



# **OFFICECONNECT REMOTE DUAL ANALOG**

## **FILTERING WHITE PAPER**



# TABLE OF CONTENTS

<b>Introduction .....</b>	<b>4</b>
<b>OfficeConnect Remote Dual Analog Filtering Capabilities .....</b>	<b>4</b>
Filter Classes .....	4
<b>Filter Types .....</b>	<b>5</b>
Data Filters .....	5
Advertisement Filters .....	5
Generic Filters .....	6
Creating Filters .....	6
Filter File Components .....	7
Protocol Sections Filters .....	7
Protocol Rules .....	8
<b>Creating Filter Files .....</b>	<b>10</b>
<b>Configuring Filters .....</b>	<b>12</b>
Interface Filters .....	12
Input Filter .....	12
Output Filters .....	12
Call Filters .....	12
Input Filters vs. Output Filters .....	13
Remote Site Filters .....	13
<b>Assigning Filters .....</b>	<b>13</b>
Assigning a Filter on an Interface .....	13
Configuring a Filter for a User .....	14
<b>Converting Filter Files for the HTML Manager .....</b>	<b>14</b>
Change the File Name .....	14
Change the File Content .....	15
Complete the File Update .....	17
<b>Setting Filter Access .....</b>	<b>19</b>
<b>Managing Filters .....</b>	<b>19</b>

Displaying the Managed Filter List.....	19
Adding Filters to the Managed List.....	20
Removing a Filter from an Interface .....	20
Removing a Filter from a Remote Site.....	20
Deleting a Packet Filter .....	21
Verifying Filter File Syntax .....	21
Showing Filter File Contents.....	21
Source and Destination Address Filtering.....	21
<b>IP Filters.....</b>	<b>22</b>
IP RIP Packet Filtering.....	22
IP Call Filtering .....	22
<b>IPX Filters .....</b>	<b>23</b>
Source and Destination Network Filtering.....	23
Source and Destination Host Filtering .....	23
Source and Destination Socket Number Filtering.....	23
IPX RIP Packet Filtering.....	23
IPX SAP Packet Filtering.....	24
IPX Call Filtering .....	24
<b>Using Filters to Approximate Spoofing.....</b>	<b>24</b>
<b>Sample Filter.....</b>	<b>25</b>

---

## **Introduction**

The OfficeConnect Remote Dual Analog provides an extensive set of data and call filtering capabilities. For instance, filters can accept packets only from specific addresses to provide added security or can be added to reduce network traffic and improve overall performance.

Technically speaking, packet filters control inter-network data transmission by accepting or rejecting the passage of specific packets through network interfaces based on packet header information. When data packets are received by a network interface such as an Ethernet (LAN) or WAN port, a packet filter analyzes packet header information against a set of rules you define. A filter then lets the packet pass through or discards it.

---

## **OfficeConnect Remote Dual Analog Filtering Capabilities**

The OfficeConnect Remote Dual Analog supports the following filtering capabilities:

- Input and output data filtering.
- Source and destination address filtering.
- Protocol filtering.
- Source and destination port filtering; a packet filter can control what services local or remote users can access.
- Call filtering can control whether a packet can initiate an outgoing call.
- Route filtering can filter source and destination addresses in packets that exchange routing table information.
- Established session filtering; a packet filter can permit users to connect with a remote network without letting remote users have access to the local network (or vice versa).

### **Filter Classes**

OfficeConnect Remote Dual Analog supports four filter classes:

- Input data
- Output data

- Output call
- Embedded bypass of idle reset for periodic router protocol packets (IP RIP, IPX RIPSAP)

---

## **Filter Types**

Filters can be classified by the following types:

- **Data filters**—based on protocol-specific packet information
- **Advertisement filters** — based on broadcast packet information
- **Generic filters** — based on packet structure

### **Data Filters**

Data filters control network access based on the protocol, source/destination address, and port designation (for example, TCP and UDP port designations) of the packet. Table 1 describes the data filters supported by the OfficeConnect Remote Dual Analog.

