Novell NetWare® 6

www.novell.com

FILTER CONFIGURATION

Novell®

Legal Notices

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

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

U.S. Patent No. 5,157,663; 5,349,642; 5,455,932; 5,553,139; 5,553,143; 5,572,528; 5,594,863; 5,608,903; 5,633,931; 5,652,859; 5,671,414; 5,677,851; 5,692,129; 5,701,459; 5,717,912; 5,758,069; 5,758,344; 5,781,724; 5,781,724; 5,781,733; 5,784,560; 5,787,439; 5,818,936; 5,828,882; 5,832,274; 5,832,275; 5,832,483; 5,832,487; 5,850,565; 5,859,978; 5,870,561; 5,870,739; 5,873,079; 5,878,415; 5,878,434; 5,884,304; 5,893,116; 5,893,118; 5,903,650; 5,903,720; 5,905,860; 5,910,803; 5,913,025; 5,913,209; 5,915,253; 5,925,108; 5,933,503; 5,933,826; 5,946,002; 5,946,467; 5,950,198; 5,956,718; 5,956,745; 5,964,872; 5,974,474; 5,983,223; 5,983,234; 5,987,471; 5,991,771; 5,991,810; 6,002,398; 6,014,667; 6,015,132; 6,016,499; 6,029,247; 6,047,289; 6,052,724; 6,061,743; 6,065,017; 6,094,672; 6,098,090; 6,105,062; 6,105,132; 6,115,039; 6,119,122; 6,144,959; 6,151,688; 6,157,925; 6,167,393; 6,173,289; 6,192,365; 6,216,123; 6,219,652; 6,229,809. Patents Pending.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Filter Configuration
October 2001
103-000178-001

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

Third-Party Trademarks

Contents

About This Guide

This guide provides the information you need to configure and manage Novell® Internet Access Server 4.1 filters.

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

Also, a trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

1 Understanding

This chapter describes the Filter Configuration utility (FILTCFG) that you use to configure filters that selectively discard packets to be sent or received by a router. Filters let you control the service and route information that is accepted or advertised by a router.

Filters can be useful when you want to limit specific kinds of traffic to certain parts of your network topology, or when you want to provide a certain level of security.

The Use of Filters

The Novell® Internet Access Server 4.1 routing software supports filtering to control the service and route information that is accepted or advertised by a router. Filters are useful when you want to limit specific types of traffic to certain parts of your network and when you want to provide a certain level of security. You use FILTCFG to configure the filters for the Internetwork Packet Exchange™ (IPX™) protocol, IP, AppleTalk*, and the source route bridge to selectively discard packets sent or received by a router. The following types of filters are supported:

- *Packet forwarding* —Prevents selected data packets from being forwarded by the router. Packet forwarding filtering is available for IPX and TCP/IP.
- *Service information* —Limits the services added to the service information (SAP) tables of specified routers. Service information filtering is available for IPX and AppleTalk.
- *Routing information* —Limits the routes added to the routing tables of specified routers. Routing information (RIP) filtering is available for IPX, AppleTalk, and TCP/IP.

- *OSPF* —Controls the propagation of routing information from non-OSPF domains (RIP, EGP, and so on) to the OSPF domain.
- *EGP* —Defines the routes that a router can share with other EGP peers.
- *Protocol ID and ring number* —Filters packets of certain protocol types received by the bridge (Protocol ID filter), and filters packets received from specific rings on a token ring network (ring number filter). Both types of filters are only available for source route bridge.

Table 1 lists the protocol suites and the filter types that you can configure for each with FILTCFG.

Table 1 Filter Types and Protocol Suites

Protocol Suite	Packet Forwarding Filters	Service Filters	Route Filters	Bridge Filters
IPX	X	X	X	
AppleTalk		X	X	
TCP/IP	X		X	
Bridging				X

Packet Forwarding Filters

Packet forwarding filters limit access to specific services by preventing selected data packets from being forwarded by the router. These filters provide the highest level of security because they examine each data packet forwarded by the router. The filtering is based on the following packet characteristics:

- Source interface
- Destination interface
- Source address
- Destination address
- Content

Packet forwarding filters do not restrict service advertisement packets sent by servers. Therefore, restricted users might see advertisements of services even when they cannot access the service.

Although packet forwarding filters provide the highest level of security, they might affect the performance of the router because the filters are applied to each data packet received by the router.

Packet forwarding filters are available for IPX and TCP/IP protocols.

Service Information Filters

Service information filters restrict the advertisement or acceptance of specified services by filtering out information in the data packets that advertise the services destined for particular parts of the network. These filters increase security by limiting the visibility of selected services. However, service information filters provide a lower level of network security than packet forwarding filters because they only monitor service information packets. They also reduce the network traffic caused by periodic service information messages sent by routers.

Service information filters are available for IPX (as outgoing and incoming SAP filters) and AppleTalk (as device hiding filters).

Routing Information Filters

Routing information filters restrict the exchange of routing information between routers by limiting the routes added to the routing tables of specified routers. These filters increase network security by limiting the visibility of specified networks. However, like service information filters, routing information filters provide a low level of network security because they only monitor routing information packets. They also reduce the network traffic caused by the periodic exchange of routing information messages between routers.

Routing information filters are available for IPX, AppleTalk, and TCP/IP.

There are two types of routing information filters:

- Outgoing routing information filters, which limit the route advertisements sent out by a router to a specified set of routers
- Incoming routing information filters, which limit the acceptance of route advertisements received by the router from its neighboring routers

For more information about routing information filters, refer to

- "Outgoing Routing Information Filters" on page 12
- "Incoming Routing Information Filters" on page 13

Outgoing Routing Information Filters

Outgoing routing information filters limit routing information advertised by a router to its neighboring routers. When these filters are enabled on a router, only the allowed routes are advertised to each neighboring router. This hides specified routes from some routers and from certain parts of the network.

A typical outgoing routing information filter consists of the route to the destination network and the interface through which filtered advertisements of the route are sent. The filters affect all routers on the network to which this interface connects.

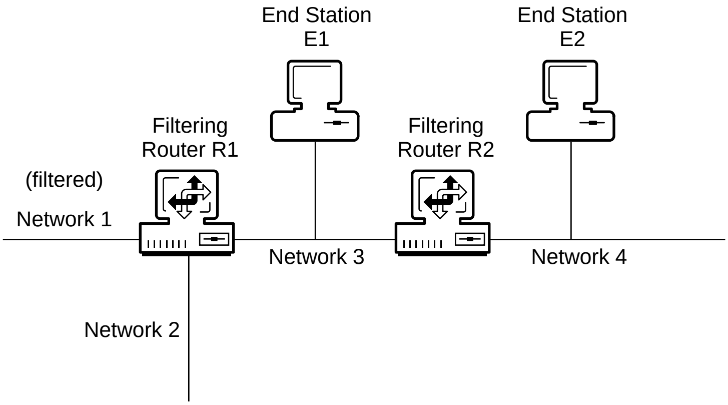
Outgoing routing information filters might not affect whether the end stations that are on the same LAN segment as the filtering router can access the filtered routes. Because these filters only keep from advertising filtered routes to other routers but do not affect the filtering router's routing table, the filtering router delivers all packets that it receives as destined for filtered routes.

End stations at least one router away usually cannot access networks with routes that are filtered out.

In addition to being able to filter by interface, you can also filter on a WAN circuit. You can assign filters with specific circuit information, including remote system ID, remote DTE address, and DLCI number. If the specific router is connected by the specified circuit information in the filter, then the filter is applied. Filtering on circuits is supported for X.25, ATM, frame relay, and PPP.

Figure 1 on page 13 shows two networks; the route for one network has been filtered.

Figure 1 Outgoing RIP Filters



The route to Network 1 is filtered out in Router R1's advertisement to Network 3. If End Station E2 sends a packet to Network 1, Router R2 drops that packet because it does not have a route. If End Station E1 sends a packet to Network 1, Router R1 forwards it because it does have a route. End Station E1 can send a packet to Network 1 only if it has a route to that network. End station E2 can see only Networks 2, 3, and 4. End station E1 can see both Networks 1 and 2.

When IPX is used, route information filters affect both clients and routers. A client will make a route request that passes through the same filters as for the routinely transmitted route information. However, if a client is attached locally to a router that is performing outbound route information filtering and the client is using software that can use static routing, the client can send packets to Network 1 through Router R1 because R1 knows about Network 1 in its routing tables. If only standard IPX route lookups are done (true for a majority of sites), a path to the filtered networks is not possible.

Incoming Routing Information Filters

Incoming routing information filters limit the routing information accepted by a router from its neighboring routers.

When incoming routing information filters are enabled on a router, the router accepts only the allowed routes from each neighboring router, thereby hiding specified routes from some routers and from certain parts of the network. However, incoming routing information filters cannot be used to filter out directly connected networks.

A typical incoming routing information filter consists of the destination network of the route and the interface through which advertisements of the route are expected to be received.

Incoming routing information filters keep the filtering router from adding certain routes to its routing table when it receives the information from its neighbors. The filtering router cannot forward a packet to a filtered route even if it receives a packet destined for it. In this way, incoming routing information filters provide a higher level of security than that provided by outgoing routing information filters.

IPX Filtering

IPX supports the following types of filters:

- Outgoing SAP filters
- Incoming SAP filters
- Outgoing RIP filters
- Incoming RIP filters
- NetBIOS filters

For more information about IPX filtering, refer to

- "IPX SAP Filters" on page 14
- "IPX RIP Filters" on page 15
- "IPX NetBIOS and Packet Forwarding Filters" on page 16

IPX SAP Filters

Servers and routers on an IPX network exchange information about the name, type, and location of the various service providers on the internetwork by way of SAP packets. This information is distributed to users through SAP packets. By limiting the propagation of this information, SAP filters provide limited security at the servers and reduce the bandwidth required by the SAP exchanges.

There are two types of service information filters:

- Outgoing SAP filters (service advertisement filters)

  Outgoing SAP filters restrict the propagation of the SAP information that is known to the router. An outgoing SAP filter specifies the service provider and the potential recipient of the information. The service provider is defined by a service name and service type. The recipient is defined as an outbound interface or interface group. The filter is applied to all servers, users, and routers that would receive the SAP information through the interface. In large NetWare® internetworks, outbound SAP filtering can save valuable WAN bandwidth, although the NetWare Link Services Protocol™ (NLSP™) protocol might offer greater bandwidth savings.

