this configuration, the router will block any TCP SYN packets from being sent over the ISDN line to the remote device, a Cisco 2503. Because a TCP SYN packet is used to establish network connections, the Cisco 765 is prevented from connecting to the Cisco 2503.

Note Configuring IP filters as ACCEPT is more restrictive than configuring IP filters as BLOCK. If you configure a profile with ACCEPT filters, the router will only accept IP packets from the remote device that match the IP filter.

For more information on the **set ip filter** command, refer to the *Cisco 750 Series and Cisco 760 Series Command Reference* publication.