**Table 1: Data Filters**

<b>Filter</b>	<b>Description</b>
IP	Controls network access based on the protocol and source/destination address. IP filter rules allow filtering on source address, destination address, protocol type, source port, and port designation of the IP packet.
IPX	Controls network access based on the protocol and source/destination network. IPX filter rules allow filtering on source network, destination network, protocol type, source socket, destination socket, source node, and node designation of the IPX packet.
Bridge	Controls network access based on source and destination MAC address

### **Advertisement Filters**

Advertisement filters operate on network protocol packets that contain varying information such as SAP or RIP. Filtering of these packets is performed by the specific protocol process. Table 2 describes the advertisement filters supported by the OfficeConnect Remote Dual Analog.

**Table 2: Advertisement Filters**

<b>Filter</b>	<b>Description</b>
IP-RIP	Controls the content of IP Routing Information Protocol (RIP) packets that are sent out or received on specific ports. The IP RIP filtering process filters addresses from the RIP packet upon transmission, and does not enter routes into the routing table upon receipt.
IPX-SAP	Controls the content of Service Advertising Protocol (SAP) packets that are sent out or received on specific ports. The IPX-SAP filter rules allow filtering on service type, server name, network address, node address, and socket number fields of the service entry. The forwarding process uses the filter information to prevent the service information from being included in the SAP packet.
IPX-RIP	Controls the content IPX RIP packets that are sent out or received on specific ports. The IPX RIP filtering process filters addresses from the RIP packet upon transmission, and does not enter routes into the routing table upon receipt.

## **Generic Filters**

Generic filters are protocol-independent and are specified by byte and offset values in a packet. Packets are filtered by comparing the packets offset value and byte information with the values that you define in the filter. The OfficeConnect Remote Dual Analog will accept or reject the packet based on the result.

*NOTE: Creating generic filters can be a complex task. Only experienced users should employ generic filters, and strictly in cases where data and advertising filters cannot provide the filtering capabilities that you require.*

## **Creating Filters**

The OfficeConnect Remote Dual Analog performs packet filtering based on packet filters that you create. There are two methods of creating filters: Through the HTML Manager or by editing a filter file, TFTPing it to the OfficeConnect Remote Dual Analog, and using CLI to add and apply the filters. The recommended method is to use the HTML Manager. See the HTML Manager User's guide for instructions for creating filters with HTML. This following section describes how to create the packet filters using CLI. To convert filter files created with CLI for the HTML Manager, see the section "Converting Filter Files for the HTML Manager."

## **Filter File Components**

You define the filtering rules used by the OfficeConnect Remote Dual Analog within filter files. Filter files are text files that are stored in the unit's FLASH memory. You can create and modify filter files using an off-line text editor, then TFTPping the finished file on to the OfficeConnect Remote Dual Analog.

To be valid, a filter file must always have the following file descriptor on the first line: **#filter**

Be sure that no blank space precedes the descriptor, or an error will occur.

The remainder of the filter file is partitioned into protocol sections. Each protocol section has a descriptive header and contains the filter rules for that protocol.

## **Protocol Sections Filters**

A single filter file can contain all valid protocol sections in any order, but the sections cannot be repeated. The following conditions will generate errors or prevent normal filter operation:

- If you do not specify a protocol section in the filter file, no filtering will occur and packets of that protocol type will be accepted
- If you specify a protocol section but do not define any rules, an error will occur. Table 3 describes the valid protocol sections that you can define in the filter file.

*NOTE: To comment out a protocol section, you must place a pound (#) sign before the section header and before all rules defined in the section.*

**Table 3: Protocol Sections**

<b>Protocol Sections</b>	<b>Descriptions</b>
IP:	IP protocol data filter section
IP-CALL:	IP protocol call filter section
IP-RIP:	IP RIP advertising filter section
IPX:	IPX protocol data filter section
IPX-CALL:	IPX protocol call filter section
IPX-RIP:	IPX RIP advertising filter section
IPX-SAP:	IPX SAP advertising filter section
BR-ETH:	Bridge protocol data filter
BR-ETH-CALL:	Bridge protocol call filter section

### **Protocol Rules**

You can define protocol rules within each protocol section in the filter file. Protocol rules determine which packets may and may not access the network. The rule syntax is:

<line #> <verb> <keyword> <operator> <value>

The combination of keyword, operator, and value forms the *condition* which, when combined with the verb, determines whether the packet is accepted or rejected.