- Incoming SAP filters (service acceptance filters)

  Incoming SAP filters let the router discard information about a particular service provider. The filtered SAP information is not recorded in the local SAP information table or propagated to other routers or servers. The SAP filter includes the service name and service type. An incoming SAP filter can also specify the source of the SAP information to be filtered. The source identifies the interface from which the SAP information was received.

  NOTE: SAP filters work only on routers running the RIP and SAP protocols. They do not work on routers running the NLSP protocol. For filtering to work, either IPXRTR must be configured for RIP/SAP only, or the bind options on selected interfaces must be set up to read RIP=Yes , SAP=Yes , and NLSP=No .

IPX RIP Filters

Routers on an IPX network exchange routing information through RIP packets. By limiting the propagation of this information, RIP filters provide limited security to IPX networks, reduce the bandwidth required for RIP updates, and reduce the memory requirements for routing tables.

There are two types of IPX RIP filters:

- Outgoing RIP filters

  Outgoing RIP filters restrict the propagation of routing information by the router. An outgoing RIP filter specifies the network to be filtered and the interface or interface group to which the filter should be applied. The filter is applied to all servers, users, and routers that receive the RIP information through that interface or interface group.

- Incoming RIP filters

  Incoming RIP filters let the router discard information about a particular network. The filtered network is not recorded in the local forwarding table and cannot be propagated to other routers, servers, or users. The filter includes the network and the source of the route. The source identifies the interface or interface group from which the routing information was received. This is the most effective route filter for improving security.

  WARNING: RIP filters work only on routers running the RIP protocol. They do not work for routers running the NLSP protocol. Use RIP filters with care because they can partition a physical network into two or more segments.

IPX NetBIOS and Packet Forwarding Filters

NetBIOS filters allow the router to forward NetBIOS broadcast packets only on selected interfaces.

IPX packet forwarding filters allow the router to filter a packet based on the source and destination interface fields, the packet type, and the source and destination address type. The interface can be specified as an interface or interface type, and address types can be specified as any address, network, or node. Some services can be identified by the presence of expected values in the Packet Type and/or Destination Socket fields.

NOTE: IPX NetBIOS and packet forwarding filters work while using either NLSP or RIP/SAP routing modes.

TCP/IP Filtering

The TCP/IP protocol supports the following types of filters:

- IP outgoing route filters
- IP incoming route filters
- Outgoing EGP filters
- Incoming EGP filters
- OSPF external route filters
- Packet forwarding filters

For more information about TCP/IP filtering, refer to

- "IP Routing Information Filters" on page 17
- "IP Packet Forwarding Filters" on page 18

IP Routing Information Filters

IP routing information filters let the router restrict the routes that it accepts from neighbors (incoming filters) and limit the advertised routes (outgoing filters). The router can use RIP, Open Shortest Path First (OSPF), or Exterior Gateway Protocol (EGP) to exchange routing information with other neighboring routers, as follows:

- RIP filters control the propagation of routing information and hide the existence of specific IP networks from other routers.
- OSPF filters control the propagation of routing information from non-OSPF domains (RIP, EGP, and so on) to the OSPF domain.
- EGP filters define the routes a router can share with other EGP peers.

IP Incoming Filters

IP incoming filters let the router restrict information about the routes it accepts from its neighbors. Filtered routes are not recorded in the local forwarding table and cannot be propagated to other routers or hosts. The filter includes the destination network and the source of the route. The source identifies the interface, interface group, or WAN connection from which the route information was received or the address of the router that provided the information.

You can apply IP incoming filters only to RIP and EGP routes. You cannot filter routes to directly connected networks. Incoming filters do the following:

- RIP incoming filters restrict the acceptance of routing information from other RIP routers.
- EGP incoming filters restrict the routes accepted from the EGP peers.

IP Outgoing Filters

IP outgoing filters restrict the propagation of route information from the router. You can also use them to control the flow of routes between the routing protocols. An outgoing filter specifies a route and a potential recipient of the information. The recipient is an outbound interface, an interface group, a WAN connection, or the IP address of another router.

You can apply IP outgoing filters to RIP, EGP, and OSPF routes. You cannot filter directly connected networks. The following outgoing IP filters are available:

- RIP outgoing filters restrict the advertising of routing information and hide the existence of specific IP networks from other routers.
- OSPF external route filters define the routes learned from RIP, EGP, or static routes that are propagated into the OSPF domain.
- EGP outgoing filters restrict the routes that are propagated to the EGP peers.

IP Packet Forwarding Filters

IP packet forwarding filters let the router filter packets selectively, based on their source and destination interface fields, the packet type, and the source and destination address type. The interface can be specified as an interface or interface type, and the address types can be specified as any address, network, or host. The packet type is identified by the presence of expected values in the protocol type field of the IP header and in a protocol-specific operator. Packet forwarding filters recognize the following protocol types:

- Internet Control Message Protocol (ICMP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- NetWare Core Protocol (NCP)

The packet type can be further identified by the TCP/UDP port. You can filter only TCP packets that initiate a connection; therefore, you can restrict access to TCP services in a specific location while allowing clients in that location to access outside TCP services.

AppleTalk Filtering

The AppleTalk protocol supports the following types of filters:

- Device hiding filters
- Routing information filters

For more information about AppleTalk filtering, refer to

- "AppleTalk Device Hiding Filters" on page 19
- "AppleTalk Routing Information Filters" on page 20
- "AppleTalk Routing Information Filters over AURP" on page 23

AppleTalk Device Hiding Filters

AppleTalk device hiding filters restrict the advertisement of services on a router's internetwork by filtering out packets that advertise those services. These filters both prevent users from finding the network addresses of services and provide a level of network security.

In AppleTalk, the Name Binding Protocol (NBP) lets users access services such as file servers and printers. Specifically, it allows a user or application to specify search parameters such as the network entity name and service type, and a zone in which the search should be done. The search is represented in an NBP lookup request sent to the appropriate zone where the service might be. Services matching the search parameters reply directly to the requesting user or application with the AppleTalk address of the service. Once the user or application has received the NBP reply, the user or application can use the AppleTalk address to communicate with the service.

When AppleTalk device hiding filters are enabled on a router, the router drops the NBP replies for specified services. (That is, it does not deliver the replies to the client machine or application that requested them.) Thus, the services are hidden from that part of the network.

A common use of NBP is the Macintosh* Chooser application. The user or application issues an NBP lookup, specifying a zone and service type of interest. The lookup is sent to the appropriate zone. All devices or services of the specified type in the zone respond with an NBP reply. The Chooser displays the list of available devices, based on the NBP replies it receives. Using the AppleTalk address supplied in each NBP reply, the user or application can then communicate with the device or service.

If filtering for that device or service location is enabled, the router drops the NBP reply so that a user or application cannot get the network address of these services. Without the NBP reply, the application cannot know about the existence of the device.

NOTE: Device hiding filters provide a low level of security, but they do have limitations. Because filtering is enabled on a router, if the client machine requesting the address is on the same network as the service, the NBP reply goes directly to the client and the router has no opportunity to filter it out. Additionally, if a client machine knows the address of a specific service, it does not need the NBP reply to access the service.

You can configure AURP routers to filter service information traveling through an IP tunnel. If a filter is enabled on the tunnel, all networks accessible through the tunnel are affected by service information filters configured for the AURP router.

AppleTalk Routing Information Filters

AppleTalk routing information filters restrict the exchange of routing information between routers by limiting the routes added to the routing tables of specified routers. These filters increase security by limiting the visibility of selected networks or zones and reduce the network bandwidth consumed by the periodic exchange of routing information between routers. There are two types of AppleTalk routing information filters:

- Outgoing route filters
- Incoming route filters

AppleTalk uses Routing Table Maintenance Protocol (RTMP) as its primary routing protocol. This protocol is similar to the RIP used by TCP/IP and IPX. The routing tables maintained by RTMP contain an entry for every known route. These routing tables acquire routing information in two ways:

- For directly connected networks, through AppleTalk configuration
- For networks not directly connected, through the routing updates from each of a router's neighboring routers

When all routing information filters are not enabled, an AppleTalk router learns all the routes known by its neighboring routers through periodic routing table updates (sent by RTMP). In this way, every router on the internetwork acquires the routing information from all other routers on the internetwork.

Routing information filters are also available over AppleTalk Update-based Routing Protocol (AURP). In this case, a neighboring router can be either a network interface (all neighbors directly connected to the cable) or all peers on the AURP tunnel.

AppleTalk outgoing route filters can be used for networks and zones. Incoming route filters can be used only for networks.

NOTE: If AppleTalk networks have more than one router between them (such as for redundant or loop routing), these routers are required to have the same filters configured (device hiding, outgoing router, or incoming route filters). Configuring filters in only one router does not filter out the required information.

For more information on AppleTalk routing information filters, refer to

- "AppleTalk Outgoing Route Filters" on page 21
- "AppleTalk Incoming Route Filters" on page 22

AppleTalk Outgoing Route Filters

AppleTalk outgoing route filters limit the routing information advertised by a router to its neighbors. A typical outgoing route filter consists of a network or zone (the route) and the interface through which filtered advertisements are sent. The filters affect all routers on the network to which the interface connects.

An AppleTalk router learns only about networks that are not directly connected through its neighbors. Because of this, neighboring routers with enabled outgoing route filtering can limit the routing information that the AppleTalk router receives. This effectively cuts off access from one part of the network to another.

NOTE: If you hide a route from a neighbor, none of the routers on the neighbor's side of the network has any information about this route.

If the specified action is to deny routes in the filter list, the router ignores all the route information in the filters going to the designated neighbors, but sends all other routing information. If the specified action is to permit routes in the filter list, the router uses only routes designated in the filter list to the specific neighbors and ignores everything else.

Novell Internet Access Server 4.1 supports zone-based and network number-based outgoing route filters, as discussed in the following sections.

Zone-Based Outgoing Route Filters

Zone-based outgoing route filters limit the advertisement of all routes associated with a particular zone. A zone is an abstraction of networks into which many physical networks, including noncontiguous networks, can be grouped. The main advantage of using zone names in filters is that the filter does not need to be modified when new networks are added to the zone.

For example, when filters are configured for the Marketing zone, the zone is made up of only one physical network. As the department grows, more physical networks are added, but they are still grouped under the Marketing zone. All filters configured for the Marketing zone are enforced automatically for all new physical networks added to the zone. This capability greatly simplifies network management.

NOTE: When you specify a zone from a network that has multiple zones, all set filters affect the entire network, not just the selected zone.

Network Number-Based Outgoing Route Filters

Network number-based outgoing route filters limit the advertisement of the routes to specific networks. This kind of filtering gives very explicit control to the user about which physical network should or should not be advertised to different neighbors.

You must reconfigure network number-based outgoing route filters when changes occur in the network topology.

AppleTalk Incoming Route Filters

AppleTalk incoming route filters limit the routing information that a router accepts and adds to its routing tables.

When these filters are enabled on a router, the router accepts only the allowed routes from each of its neighboring routers so that specified routes are hidden from particular routers and from particular parts of the network. Novell Internet Access Server 4.1 supports only network number-based incoming route filters.

An incoming route filter consists of a route and the interface through which the route advertisements are expected to be transmitted. The specified route can be to a nonextended network or to an extended network.

Directly connected networks cannot be filtered by incoming route filters. If the specified action is to deny routes in the filter list, the router ignores all the route information designated in the filters received from the specified neighbors, but accepts and records all other routing information. If the specified action is to permit routes in the filter list, the router accepts only routes designated in the filter list from the named neighbors and ignores everything else.

AppleTalk Routing Information Filters over AURP

Routing information filters configured for AURP routers affect all AURP routers on the tunnel in the same way. AppleTalk routers running AURP cannot filter routes on a per-router basis.

WARNING: You should not change AURP route filters dynamically unless it is absolutely required. Because AURP routers exchange complete route information only during connection setup and only send updates to the information thereafter, changing route filters can cause large volumes of AURP routing information to be exchanged as the routers adapt to the new filter configuration. During this information exchange, connectivity over the tunnel can be affected.

Source Route Bridge Filtering

Source route bridge supports the following two types of filters:

- Protocol ID filters
- Ring number filters

Protocol ID Filters

Protocol ID filters filter out packets of certain protocol types received by the source route bridge. Protocol ID filtering can help control traffic, balance bridge loads, and increase security.

Ring Number Filters

Ring number filters filter out packets received from specific rings in a token ring network. This lets you limit the traffic that crosses a bridge from a source. Use ring number filters to balance the load among your network bridges and to increase network security.

2 Planning

This chapter explains the decisions you must make before you can configure filters.

Configuration Decisions

How you configure filters depends on the following decisions:

- Whether you want to control access to services on your network

  You should enable filtering support if you want to control access to services on your network. Filters increase security by limiting the visibility of selected services. Packet forwarding filters provide the highest level of security.

- Whether you want to reduce the bandwidth consumed by unnecessary routing traffic

  Enabling filtering reduces network traffic caused by periodic service information messages sent by routers.

3 Setting Up

You use the Filter Configuration utility (FILTCFG) to configure filters that selectively control which packets will be sent or received by a router. Filters let you control the service and route information that is accepted or advertised by a router.

Filters can be useful when you want to limit specific kinds of traffic to certain parts of your network topology, or when you want to provide a certain level of security.

How to Run FILTCFG

Before you begin, make sure that the Filter Support option is enabled in the Novell® Internet Access Server Configuration utility (NIASCFG) for each protocol that needs filtering.

NOTE: When Filter Support is disabled, the protocol operates as if the filter module is not loaded, and no filtering occurs. However, the changes you make will have no effect until you enable Filter Support. When Filter Support is enabled, any changes you make to the filter configurations take effect immediately. It is not necessary to use the REINITIALIZE SYSTEM command.

To set up and modify filters, complete the following steps:

1. Load FILTCFG.

   The Filter Configuration Available Options menu is displayed.

2. Select the protocol for which you want to configure filters.

   The main filter menu for the protocol you selected is displayed.

3. Optionally, for IPX and IP filtering, select Global Logging and select Enabled to log packets that match the Filters or Exceptions definitions.

The header of packets that match the Filters or Exceptions definitions are logged as long as the global logging status and the filters or exceptions logging status are both enabled. The logs are viewed using the NetWare Administrator utility.

4 Select the type of filter you want.

The corresponding option menu is displayed.

5 For each option you select, you can configure the following general parameters:

- Status —Specifies the status of the selected filters. Any configured filters immediately become active (enabled) or inactive (disabled), depending on your choice.
- Action —Permits or denies the packet, route, or service listed in the filter list.

  When the action is permitted, the specified filters are accepted; any filters that are not explicitly permitted are denied. One of the following occurs:

  Packets matching the entries in the Packet Forwarding List are allowed through.

  Services or routes matching the entries in the Outgoing Service/ Routing Information Filter Lists are advertised.

  Services or routes matching the entries in the Incoming Service/ Routing Information Filter Lists are accepted.

  If the action is denied, the specified filters are denied (the packets are discarded); any filters that are not explicitly denied are permitted.
- Filters —Displays a list of filters that are accepted (permitted) or filtered (denied) on an interface.

  You can select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new filter.

  Refer to the corresponding section later in this section for the steps you use to define a filter if you are modifying or adding a filter.
- Exceptions —Displays a list of exceptions to the Filters list, to which the Action parameter setting—permit or deny—*does not* apply.

  The Exceptions list is examined before the Filters list. If there is a conflict between the two lists, the Exceptions list is used. The action taken on the Exceptions list is always the opposite of the action taken on the Filters list.

You select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new filter. For example, you could use a filter to hide all Marketing file servers from Engineering, except the server named MKTG-DEMO.

6 Press Esc to exit.

NOTE: All filters affecting a primary call are automatically mapped to a configured backup call. Optionally, the automatic mapping of filtering can be disabled with the LOAD FILTSRV NOBACKUP command. With automatic mapping of filtering disabled, you can configure a selective filtering scheme that is specific to the needs of a backup link. The primary call and its associated backup call should use the same remote system ID. For information on configuring backup calls, refer to "Configuring Backup Calls."

How to Save Filters to a Text File

To save your filter information to a text file, complete the following steps:

1. Load FILTCFG.

   The Filter Configuration Available Options menu is displayed.

2. Select Save Filters to a Text File, then press Enter.

3. Enter the pathname for the filter file.

   For example, enter `SYS:\ETC\TEMP` . You can also save the filter file to a floppy disk (for example, A:\filename).

Configuring IPX Filters

The Internetwork Packet Exchange™ (IPX™) protocol supports the following types of filters:

- SAP (service information) filters
    - Outgoing SAP filters (services advertised)
    - Incoming SAP filters (services accepted)
- RIP (routing information) filters
    - Outgoing RIP filters (routes advertised)
    - Incoming RIP filters (routes accepted)
- NetBIOS and packet forwarding filters

Refer to Understanding for more information.

NOTE: When you configure a filter for a primary WAN call, an equivalent filter is automatically generated for the backup call. If the primary call should fail, the backup call is automatically connected.

This topic contains the following sections:

- "How to Configure IPX SAP Filters" on page 30
- "IPX SAP Filter Example" on page 33
- "How to Configure IPX RIP Filtering" on page 34
- "IPX RIP Filter Example" on page 37
- "IPX NetBIOS and Packet Forwarding Filters" on page 39
- "Configuring IPX Packet Forwarding" on page 39
- "IPX Packet Forwarding Filter Example" on page 43

How to Configure IPX SAP Filters

Before you begin, make sure that filtering support is enabled for IPX in NIASCFG.

To configure IPX incoming (or outgoing) SAP filtering, complete the following steps:

1 Load FILTCFG, then select the following parameter path:

   Select Configure IPX Filters > Incoming SAP Filters (or Outgoing SAP Filters)

2 Select Status and toggle the choice to read Enabled or Disabled .

   Any configured filters immediately become active (enabled) or inactive (disabled).

   NOTE: It might be easier to configure filters while they are disabled. Otherwise, you might experience temporary service loss while you are adding and setting up wildcard filters.

3 Select Action and toggle the choice to permit or deny the services on the filter list.

   This specifies the action taken when an incoming (or outgoing) service (SAP packet) matches a filter in the filter list. If you select to permit the services, the SAP information is received from (or broadcast to) the local networks. If you select to deny the services, the SAP information is not received from (or broadcast to) the local networks.

NOTE: Changing a filter to permit the services on the filter list when the filter list is empty denies all services and might produce undesirable results.

4 Select Filters .

This lists the incoming (or outgoing) SAP services that are currently permitted or denied, according to the Action parameter setting.

5 Modify the service list.

You can select a service from the list and press Enter to modify the service or Del to remove it. Press Ins to add a new service.

If you are modifying an existing filter, or adding a new filter, modify the following parameters from the Define Filter menu:

- Logging —Optionally select Enabled to log packets that match the Filters or Exceptions definitions.

  The header of packets that match the Filters or Exceptions definitions are logged as long as the global logging status and this logging status are both enabled. The logs are viewed using the NetWare Administrator utility.

- Service Name —Press Ins, then select from a list of unfiltered NetWare® services known to the router, or enter a service name.

  NOTE: You can use the asterisk (*) and question mark (?) wildcards. The * wildcard is equal to zero or more character matches. The ? wildcard is equal to precisely one character match. For example, SERVER-A* matches Server-A, SERVER-A2, and SERVER-A-MKTG, whereas SERVER-A? matches only SERVER-A2. You can enter several wildcard characters in a string. We recommend that you enter exceptions to wildcards first when working with an enabled filter list.

- Service Type —Enter a hexadecimal SAP number, or press Ins, then select from a list of defined IPX service types.

  You can use FFFF as a wildcard for any or all types.

- Source (or Destination) Type —Press Enter , then select Interface or Interface Group .

- Source (or Destination)—Press Enter and specify the source (or destination) for the filter.

  If you specified Interface as the Source (or Destination) Type , select a specific interface on which you want to filter the service. You can select a LAN interface, a WAN interface, the internal network, or all interfaces. The default is All Interfaces .

- Source (or Destination) Circuit —If you selected a WAN source (or destination), press Enter to define optional circuit information:

  Local Frame Relay DLCI # (for frame relay)—The DLCI circuit number used for calls.

  Remote System ID (for PPP, X.25, or ATM)—The name of the remote system server or remote peer associated with this circuit.

  Circuit Parameter Type (for X.25 or ATM)—The type of virtual circuit used to establish a connection.

  Remote DTE Address (for X.25)—The X.121 DTE address assigned to the specific remote DTE.

  Remote ATM Address (for ATM)—The address assigned to the specific remote ATM.

  NOTE: If the optional fields are left blank, the filter will match all WAN calls on the interface. If authentication is not enabled and the optional fields are specified, the filter will not work.

- Comment —Enter an optional short description.

6 Press Esc and save the information.

7 Select Exceptions .

This displays a list of exceptions to the incoming (or outgoing) SAP filters. Depending on the Action parameter setting, services that match a filter on this list are always or are never accepted (or advertised) by the router, even if another filter is configured to do the opposite.