When a packet is filtered, for example an IP packet, the OfficeConnect Remote Dual Analog parses each rule defined in the IP protocol section sequentially according to the line number. Filtering is performed based on the first match that occurs. If there is no match, by default the packet is accepted. For this reason, you should order your protocol rules so that the rules you expect to be most frequently matched are in the beginning of the section. This reduces the amount of parsing time that occurs during filtering. Table 4 describes each field used in the rule syntax.

**Table 4 : Protocol Rules**

<b>FIELD</b>	<b>DESCRIPTION</b>
line #	Each rule must have a unique line number (1 — 10). You must arrange rules in increasing order.
Verb	This field can be one of the following:  <b>ACCEPT</b> — Allow the packet access if the condition is met  <b>REJECT</b> — Do not allow the packet access if the condition is met  <b>AND</b> — Logically use the AND condition with condition of the next rule to determine if the packet is accepted or rejected. Both defined conditions must be met.
Keyword	The keywords for all protocol, descriptions, corresponding operators and values.
Operator	Describes the relationship between the keyword and its value. The operator field must be one of the following:  =Equal  !=Not equal  >Greater than  <Less than
Operator	=Greater or Equal  <=Less or Equal  =>Generic
value	Contains a entity that is appropriate for the keyword.

*NOTE: The OR operation can be implemented by successive ACCEPT rules. For example, to accept a packet if the source address is **xxx**, or the destination address is **yyy**, the following rules are used:*

*IP: 1 ACCEPT src-addr=xxx; 2 ACCEPT dst-addr=yyy;*

---

## Creating Filter Files

You can create filter files using any text editor. Once the file is created, use the Trivial File Transfer Protocol (TFTP) to place the filter file in the OfficeConnect Remote Dual Analog FLASH memory.

To create a filter file:

- 1 Open a new text file. Enter the file descriptor on the first line:  
**#filter**
- 2 Enter a file section header followed by a colon for the protocol rules you want to define. For example, if you want to define IP filtering rules, enter the following section header: IP:
- 3 You can comment a section header out by placing a # sign before the section header. This is useful if you want to insert a placeholder for a protocol section you will define in the future.
- 4 Enter the protocol rules for the protocol section you are defining. Observe the following guidelines.
- 5 Begin each rule with a unique line number (1 — 10).
- 6 Arrange rules in increasing order within each protocol section.
- 7 Arrange rules so that the rules you expect to be matched most frequently are toward the top of the list.
- 8 Delimit each rule with a semi-colon.

*IP 1 ACCEPT src-addr = 128.100.33.1; 2 ACCEPT dst-addr = 200.135.38.9;*

- 9 Continue to define protocol rules for each protocol section you want to filter.
- 10 Inspect the file to ensure that it meets all filtering rules.
- 11 This step is important since you cannot edit the filter file from within the CLI. To edit the file, you must modify it using a text editor, TFTP the modified file into the FLASH - replacing the original file - and verify the filter using the verify filter command.

- 12 Save the filter file using a .fil extension. The filter file extension will allow you to differentiate the filter file from other files stored in the OfficeConnect Remote Dual Analog FLASH memory.
- 13 You can use the list files command to ensure the filter file was successfully stored in the OfficeConnect Remote Dual Analog FLASH memory.
- 14 Configure a PC as a Trivial File Transfer Protocol (TFTP) client of the OfficeConnect Remote Dual Analog by entering the following command: add TFTP client <hostname or IP address>
- 15 From a machine that has access to the same network as the OfficeConnect Remote Dual Analog, use the following TFTP commands to transfer the filter file to the OfficeConnect Remote Dual Analog FLASH memory.

*tftp <OfficeConnect Remote Dual Analog IP address> put <filter filename>*

- 16 The OfficeConnect Remote Dual Analog does not recognize a filter file stored in its FLASH memory until you add it to the managed filter table. To notify the unit about the filter file for the first time, you must issue a CLI command. Use the following CLI command to add the filter to the managed filter table: **add filter <name>**.

*NOTE: See the CLI reference manual for instructions for connecting the console cable and communicating with the OfficeConnect Remote Dual Analog using a terminal emulator like Microsoft's HyperTerminal.*

*NOTE: If you are editing a filter file already stored in FLASH, you don't have to use the add filter command. Be sure it has been verified though.*

- 17 When the filter is added, the unit automatically verifies the filter file syntax. If the syntax is valid, no message is generated and the command prompt returns. If the syntax is not valid, error messages are generated detailing the source of the errors.