8 Modify the exceptions list.

Select a service from the list and press Enter to modify the service or Del to remove it. Press Ins to add a new service. Refer to Step 5 and Step 6 to modify or add an exception.

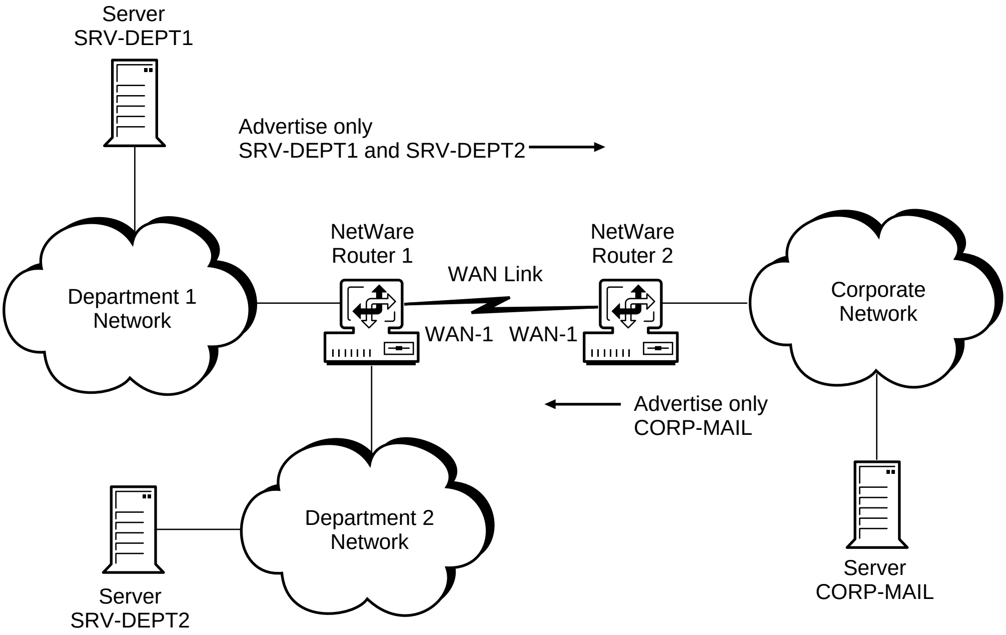
9 Press Esc to save the information and return to the Configure IPX Filters menu.

IPX SAP Filter Example

In this example, two departmental networks are connected to a corporate network through a WAN link between Router 1 and Router 2. The two routers use the RIP/SAP routing protocol to communicate with each other. RIP enables routers to send out periodic updates of service and routing information. The internetwork topology is shown in Figure 2 below.

NOTE: Either Router 1 or Router 2 can be set up to do the following: RIP/SAP can be run over the WAN link with an outbound SAP filter and with the NetWare Link Services Protocol™ (NLSP™) software on the LAN. RIP/SAP can be run on the LAN with an inbound filter and with NLSP on the WAN. RIP/SAP can be run on the LAN and WAN links, and both inbound and outbound filtering is enabled. On the WAN, both ends need to be consistently configured.

Figure 2 IPX SAP Filter Example



To minimize the load on the WAN link, an IPX SAP filter is configured on Router 1 and Router 2. This filter cuts down the periodic service information updates across the WAN link by advertising only a few selected servers. The clients across the WAN link can access the servers on the other network by first attaching to these selected servers.

When configuring this example, set the parameters as shown in Table 2.

Table 2 Parameters for IPX SAP Filter Example

Parameter	Value
Router 1 Action	Permit Services
Router 1 Filters:	.
Filter 1:	.
Service Name	SRV-DEPT1
Service Type	FFFF (All Types)
Destination Type	Interface
Destination	WAN-1
Destination Circuit	All Circuits
Filter 2:	
Service Name	SRV-DEPT2
Service Type	FFFF (All Types)
Destination Type	Interface
Destination	WAN-1
Destination Circuit	All Circuits
Router 2 Action	Permit Services
Router 2 Filters:	.
Service Name	CORP-MAIL
Service Type	FFFF (All Types)
Destination Type	Interface
Destination	WAN-1
Destination Circuit	All Circuits

How to Configure IPX RIP Filtering

Before you begin, make sure that filtering support is enabled for IPX in NIASCFG.

To configure IPX incoming (or outgoing) RIP filtering, complete the following steps:

1 Load FILTCFG, then select the following parameter path:

Select Configure IPX Filters > Incoming RIP Filters (or Outgoing RIP Filters)

2 Select Status and toggle the choice to read Enabled or Disabled.

Any configured filters immediately become active (enabled) or inactive (disabled).

NOTE: It might be easier to configure filters while they are disabled. Otherwise, you might experience temporary service loss while you are adding and setting up wildcard filters.

3 Select Action and toggle the choice to permit or deny the networks on the filter list.

This specifies the action taken on an incoming (or outgoing) network (RIP packet) in the filter list. If you select to permit networks, the RIP information is received from (or advertised to) local networks. If you select to deny networks, the RIP information is not received from (or advertised to) local networks.

NOTE: Changing a filter to permit the routes on the filter list when the filter list is empty denies all routes.

4 Select Filters .

This lists the incoming (or outgoing) RIP routes that are permitted or denied, according to the Action parameter setting.

5 Modify the network list.

Select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new network filter.

If you are modifying an existing filter or adding a new filter, modify the following parameters from the Define Filter menu:

NOTE: Whenever the internal network number of a server is filtered, the SAPs from the server are also filtered automatically.

- Logging —Optionally select Enabled to log packets that match the Filters or Exceptions definitions.

  The header of packets that match the Filters or Exceptions definitions are logged as long as the global logging status and this logging status are both enabled. The logs are viewed using the NetWare Administrator utility.

- Network Number —Enter a 4-byte hexadecimal number that identifies the IPX network.

- Network Mask —Enter a 4-byte hexadecimal number that defines the range of network numbers you want to filter.

A network number/mask pair of 0/0 matches all IPX networks. A 1 bit in the network mask means that bit must be matched. For example, C9000000/FFFFFF00 matches C90000XX network numbers.

NOTE: Bit masks do not need to be contiguous for filters.

- Source (or Destination) Type —Press Enter , then select Interface or Interface Group .
- Source (or Destination)—Press Ins and specify the source (or destination) of the route information.

  If you specified Interface as the Source (or Destination) Type , select a specific interface on which you want to filter the service. You can select a LAN interface, a WAN interface, the internal network, or all interfaces. The default is All Interfaces .

  If you specified Interface Group as the Source (or Destination) Type , select the specific interface group on which you want to filter the service.
- Source (or Destination) Circuit —If you selected a WAN source (or destination), press Enter to define optional circuit information:

  Local Frame Relay DLCI # (for frame relay)—The DLCI circuit number used for calls.

  Remote System ID (for PPP, X.25, or ATM)—The name of the remote system server or remote peer associated with this circuit.

  Circuit Parameter Type (for X.25 or ATM)—The type of virtual circuit used to establish a connection.

  Remote DTE Address (for X.25)—The X.121 DTE address assigned to the specific remote DTE.

  Remote ATM Address (for ATM)—The address assigned to the specific remote ATM.

  NOTE: If the optional fields are left blank, the filter will match all WAN calls on the interface. If authentication is not enabled and the optional fields are specified, the filter will not work.
- Comment —Enter an optional short description.

6 Press Esc and save the information.

7. Select Exceptions.

   Displays a list of exceptions to the incoming (or outgoing) RIP filters. Depending on the Actions parameter setting, routes that match a filter on this list are always or are never accepted (or advertised) by the router, even if another filter is configured to do the opposite.

8. Modify the exceptions list.

   Select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new network filter. Refer to Step 5 and Step 6 to add or modify a filter.

9. Press Esc to save the information and return to the Configure IPX Filters menu.

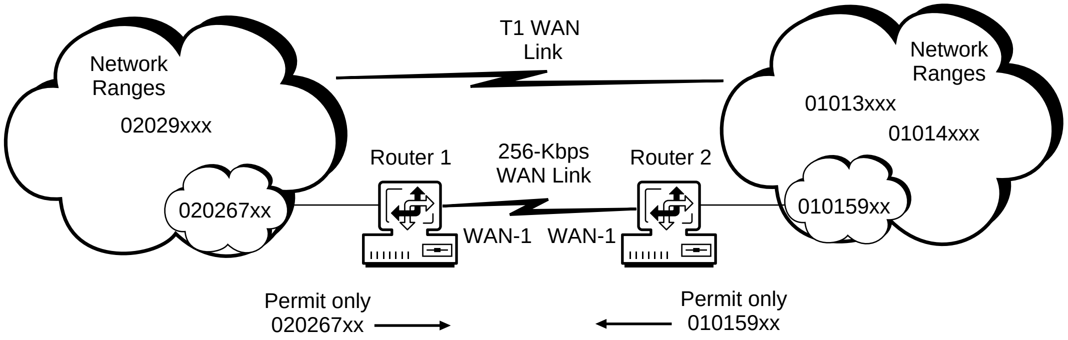
IPX RIP Filter Example

In this example, network clouds are connected to each other through a T1 WAN link and a 256-Kbps WAN link. Packets from specific network ranges in each cloud take longer to be transmitted through the T1 link than the 256-Kbps link because their proximity to the links are different.

To restrict access to the 256-Kbps link to those network ranges that benefit from it most, and to prevent other networks from accessing this slower link, outbound filters are configured in the routers attached to the 256-Kbps link. In this case, Router 1 permits only packets sent to network range 010159xx to be transmitted through the 256-Kbps link. Router 2 permits only packets sent to network range 020267xx to be transmitted through the 256-Kbps link.

The internetwork topology is shown in Figure 3 on page 38.

Figure 3 **IPX Routing Information Filter Example**



When configuring this example, set the parameters as shown in Table 3.

Table 3 **Parameters for IPX Outgoing Filter Example**

Parameter	Value
Router 1 Actions	Permit Networks
Filters: Network Number Network Mask Destination Type Destination Interface Destination Circuit	. 02026700 FFFFFF00 Interface WAN-1 All Circuits
Router 2 Actions	Permit Networks
Filters: Network Number Network Mask Destination Type Destination Interface Destination Circuit	. 01015900 FFFFFF00 Interface WAN-1 All Circuits

IPX NetBIOS and Packet Forwarding Filters

IPX packet forwarding filters allow the router to filter a packet according to the source and destination address fields and the packet type. NetBIOS filters allow the router to forward NetBIOS broadcast packets only on selected interfaces.

NOTE: IPX NetBIOS and packet forwarding filters work while using either NLSP or RIP/SAP routing modes.

Configuring IPX Packet Forwarding

Before you begin, make sure that filtering support is enabled for IPX in NIASCFG. Otherwise, filtering will not work.

To configure IPX packet forwarding filters, complete the following steps:

1. Load FILTCFG, then select the following parameter path:

   Select Configure IPX Filters > NetBIOS and Packet Forwarding Filters

2. Select Status and toggle the choice to read Enabled or Disabled .

   NOTE: It might be easier to configure filters while they are disabled. Otherwise, you might experience temporary service loss while you are adding and setting up wildcard filters.

3. Select NetBIOS Broadcast Filters Action and toggle the choice to permit or deny the IPX NetBIOS packets on the listed interfaces.

4. Select NetBIOS Broadcast Filters Interfaces, then press Enter .

   This displays a list of interfaces that are permitted or denied for NetBIOS broadcast. Press Ins to add an interface to the list, or select an interface and press Del to remove it from the list. You can select a LAN interface, a WAN interface, the internal network, or all interfaces.

5. Select Interface Groups , then press Enter .

   This displays a list of interface groups that are permitted or denied for NetBIOS broadcast. Press Ins to add an interface to the list, or select an interface and press Del to remove it from the list.

6. Select Packet Forwarding Filters Action and toggle the choice to permit or deny the packet forwarding filters on the filter list.

7. Select Filters .

   This lists the NetBIOS filters that are permitted or denied, according to the Action parameter setting.

8 Modify the filter list.

Select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new filter.

If you are modifying an existing filter or adding a new filter, modify the following parameters from the Define Filter menu:

- Source Interface Type —Press Enter and select Interface or Interface Group as the incoming IPX packet source.
- Source Interface —Press Enter and select the source from the list of network interfaces or interface groups.

  If you specified Interface as the Source Interface Type , select a specific interface on which you want to filter the service. You can select a LAN interface, a WAN interface, the internal network, or all interfaces. The default is All Interfaces .

  If you specified Interface Group as the Source Interface Type , select the specific interface group on which you want to filter the service.
- Source Circuit —If the source is a WAN interface, press Enter to modify the following optional circuit information:

  Local Frame Relay DLCI # (for frame relay)—The DLCI circuit number used for calls.

  Remote System ID (for PPP, X.25, or ATM)—The name of the remote system server or remote peer associated with this circuit.

  Circuit Parameter Type (for X.25 or ATM)—The type of virtual circuit used to establish a connection.

  Remote DTE Address (for X.25)—The X.121 DTE address assigned to the specific remote DTE.

  Remote ATM Address (for ATM)—The address assigned to the specific remote ATM.

  NOTE: If the optional fields are left blank, the filter will match all WAN calls on the interface. If authentication is not enabled and the optional fields are specified, the filter will not work.
- Destination Interface Type —Press Enter and select Interface or Interface Group as the IPX packet destination.

- Destination Interface —Press Enter and select a destination from the list of network interfaces or interface groups.

  If you specified Interface as the Source (or Destination) Interface Type , select a specific interface on which you want to filter the service. You can select a LAN interface, a WAN interface, the internal network, or all interfaces. The default is All Interfaces .

  If you specified Interface Group as the Destination (or Source) Interface Type , select the specific interface group on which you want to filter the service.

- Destination Circuit—If the destination is a WAN interface, press Enter to modify the following optional circuit information:

  Local Frame Relay DLCI # (for frame relay)—The DLCI circuit number used for calls.

  Remote System ID (for PPP, X.25, or ATM)—The name of the remote system server or remote peer associated with this circuit.

  Circuit Parameter Type (for X.25 or ATM)—The type of virtual circuit used to establish a connection.

  Remote DTE Address (for X.25)—The X.121 DTE address assigned to the specific remote DTE.

  Remote ATM Address (for ATM)—The address assigned to the specific remote ATM.

- Packet Description —Press Enter and select from a list of defined IPX packet types, or press Ins to define a packet type.

  Enter the following information to define the type of IPX packet you can filter:

  Name —Enter a name for the packet.

  Packet Type —Enter a 1-byte packet type number in hexadecimal. The FF wildcard matches all packet numbers.

  Destination Socket —Enter a 2-byte socket number in hexadecimal. The wildcard FFFF matches all socket numbers.

  Comment —Enter an optional short description.

- Source Address Type —Press Enter and select Any Address , Network , or Node as the source address type.

- Source IPX Address —Enter the address if you selected Network or Node.
- Destination Address —Press Enter and select Any Address , Network , or Node as the destination address.
- Destination IPX Address —Enter the address if you selected Network or Node .

  A network numbers/mask pair of 0/0 matches all IPX networks. A 1 bit in the network mask means that bit must be matched. For example, C9000000/FFFFFF00 matches C90000XX network numbers.
- Comment —Enter an optional short description.
- Logging —Optionally select Enabled to log packets that match the Filters or Exceptions definitions.

  The header of packets that match the Filters or Exceptions definitions are logged as long as the global logging status and this logging status are both enabled. The logs are viewed using the NetWare Administrator utility.

9. Press Esc and save the filter information.
10. Select Exceptions.

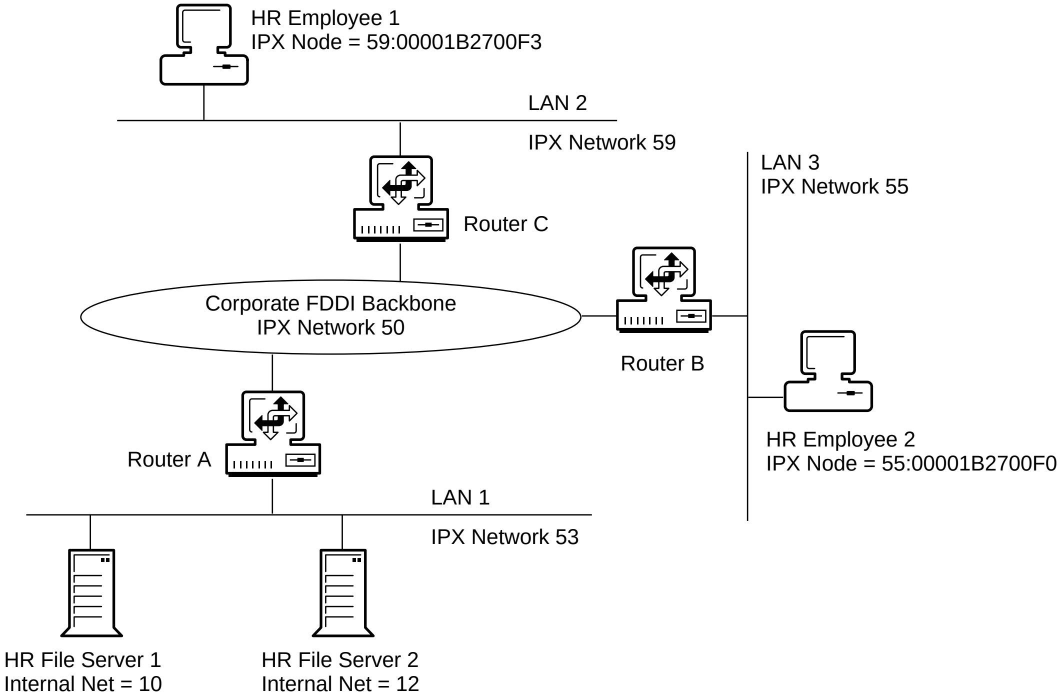
    This lists the exceptions to the IPX forwarding filters. According to the Action parameter specified, the packets that match a filter on this list are always or are never forwarded by the router, even if another filter is configured to do the opposite.
11. Modify the exceptions list.

    Press Ins to add a new filter, or select a filter from the list and press Enter to modify the filter or Del to remove it. Refer to Step 8 on page 40 and Step 9 on page 42 to modify or add a filter.
12. Press Esc to save the information and exit to the Configure IPX Filters menu.

IPX Packet Forwarding Filter Example

In this example, an FDDI backbone connects several departments in an organization. Routers A, B, and C connect the departmental networks to the backbone. Within the organization, users can access all servers. However, the Human Resources (HR) servers can be accessed only by HR employees. To make the HR servers secure, packet forwarding filters are used in addition to the usual NetWare password security. Note that some of the HR employees are connected to different networks than the one HR servers are connected to Figure 4 shows the internetwork topology.

Figure 4 IPX Packet Forwarding Filter Example



Routers B and C do not require filters because users can access all corporate servers (except for the HR server). Packet forwarding filters are installed on Router A to block packets from the FDDI interface to the HR servers, except when the packets are from the nodes 59:00001B2700F3 and 55:00001B2700F0.

When configuring this example, set the parameters as shown in Table 4.

Table 4 Parameters for IPX Packet Forwarding Filter Example

Parameter	Value
Action	Deny Packets
Filter List:	.
Source Interface Type	Interface
Source Interface	FDDI
Source Circuit	All Circuits
Destination Interface Type	Network
Destination Interface	10/FFFFFFFF
Destination Circuit	All Circuits
Packet	<Any>
Source Address Type	Network
Source IPX Address	FDDI
Destination Address	Network
Destination IPX Address	10/FFFFFFFF
Source Interface Type	Interface
Source Interface	FDDI
Source Circuit	All Circuits
Destination Interface Type	Network
Destination Interface	12/FFFFFFFF
Destination Circuit	All Circuits
Packet	<Any>
Source Address Type	Network
Source IPX Address	FDDI
Destination Address	Network
Destination IPX Address	12/FFFFFFFF

Parameter	Value
Exceptions:	.
Source Interface Type	Node
Source Interface	59:00001B2700F3
Source Circuit	All Circuits
Destination Interface Type	Network
Destination Interface	10/FFFFFFFF
Destination Circuit	All Circuits
Packet	<Any>
Source Address Type	Node
Source IPX Address	59:00001B2700F3
Destination Address	Network
Destination IPX Address	10/FFFFFFFF
Source Interface Type	Node
Source Interface	55:00001B2700F0
Source Circuit	All Circuits
Destination Interface Type	Network
Destination Interface	10/FFFFFFFF
Destination Circuit	All Circuits
Packet	<Any>
Source Address Type	Node
Source IPX Address	55:00001B2700F0
Destination Address	Network
Destination IPX Address	10/FFFFFFFF
Source Interface Type	Node
Source Interface	59:00001B2700F3
Source Circuit	All Circuits
Destination Interface Type	Network
Destination Interface	12/FFFFFFFF
Destination Circuit	All Circuits
Packet	<Any>
Source Address Type	Node
Source IPX Address	59:00001B2700F3
Destination Address	Network
Destination IPX Address	12/FFFFFFFF

Parameter	Value
Source Interface Type	Node
Source Interface	55:00001B2700F0
Source Circuit	All Circuits
Destination Interface Type	Network
Destination Interface	12/FFFFFFFF
Destination Circuit	All Circuits
Packet	<Any>
Source Address Type	Node
Source IPX Address	55:00001B2700F0
Destination Address	Network
Destination IPX Address	12/FFFFFFFF

Configuring TCP/IP Filters

TCP/IP supports the following filters:

- Incoming RIP filters (routing information)
- Outgoing RIP filters (routing advertisement)
- Packet forwarding filters
- Incoming Exterior Gateway Protocol (EGP) filters (routing information)
- Outgoing EGP filters (routing advertisement)
- Open Shortest Path First (OSPF) external route filters

Refer to Understanding for more information.