---

## **Configuring Filters**

Once a filter has been added to the OfficeConnect Remote Dual Analog's list of managed filters, you can assign it to the unit:

- Interfaces
- Users

### **Interface Filters**

You can configure interface filters for any OfficeConnect Remote Dual Analog interface. Interface filters control access to all networks available for both modem and non-modem interfaces.

You can specify whether a filter applies to packets entering the interface (input filter), leaving the interface (output filter), and packets that can initiate a call (call filter). The OfficeConnect Remote Dual Analog examines the filtering rules to determine whether the interface accepts or rejects the packet.

### **Input Filter**

If an input filter is configured on an interface, all received packets are checked against the filtering rules before being forwarded to another interface.

### **Output Filters**

If an output filter is configured on an interface, all outbound packets are checked against the filtering rules before exiting the OfficeConnect Remote Dual Analog.

### **Call Filters**

If a call filter is configured on an interface, all transmitted packets are checked against the filtering rules. The filtering rules determine whether the packet can initiate an outgoing call. Call filters are checked only after the packet has passed the output filter check. An interface without a call filter configured will allow all packets to initiate an outgoing call.

## **Input Filters vs. Output Filters**

When possible, use the input filter to filter an incoming packet rather than waiting to catch a packet as it attempts to exit the OfficeConnect Remote Dual Analog. This is recommended because:

- A packet is prevented from entering the OfficeConnect Remote Dual Analog, keeping potential intruders from attacking the unit itself.
- The OfficeConnect Remote Dual Analog routing engine does not waste time processing a packet that is going to be discarded anyway.
- Most importantly, the OfficeConnect Remote Dual Analog does not know which interface an outgoing packet came in through. If a potential intruder forges a packet with a false source address (in order to appear as a trusted host or network), there is no way for an output filter to tell if that packet came in through the wrong interface. An input filter, on the other hand, can filter out packets purporting to be from networks that are actually connected to a different interface.

## **Remote Site Filters**

You can configure remote site filters for a specific user that control access to the network for that user. This filter is only applied for the duration of the remote site's network connection. As with interface filters, a remote site filter can be configured as an input, output or call filter.

---

## **Assigning Filters**

You can assign filters to interfaces and/or users using the CLI.

### **Assigning a Filter on an Interface**

To configure an input or output filter on an interface, use the following CLI command:

```
set interface <interface_name> input_filter <filter_name>output_filter <filter_name>
```

For example, to apply an input filter to an interface: **set interface eth:1 input\_filter filter.fil**

## **Configuring a Filter for a User**

To configure an input or output filter for a specific user, use the following CLI command:

```
set user <user_name>input_filter <filter_name>output_filter <filter_name>
```

For example, to apply an output filter to a user: **set user frizzo input\_filter filter.fil**

---

## **Converting Filter Files for the HTML Manager**

If you have created filter files using the CLI Reference, you will need to modify the files slightly to make them compatible with the file format of filters created using the HTML Manager.

There are three steps to perform to achieve the file conversion:

- 1** Change the file name
- 2** Make minimal changes to the file content
- 3** Use the HTML Manager to complete the file update

### **Change the File Name**

The HTML Manager requires that there be a specific filter file for each direction/location pair to which filters can be applied (e.g. Ethernet - input filters, WAN - output filters). You will need to rename filter files according to the direction/location where the filter file is applied. If one filter file is applied to multiple direction/locations, then you need to copy the file for each direction/location and rename each copy. The names are provided in the Table 5.

**Table 5: Filter File Names**

<b>Location</b>	<b>Direction</b>	<b>New Filter File Name</b>
Ethernet Interface	Input	INETH.FLT
Ethernet Interface	Output	OUTETH.FLT
WAN Interface	Input	INWAN.FLT
WAN Interface	Output	OUTWAN.FLT
User / Remote Site	Input	INRS<name>.FLT where <name> is the user name (also called login name and remote site name)
User / Remote Site	Output	OUTRS <name>.FLT

### **Change the File Content**

If the file contains line numbers greater than 10, or if it contains the “deny” verb, it needs to be edited. Within each protocol section, the line numbers need to be reassigned numbers 1-10 except for the line number in front of a “deny”. It must be changed to “999”.