NOTE: When you configure a filter for a primary WAN call, an equivalent filter is automatically generated for the backup call. If the primary call should fail, the backup call is automatically connected.

This section contains the following topics:

How to Configure IP Routing Information Filters

Before you begin, make sure that filtering support is enabled for IP in NIASCFG under the TCP/IP Protocol menu. Otherwise, filtering will not work.

To configure IP incoming (or outgoing) RIP filters, complete the following steps:

1. Load FILTCFG, then select the following parameter path:

   Select Configure TCP/IP Filters > Incoming RIP Filters (or Outgoing RIP Filters)

2. Select Status and toggle the choice to read Enabled or Disabled .

   Any configured filters immediately become active (enabled) or inactive (disabled).

3. Select Action and toggle the choice to permit or deny the routes in the filter list.

   This specifies the action taken when an incoming (or outgoing) RIP packet matches a filter on the filter list.

   If you select to permit the routes, the matching RIP routes are accepted (or advertised) by the router. If you select to deny the routes, the matching RIP routes are not accepted (or advertised) by the router.

4. Select Filters .

   This lists the incoming (or outgoing) RIP filters that are permitted or denied, according to the Action parameter setting.

5. Modify the route list.

   You can select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new filter.

   If you are modifying an existing filter or adding a new filter, modify the following parameters from the Define Filter menu:

   - Route to Network or Host —Specify All Routes , Host , or Network as the type of route to be filtered.

   - IP Address of Network/Host —Enter a 4-byte IP address in dotted decimal notation. You do not need to enter this if you selected All Routes for the Route to Network/Hosts parameter.

- Subnetwork Mask —Enter a 4-byte mask address in dotted decimal or hexadecimal notation. Do this only if you selected Network for the Route to Network/Hosts parameter.
- Source (or Destination) Type —Select Interface , Interface Group , or Network as the source (or destination) type.
- Source (or Destination)—Press Enter , then select the source (or destination) that the route is advertised to or blocked from.

  If you specified Interface for the Source (or Destination) Type parameter, select a specific interface on which you want to filter the service. You can select a LAN interface, a WAN interface, or all interfaces. The default is All Interfaces .

  If you specified Interface Group for the Source (or Destination) Type parameter, select the specific interface group on which you want to filter the service.

  If you selected Network for the Source (or Destination) Type parameter, type the TCP/IP address and the subnet mask.
- Source (or Destination) Circuit —If you selected a WAN source (or destination), press Enter to define optional circuit information:

  Local Frame Relay DLCI # (for frame relay)—The DLCI circuit number used for calls.

  Remote System ID (for PPP, X.25, or ATM)—The name of the remote system server or remote peer associated with this circuit.

  Circuit Parameter Type (for X.25 or ATM)—The type of virtual circuit used to establish a connection.

  Remote DTE Address (for X.25)—The X.121 DTE address assigned to the specific remote DTE.

  Remote ATM Address (for ATM)—The address assigned to the specific remote ATM.
- Advertised Hop Count —Enter a number from 1 to 16.

  This option is enabled if the filter is configured to permit or advertise the route. If you leave this option blank, the TCP/IP routing table is consulted automatically for the required information. A value of 16 disables the route.
- Comment —Enter an optional short description.

- Logging —Optionally select Enabled to log packets that match the Filters or Exceptions definitions.

  The header of packets that match the Filters or Exceptions definitions are logged as long as the global logging status and this logging status are both enabled. The logs are viewed using the NetWare Administrator utility.

6 Press Esc and save the filter information.

7 Select Exceptions .

  This displays a list of exceptions to the configured filters. Depending on the Action parameter setting, packets that match a filter on this list are always or are never accepted (or advertised), even if another filter is configured to do the opposite.

  NOTE: The Exceptions list filters always takes a higher priority than other filters.

8 Modify the exceptions list.

  Select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new filter. Refer to Step 5 and Step 6 if you are adding or modifying a filter.

9 Press Esc to save the information and return to the Configure TCP/IP Filters menu.

How to Configure EGP Filters

IMPORTANT: No routes are accepted by EGP unless EGP filters are configured.

Before you begin, make sure that filtering support is enabled for IP in NIASCFG. Otherwise, filtering will not work.

To configure IP incoming (or outgoing) EGP filters, perform the following steps:

1 Load FILTCFG, then select the following parameter path:

  Select Configure TCP/IP Filters > Incoming EGP Filters (or Outgoing EGP Filters)

2 Select Status and toggle the choice to read Enabled or Disabled .

  Any configured filters immediately become active (enabled) or inactive (disabled).

3 Select Action and toggle the choice to permit or deny the routes in the filter list.

This specifies the action taken when an incoming (or outgoing) EGP packet matches a filter on the filter list. If you select to permit the routes, the matching EGP routes are accepted (or advertised) by the router. If you select to deny the routes, the matching EGP routes are not accepted (or advertised) by the router.

4 Select Filters .

This lists the incoming (or outgoing) EGP routes that are permitted or denied, according to the Action parameter setting.

5 Modify the route list.

You can select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new filter.

If you are modifying an existing filter or adding a new filter, modify the following parameters from the Define Filter menu:

- Route to Network or Host —Press Enter and specify All Routes or Network as the type of route to be filtered.
- IP Address of Network/Host —Enter an IP address in dotted decimal notation if you selected Network .
- Subnetwork Mask —Enter a 4-byte subnet mask address in dotted decimal or hexadecimal notation.
- Source (or Destination) Type —Select Autonomous System , Host , Interface , Interface Group , or Network .
- Source (or Destination)—Fill in the following information, based on what you selected for the Source (or Destination) Type :

  Autonomous System —Press Enter , then type the autonomous system number (from 0 to 65535) from which the route is learned (source) or advertised (destination).

  Host —Press Enter , then type the TCP/IP address in dotted decimal notation.

  Interface —Press Enter , then select a specific interface on which you want to filter the service. You can select a LAN interface, a WAN interface, or all interfaces. The default is All Interfaces .

  Interface Group —Press Enter , then select an interface group from the list.

  Network —Press Enter , then type the TCP/IP address and subnet mask numbers in dotted decimal notation.

- Source (or Destination) Circuit —If you selected a WAN source (or destination), press Enter to define optional circuit information:

  Local Frame Relay DLCI # (for frame relay)—The DLCI circuit number used for calls.

  Remote System ID (for PPP, X.25, or ATM)—The name of the remote system server or remote peer associated with this circuit.

  Circuit Parameter Type (for X.25 or ATM)—The type of virtual circuit used to establish a connection.

  Remote DTE Address (for X.25)—The X.121 DTE address assigned to the specific remote DTE.

  Remote ATM Address (for ATM)—The address assigned to the specific remote ATM.

- Metric Value —Enter a number to be associated with the route.

  This option is enabled only if the filter is configured to permit or advertise the route. If you leave this option blank, the TCP/IP routing table is consulted automatically for the required information.

- Comment —Enter an optional short description.

- Logging —Optionally select Enabled to log packets that match the Filters or Exceptions definitions.

  The header of packets that match the Filters or Exceptions definitions are logged as long as the global logging status and this logging status are both enabled. The logs are viewed using the NetWare Administrator utility.

6 Press Esc and save the filter information.

7 Select Exceptions .

Lists the exceptions to the configured filters. Depending on the Action parameter setting, packets that match a filter on this list are always or are never advertised (or hidden), even if another filter is configured to do the opposite.

8 Modify the exceptions list.

Select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new filter. Refer to Step 5 and Step 6 if you are adding or modifying a filter.

9 Press Esc to save the information and return to the Configure TCP/IP Filters menu.

How to Configure OSPF External Route Filters

NOTE: OSPF external route filters apply only to routes learned from RIP, EGP, or static routes.

Before you begin, make sure that filtering support is enabled for IP in NIASCFG. Otherwise, filtering will not work.

To configure OSPF external route filters, complete the following steps:

1 Load FILTCFG, then select the following parameter path:

Select Configure TCP/IP Filters > OSPF External Route Filters

2 Select Status and toggle the choice to read Enabled or Disabled .

Any configured filters immediately become active (enabled) or inactive (disabled).

3 Select Action and toggle the choice to permit or deny the routes in the filter list.

If permitted, all matching routes are forwarded by the router. If denied, all matching routes are not forwarded by the router.

4 Select Filters.

This lists the routes that are permitted or denied, according to the Action parameter setting.

5 Modify the route list.

Select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new filter.

If you are modifying an existing filter or adding a new filter, modify the following parameters from the Define Filter menu:

- Route to Network or Host—Press Enter to specify All Routes , Host, or Network as the type of route to be filtered.
- IP Address of Network Host —Enter a 4-byte IP address in dotted decimal notation if you specified Network or Host for the Route to Network or Host parameter.
- Subnetwork Mask —Enter a 4-byte mask address in dotted decimal or hexadecimal notation if you specified Network for the Route to Network or Host parameter.

- Metric Value —Enter a metric or cost associated with the route.

  This option is enabled only if the filter is configured to permit or advertise the route. If you leave this option blank, the TCP/IP routing table is consulted automatically for the required information.

- Comment —Enter an optional short description.
- Logging —Optionally select Enabled to log packets that match the Filters or Exceptions definitions.

  The header of packets that match the Filters or Exceptions definitions are logged as long as the global logging status and this logging status are both enabled. The logs are viewed using the NetWare Administrator utility.

6. Press Esc and save the filter information.
7. Select Exceptions .

   This lists the exceptions to the configured route filter list. Depending on the Action parameter setting, packets that match a filter on this list are always or are never permitted or denied, even if another filter is configured to do the opposite.

8. Modify the exceptions list.

   Select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new filter. Refer to Step 5 and Step 6 if you are adding or modifying a filter.

9. Press Esc to save the information and return to the Configure TCP/IP Filters menu.

IP Routing Information Filter Example

In this example, the Accounting department is connected to the FDDI backbone by Router C. One of the networks within Accounting is 151.1.0.0 (subnet mask of 255.255.255.0). Because access to this network from outside the Accounting department is not required, the administrator has selected not to propagate a route to this network outside the Accounting department.

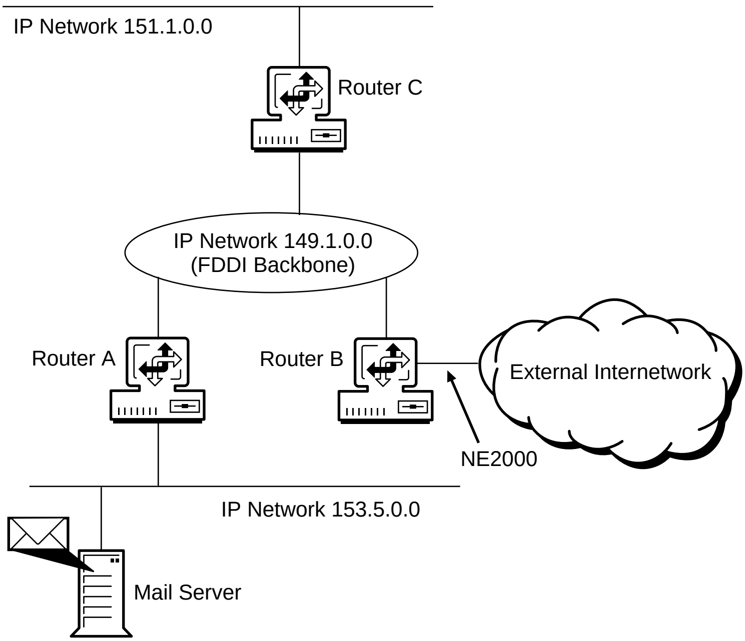
To hide network 151.1.0.0 from the rest of the organization, an outgoing RIP filter is configured on Router C.

Because IP supports RIP, OSPF, and EGP, routing filters must always specify the routing protocol for which the filter applies. In this case, RIP is used by all routers in the organization, and a RIP routing information filter is configured.

The route being hidden from the rest of the network is defined by the Accounting department network with IP network address 151.1.0.0. Router C's connection to the departments outside Accounting is through the FDDI backbone. The destination from which network 151.1.0.0 is hidden is most easily defined as the FDDI interface to the backbone. Figure 5 shows the internetwork topology.

Note that Router C has the route to network 151.1.0.0 in its routing table. If Router C receives a packet from the FDDI backbone that is destined for network 151.1.0.0, it forwards the packet.

Figure 5 IP Routing Information Filter Example



When configuring this example, set the parameters as shown in Table 5 .

Table 5 Parameters for IP Outgoing Routing Information Filter Example

Parameter	Value
Action	Deny Routes
Filters: Route to Network or Host IP Address of Network Host Subnet Mask Destination Type Destination	. Network 151.1.0.0 255.255.255.0 Interface FDDI Interface

IP Packet Forwarding Filters

IP packet forwarding filters let the router filter packets selectively, according to their type, source, and destination.

Configuring IP Packet Forwarding Filtering

Before you begin, make sure that filtering support is enabled for IP in NIASCFG. Otherwise, filtering will not work.

To configure IP packet forwarding filtering, complete the following steps:

1. Load FILTCFG, then select the following parameter path:

   Select Configure TCP/IP Filters > Packet Forwarding Filters

2. Select Status and toggle the choice to read Enabled or Disabled .

   Any configured filters immediately become active (enabled) or inactive (disabled).

3. Select Action and toggle the choice to permit or deny the packets in the filter list.

   If denied, matching packets are not forwarded by the router. If permitted, matching packets are forwarded by the router.

4. Select Filters .

   This lists the packets that are permitted or denied, according to the Action parameter setting.

5 Modify the packet list.

Select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new packet filter.

If you are modifying an existing filter or adding a new filter, specify the following parameters from the Define Filter menu:

NOTE: You cannot modify a predefined packet type.

- Source Interface Type —Press Enter and select Interface or Interface Group as the source type.
- Source Interface —Press Enter and select an interface or interface group from the list.

  If you specified Interface as the Source Interface Type , select a specific interface on which you want to filter the service. You can select a LAN interface, a WAN interface, or all interfaces. The default is All Interfaces .

  If you specified Interface Group as the Source Interface Type , select the specific interface group on which you want to filter the service.
- Source Circuit —If you selected a WAN interface source, press Enter to define optional circuit information:

  Local Frame Relay DLCI # (for frame relay)—The DLCI circuit number used for calls.

  Remote System ID (for PPP, X.25, or ATM)—The name of the remote system server or remote peer associated with this circuit.

  Circuit Parameter Type (for X.25 or ATM)—The type of virtual circuit used to establish a connection.

  Remote DTE Address (for X.25)—The X.121 DTE address assigned to the specific remote DTE.

  Remote ATM Address (for ATM)—The address assigned to the specific remote ATM.
- Destination Interface Type —Select Interface or Interface Group as the interface type.
- Destination Interface —Press Enter and select an interface or interface group from the list.

  If you specified Interface as the Destination Interface Type , select a specific interface on which you want to filter the service. You can select a LAN interface, a WAN interface, or all interfaces. The default is All Interfaces .

If you specified Interface Group as the Destination Interface Type , select the specific interface group on which you want to filter the service.

- Destination Circuit —If you selected a WAN interface destination, press Enter to define optional circuit information:

  Local Frame Relay DLCI # (for frame relay)—The DLCI circuit number used for calls.

  Remote System ID (for PPP, X.25, or ATM)—The name of the remote system server or remote peer associated with this circuit.

  Circuit Parameter Type (for X.25 or ATM)—The type of virtual circuit used to establish a connection.

  Remote DTE Address (for X.25)—The X.121 DTE address assigned to the specific remote DTE.

  Remote ATM Address (for ATM)—The address assigned to the specific remote ATM.

- Packet Type —Press Enter and select a packet type from the list.

  The Protocol and Port(s) fields are automatically filled in, according to your packet type selection.

- Source Address Type —Press Enter and select Any Address , Host , or Network .
- Source TCP/IP Address —Enter the address and subnet mask of the network or host.
- Destination Address Type —Press Enter and select Any Address , Host , or Network .
- Destination TCP/IP Address —Enter the address and subnet mask of the network or host.
- Comment —Enter an optional short description.
- Logging —Optionally select Enabled to log packets that match the Filters or Exceptions definitions.

  The header of packets that match the Filters or Exceptions definitions are logged as long as the global logging status and this logging status are both enabled. The logs are viewed using the NetWare Administrator utility.

6. Press Esc and save the filter information.

7. Select Exceptions to display a list of exceptions to the permitted or denied packets.

   This lists the exceptions to the configured packet filter list. Depending on the Action parameter setting, packets that match a filter on this list are always or are never permitted or denied, even if another filter is configured to do the opposite.

8. Modify the exceptions list.

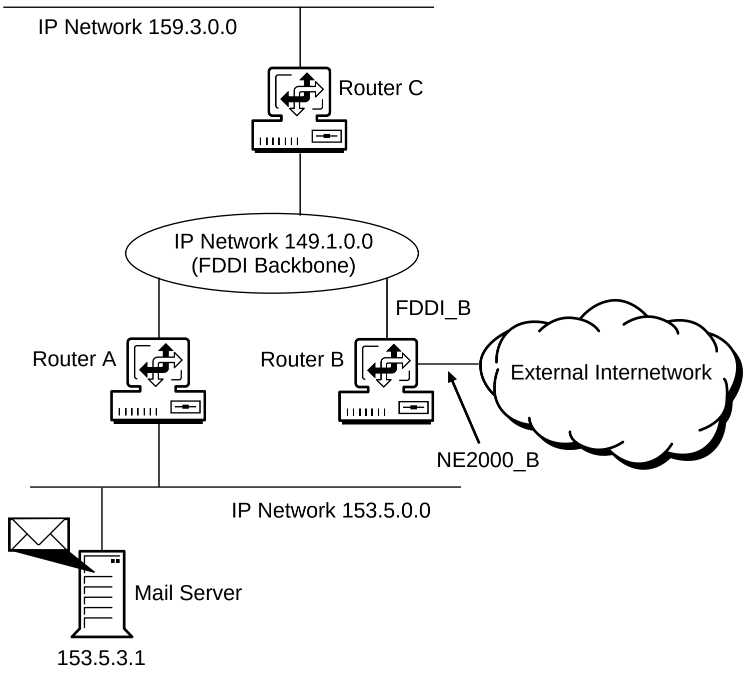
   Select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new filter. Refer to Step 5 and Step 6 if you are adding or modifying a filter.

9. Press Esc to save the information and return to the Configure TCP/IP Filters menu.

IP Packet Forwarding Filter Example

In this example, an organization has an FDDI backbone connecting several departments within the organization and a link to external networks. Routers A and C connect the departmental networks to the backbone. Router B connects the external networks to the backbone. Within the organization, users can communicate freely across the internetwork. External access is limited to electronic mail. The internetwork topology is shown in Figure 6 on page 59.

Figure 6 IP Packet Forwarding Filter Example



Because internal communication is not restricted, packet forwarding filters are not required on Routers A or C.

Two packet forwarding filters are required on Router B. The first filter ensures that any packet originating within the organization's internal networks are forwarded by Router B. The second filter provides access to the corporate mail server and allows external users to send and receive electronic mail to and from internal users.

To configure the first filter, the source identifies the packets that originate in the internal networks. The simplest way to do this on Router B is to identify all packets received from the FDDI backbone interface. Because internal users can use any service at any location, the remaining fields in the filter can be specified as ANY.

The source of the second filter is all packets originating from external networks. Because the interface NE2000_B is the only connection that Router B has to the external networks, this can be used to specify the source field for this filter. SMTP (Simple Mail Transfer Protocol) is selected from the predefined services list. The allowable destinations are limited to the corporate mail servers. Host 153.5.3.1 is the only mail server defined.

When configuring this example, set the parameters as shown in Table 6 .