For example, filter file FF1 originally looked like this:

```
#filter
```

```
IP:
```

```
#10 and src-socket = 14;
```

```
20 and src-socket = 15;
```

```
30 accept dst-socket = 16;
```

```
40 deny;
```

IPX-SAP:

```
10 reject server = Server1;
```

You rename it to INETH.FLT and edit it as shown below:

```
#filter
```

```
IP:
```

```
#1 and src-socket = 14;
```

```
2 and src-socket = 15;
```

```
3 accept dst-socket = 16;
```

```
999 deny;
```

IPX-SAP:

```
1 reject server = Server1;
```

*NOTE: There is a case that is legal in the current filter implementation that is illegal in the new implementation. It is currently possible for the user to have a filter file containing a call filter that is assigned to a direction/location that is not output - user (remote site). Creating such a filter using the HTML Manager is possible only for output - user. The reason is that applying a call filter to any other direction/location is useless. Call filters apply only when a user profile is being used to make an outgoing call. Therefore, any filter file containing a call filter that is applied to an incorrect direction/location will be rejected. To prevent this, you should delete any call filter from filter files that you have renamed to INETH.FLT, OUTETH.FLT, INWAN.FLT, OUTWAN.FLT or INRS<name>.FLT.*

## **Complete the File Update**

When an old, renamed filter is read in by the HTML Manager, it will not contain new special comment lines. These lines are added when the filter file is written back out. The lines expand the filter definitions to allow you to name filters and to enable and disable filters and filter conditions individually.

*NOTE: There is a change in the way the term “filter” is used here. Using CLI, the term was used to describe an entire filter file. Now the term describes a single action within the filter file. This means that a filter file may contain multiple filters, for example, one to block a specified IP address and another to block on a specified MAC address.*

Since these lines are not present in the old file, a few assumptions are made when an old file is first read in:

- Each protocol section in the filter file will be displayed as a separate filter in the HTML Manager screen.
- The filter names will be assigned simply as Filter #1, Filter #2, etc.
- All filters are enabled.
- All conditions are enabled.
- Any condition that is commented out using the conventional comment character ('#') will not be read in and will be lost.

To complete the file update, do the following in the HTML Manager screens:

- On the Filters Screen (the first screen), select the appropriate direction/location (e.g. “coming from the Ethernet Interface”) to bring up the Filter Summary screen shown on the following page.

Filter Summary

**Filter For Packets** Coming From the Ethernet Interface

Filter Name	Protocol	Filter Enabled	Condition Enabled	Action	Keyword	Operator	Value
Filter 1	IP	Yes	Yes Yes	Accept Packets if And	Source Socket Destination Socket	is Equal to is Equal to	15 16
Filter 2	IPX-SAP	Yes	Yes	Remove Entry if	Source Name	is Equal to	Source 1

Add

Modify   Delete   Filter: Filter 1 ▾

- Press the **Modify** button.
- On the Modify screen, press the **Finish Filter** button. This will cause the filter file to be written as shown below.

#filter

IP:

[FN = Filter1 | FI = 1 | Enabled = yes]

{ CI = 1 | Enabled = yes }

2 and src-socket = 15;

{ CI = 2 | Enabled = yes }

3 accept dst-socket = 16;

999 deny;

IPX-SAP:

[FN = Filter2 | FI = 2 | Enabled = yes]

{CI = 1 | Enabled = yes}

1 reject server = Server1;

---

## Setting Filter Access

When filters are assigned to both the interface and the user, you need to tell the OfficeConnect Remote Dual Analog which one to use using the filter access parameter. If filter access is ON, the user filters will override interface filters. If filter access is OFF, then the interface filters are used.

To set the filter access parameter to **ON** for a specific interface, use the following command:

```
set interface <interface_name> filter_access ON
```

To set the filter access parameter to **OFF** for a specific interface, use the following command:

```
set interface <interface_name> filter_access OFF
```

---

## Managing Filters

This section provides information about how to perform filter management tasks.

### Displaying the Managed Filter List

To display the list of managed filters, use the following command: **list filters** <filter\_name>

The resulting display might look like this:

Filter Name	Status	Protocols
filter.fil	NORMAL	IP IP-RIP

## Adding Filters to the Managed List

The **add filter** command verifies filter syntax prior to adding the filter to the managed list. If the syntax is valid, no message is generated and the command prompt returns. If syntax errors exist, error messages are generated detailing the cause of the errors.

If the syntax is invalid, the filter is still added to the managed list with a status of *verify failed*. To correct filter file errors, you must make the changes to the original filter file using a text editor, and re-TFTP the file to the OfficeConnect Remote Dual Analog FLASH memory.

Then use the **verify filter** command to check the filter file syntax.

To add a filter file to the list of managed filters, use the following command: **add filter** <filter\_name>

It may be helpful to use the **list files** command to see files successfully stored in the OfficeConnect Remote Dual Analog FLASH memory.

## Removing a Filter from an Interface

To remove a filter that is assigned to an interface, use the following command:

```
set interface <interface_name> input_filter ""output_filter ""
```

The "" value represents a null value and removes the defined filter from the interface. For example, to remove an output filter from an interface named eth:1, you would use the following command: **set interface eth:1 output\_filter ""**

## Removing a Filter from a Remote Site

To remove a filter that is assigned to a remote site profile, use the following command:

```
set user <user_name> input_filter ""output_filter ""
```

The "" value represents a null value and removes the defined filter from the user profile. For example, to remove an input filter from a remote site profile named **john\_d**, you would use the following command: **set user john\_d input\_filter ""**

## Deleting a Packet Filter

To delete a specific packet filter, removing the filter file permanently from the OfficeConnect Remote Dual AnalogOfficeConnect Remote Dual Analog FLASH memory, use the following command: **delete filter <filter\_name>**

## Verifying Filter File Syntax

The verify filter command *must* be used if you make changes to a filter file that has already been added to the managed list and re-TFTP it back to the OfficeConnect Remote Dual Analog FLASH memory (using the same filename). The verify filter file will check the filter syntax. If the syntax is valid, no message is generated and the command prompt returns. If the syntax is not valid, error messages are generated detailing the source of the errors.

To verify a filter file, use the following command: **verify filter <filter\_name>**

## Showing Filter File Contents

To view the contents of an entire filter file that has been added to the managed list of filters, use this command: **show filter <filter\_name>**

To display the contents of the filter file by protocol, use this command:

**show filter <filter\_name> protocol** BR-ETH | BR-ETH-CALL | IP | IP-CALL | IP-RIP | IPX | IPX-CALL | IPX-RIP | IPX-SAP

## Source and Destination Address Filtering

Source and destination address filtering is generally used to limit permitted access to trusted hosts and networks only, to explicitly deny access to hosts and networks that are not trusted, or to limit external access to a given host (for example, a Web server or a firewall).

Note that only the part of the IP address specified by the *mask* field is used in the comparison. If a match is found, the packet is forwarded (rules containing *accept*) or discarded (rules containing *reject*).

The following rule example allows forwarding of IP packets with source addresses that match the first 16 bits of the given IP address (that is, addresses beginning with 192.77):

**IP:1 ACCEPT src-addr = 192.77.200.203/16;**

The following rule example prevents forwarding of IP packets with destination addresses that match the first 16 bits of the given IP address (that is, addresses beginning with 188.39):

**IP:1 REJECT dst-addr = 188.39.150.166/16;**

The following rule example allows forwarding of IP packets with source address **192.77.100.32** and destination address **201.128.11.34**:

**IP: 1 AND src-addr = 192.77.100.32;020 ACCEPT dst-addr = 201.128.11.34;**

---

## **IP Filters**

### **IP RIP Packet Filtering**

Routing Information Protocol (RIP) packets are used to identify all attached networks as well as the number of router hops required to reach them. The responses are used to update a router's routing table

If the OfficeConnect Remote Dual Analog is listening for or broadcasting RIP messages, you should allow them to pass in the appropriate direction(s). You define IP RIP filtering rules in the IP-RIP protocol section of the filter file.

For example, if you want to filter all routes except the one specified by the IP network address **195.12.254.45**, you would create this rule: **IP-RIP: 1 ACCEPT network = 195.12.254.45;**

This filter only allows the route **195.12.254.45** into the route table. All other routes are rejected.

*NOTE: Spurious RIP messages can disrupt your routing tables. If you are listening for RIP messages on a given interface, you may wish to consider filtering out RIP updates from untrusted networks.*

### **IP Call Filtering**

You define IP call filtering rules in the IP-CALL protocol section of the filter file. Like the rules defined in the IP protocol section, the IP-CALL filtering rules compare the source or destination network address, host address and port number defined in the IP-CALL filter rules.

---

## **IPX Filters**

### **Source and Destination Network Filtering**

IPX network numbers must be specified as an network number no greater than 8-digits in hexadecimal format. The following rule example rejects IPX packets with a source address: 00-03-42-BF.

**IPX: 1 REJECT src-net = 00-03-42-BF;**

### **Source and Destination Host Filtering**

Host addresses must consist of the 8-digit network number, followed by the four digit node number in hexadecimal format.

The following rule example accepts IPX packets with a destination address of 04-0B-43-AA:

**IPX: 1 ACCEPT dest-host = 04-0B-43-AA;**

### **Source and Destination Socket Number Filtering**

Sockets numbers represent communications interfaces that let an application access a network protocol by "opening a socket" and declaring a destination. Sockets are useful because they provide a simple way to direct an application onto the network (TCP/IP protocol).

You can compare the source or destination IPX socket number contained in the packet to the socket number defined in the filter rules. You must specify the type of the comparison.

For example, the following rule example accepts IPX packets with the IPX source socket number 0x001: **IPX: 1 ACCEPT src-socket = 0x001;**

### **IPX RIP Packet Filtering**

Routing Information Protocol (RIP) packets are used to identify all attached networks as well as the number of router hops required to reach them. The responses are used to update a router's routing table.

You define IPX RIP packet filtering rules in the IPX-RIP protocol section of the filter file. You can filter IPX RIP packets by network only.

The following rule example filters the route specified by the IPX network address 00-03-55-BF:

**IPX-RIP: 1 REJECT network = 00-03-55-BF;**

### **IPX SAP Packet Filtering**

SAP packets are used to identify the services and addresses of servers attached to the network. The responses are used to update a table in the router known as the Server Information Table.

You define IPX SAP packet filtering rules in the IPX-SAP protocol section of the filter file. You can filter SAP packets by network, node, server, service-type, and socket.

The following rule example accepts SAP services from the server name sales\_1, with a socket number is less than 32: **IPX-SAP: 1 AND server = sales\_1; 2 ACCEPT socket < 32;**

### **IPX Call Filtering**

You define IPX call filtering rules in the IPX-CALL protocol section of the filter file. Like the rules defined in the IPX protocol section, the IP-CALL filtering rules compare the source or destination network address, host address and socket number of an IPX packet the rules defined in the IPX-CALL filter rules.

---

## **Using Filters to Approximate Spoofing**

Filters are best employed to curtail unneeded network traffic and establish network security, but they can also be used to approximate spoofing when routers with different or incompatible spoofing methods are linked over the WAN. A unit to unit connection supports spoofing, rendering filtering unnecessary for this purpose.

If you decide to use the following sample filter to accomplish spoofing over the WAN, be aware of the following:

- Spoofing is preferred over call filters when both ends are 3Com products. This is the best solution.
- IP and IPX static routes must be configured on both routers when filtering IP-RIP and IPX-RIP packets.
- Static IPX services must be configured on both routers when filtering IPX SAP packets.

---

## Sample Filter

The following sample filter is loaded on the floppy diskette included in your unit's package as well as in the OfficeConnect Remote Dual Analog FLASH file.

#filter

# OVERVIEW: #

# The rules in this filter file are setup to prevent calls  
# from being initiated as a result of periodic advertisement  
# packets such as RIP and SAP. Be sure to configure static  
# routes and service when filtering RIP and SAP packets. This  
# filter should be applied as an output filter on the WAN port# to prevent such calls.

IP-CALL: # This rule prevents RIP packets from initiating a call. 1 reject udp-dst-port = 520;

IPX-CALL: # This rule prevents RIP packets from initiating a call. 1 reject dst-socket = 0x0453; #  
This rule prevents SAP packets from initiating a call. 2 reject dst-socket =  
0x0452; Filtering Filtering