Table 6 Parameters for IP Packet Forwarding Filter Example

Parameter	Value
Action	Permit Packets
Filters List	.
Filter 1:	.
Source Interface Type	Interface
Source Interface	FDDI backbone
Destination Interface Type	Interface
Destination Interface	All Interfaces
Packet Type	Any
Source Address Type	Any Address
Destination Address Type	Any Address
Filters List	.
Filter 2:	.
Source Interface Type	Interface
Source Interface	NE2000_B
Destination Interface Type	Interface
Destination Interface	All Interfaces
Packet Type	SMTP
Source Address Type	Any Address
Destination Address Type	Host
Destination TCP/IP Address	153.5.3.1

Configuring AppleTalk Filters

AppleTalk supports the following types of filters:

- Device hiding filters
- Outgoing route filters (routes advertised)
- Incoming route filters (routes accepted)

NOTE: When you configure a filter for a primary WAN call, an equivalent filter is automatically generated for the backup call. If the primary call should fail, the backup call is automatically connected. You can only view primary filters using FILTCFG. Backup filters do not appear in FILTCFG.

Refer to Chapter 1, “Understanding,” on page 9 for more information.

This section contains the following topics:

- “How to Configure AppleTalk Device Hiding Filtering” on page 61
- “Example AppleTalk Device Hiding Filter” on page 65
- “How to Configure AppleTalk Route Filtering” on page 66
- “AppleTalk Outgoing Routing Information Filter Example” on page 68

How to Configure AppleTalk Device Hiding Filtering

Before you begin, make sure that filtering support is enabled for AppleTalk in NIASCFG. Otherwise, filtering will not work.

To configure AppleTalk device hiding filtering, complete the following steps:

1 Load FILTCFG, then select the following parameter path:

Select Configure AppleTalk Filters > Device Hiding Filters

2 Select Action and toggle the choice to show or hide the devices listed in the filter list.

This specifies the action taken when an NBP reply packet matches a filter in the filter list. If you specify to show the devices, the AppleTalk router forwards only the NBP replies that match a filter in the filter list. If you specify to hide the devices, the AppleTalk router discards all NBP replies that match a filter in the filter list.

3 Select Filters .

This displays a list of filters that hide or show devices, depending on the setting of the Action parameter. The name, type, device location, and user location are listed for each device filter.

4 Modify the filter list.

Select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new filter.

If you are modifying an existing filter or adding a filter, specify the following parameters in the Define Filter menu:

- Device Name —Enter an NBP name of up to 32 characters.

  Keep the default (=) to select all NBP names. An AppleTalk device advertises itself on the network according to the Device Name and Device Type values.

- Device Type —Press Enter and select from a list of defined AppleTalk NBP device types, or press Ins to add a new NBP type with the following information:

  Device Type —Enter a text string of up to 32 characters.

  Comment —Enter an optional short description.

- Device Location Type —Specify where the filtered device is located from the following choices: <Any> (the default), Interface , Interface Group , Non-extended Network , Multiple/Extended Network, Zone , or AURP Tunnel .

  Select <Any> to select all device locations to show or hide all devices to the user location.

- Device Location —Specify the following parameters, based on what you selected for Device Location Type :

  <Any > or AURP Tunnel —This field cannot be edited.

  Interface —Press Enter , then select a specific interface on which you want to filter the service. You can select a LAN interface, a WAN interface, the internal network, or all interfaces. The default is All Interfaces .

  Interface Group —Press Enter , then select a network interface group from the list.

  Non-extended Network —Press Enter , then type a network number to identify the nonextended network in which the filtered device is located.

  Multiple/Extended Networks —Press Enter , then type the start and end network numbers for the extended network in which the filtered device is located. The start number must be greater than zero, and the end number must be greater than or equal to the start value.

  You can enter a specific extended network, or a range of extended and nonextended networks. For example, for networks 1-9, 10, 11-20, 21-30, specifying an extended range of 1-30 will filter all devices in the 1-9, 10, 11-20, and 21-30 extended networks.

  Zone —Press Enter , then type the name of the AppleTalk zone in which the filtered device is located.

- Device Circuit —If you selected a WAN circuit, press Enter to modify the following optional circuit information:

  Local Frame Relay DLCI # (for frame relay)—The DLCI circuit number used for calls.

  Remote System ID (for PPP, X.25, ISDN, or ATM)—The name of the remote system server or remote peer associated with this circuit.

  Circuit Parameter Type (for X.25 or ATM)—The type of virtual circuit used to establish a connection.

  Remote DTE Address (for X.25)—The X.121 DTE address assigned to the specific remote DTE.

  Remote ATM Address (for ATM)—The address assigned to the specific remote ATM.

- User Location Type —Select a location type from one of the following choices: <Any> (the default), Interface , Interface Group , Non-extended Network , Multiple/Extended Network , Zone , or AURP Tunnel . Select <Any> if you do not know the location of the device or if the network location does not matter.

- User Location —Specify the locations of the users whose access to the devices must be controlled. Specify one of the following, based on what you selected for User Location Type :

  <Any > or AURP Tunnel —This field cannot be edited.

  Interface —Press Enter , then select a specific interface on which you want to filter the service. You can select a LAN interface, a WAN interface, the internal network, or all interfaces. The default is All Interfaces .

  Interface Group —Press Enter , then select a network interface group from the list.

  Non-extended Network —Press Enter , then type a network number to identify the nonextended network in which the filtered device is located.

  Multiple/Extended Networks —Press Enter , then type the start and end network numbers for the extended network in which the filtered device is located. The start number must be greater than zero, and the end number must be greater than or equal to the start value.

  You can enter a specific extended network, or a range of extended and nonextended networks. For example, for networks 1-9, 10, 11-20, 21-30, specifying an extended range of 1-30 will filter all devices in the 1-9, 10, 11-20, and 21-30 extended networks.

Zone —Press Enter , then type the name of the AppleTalk zone in which the filtered device is located.

- User Circuit —If you selected a WAN interface, press Enter to modify the following optional circuit information:

  Local Frame Relay DLCI # (for frame relay)—The DLCI circuit number used for calls.

  Remote System ID (for PPP, X.25, ISDN, or ATM)—The name of the remote system server or remote peer associated with this circuit.

  Circuit Parameter Type (for X.25 or ATM)—The type of virtual circuit used to establish a connection.

  Remote DTE Address (for X.25)—The X.121 DTE address assigned to the specific remote DTE.

  Remote ATM Address (for ATM)—The address assigned to the specific remote ATM.

- Comment —Enter an optional short description.

5 Press Esc and save the filter information.

6 Select Exceptions .

This lists the exceptions to the device filter list. Depending on the Action parameter setting, devices that match a filter on this list are always or are never permitted or denied, even if another filter is configured to do the opposite.

7 Modify the exceptions list.

Select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new filter. Refer to Step 4 and Step 5 to modify or add a filter to the exceptions list.

8 Select Status and toggle the choice to read Enabled or *Disabled* .

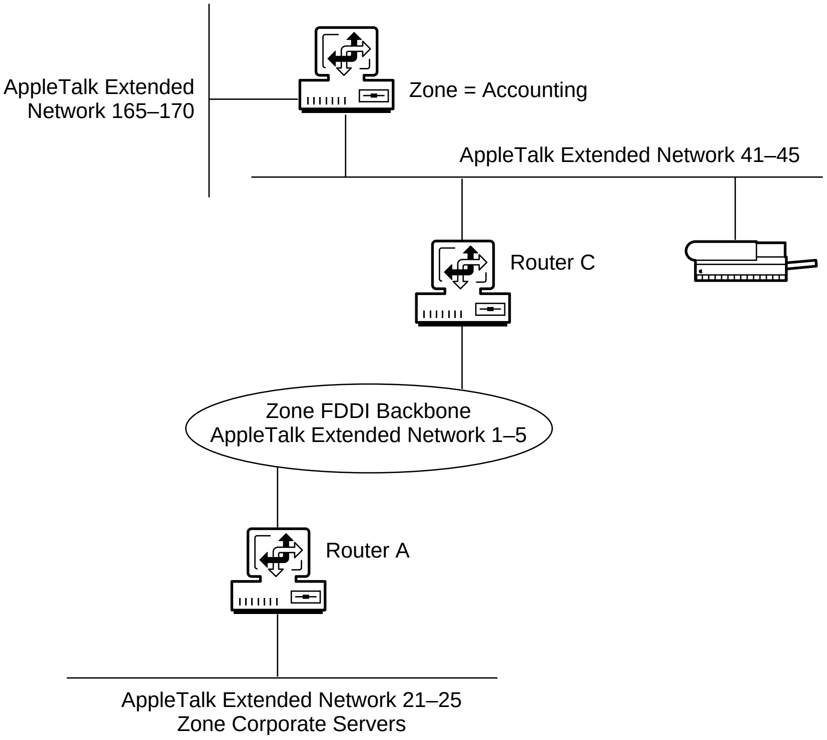
All configured filters immediately become active (enabled) or inactive (disabled).

9 Press Esc to save the information and return to the Configure AppleTalk Filters menu.

Example AppleTalk Device Hiding Filter

FigureFigure 7 on page 65 shows the internetwork topology for an organization with an FDDI backbone connecting several departments within the organization and a link to external networks. Routers A and C connect the departmental networks to the backbone. In general, users can communicate freely across the internetwork. However, access to printers within the Accounting department is restricted.

Figure 7 AppleTalk Device Hiding Filter Example



All networks within the Accounting department are in Zone Accounting. A device hiding filter on Router C stops access from specific areas to the LaserWriter* printers within the Accounting zone.

When configuring this example, set the parameters as shown in Table 7 on page 66.

Table 7 Parameters for AppleTalk Device Hiding Filter Example

Parameter	Value
Action	Deny
Device Name	= (for all NBP names)
Device Type	LaserWriter
Device Location Type	Zone
Device Location	Accounting
User Location Type	Interface
User Location	FDDI Backbone-Interface connecting to FDDI
User Circuit	All Circuits

How to Configure AppleTalk Route Filtering

Before you begin, make sure that filtering support is enabled for AppleTalk in NIASCFG. Otherwise, filtering will not work.

To configure AppleTalk routing information filtering for incoming (or outgoing) route filters, complete the following steps:

1. Load FILTCFG, then select the following parameter path:

   Select Configure AppleTalk Filters > Incoming Route Filters (or Outgoing Route Filters)

2. Select Action and toggle the choice to permit or deny the routes listed in the filter list.

   This specifies the action taken with a route that appears in the filter list. If you select to permit routes, the AppleTalk router accepts (or advertises) only the routes from (or to) the networks in the filter list. If you select to deny routes, the AppleTalk router does not accept (or advertise) specific routes from (or to) specific networks in the filter list, but does accept (or advertise) all other entries in the routing table.

3. Select Filters .

   This lists the filters that are permitted or denied, according to the Action parameter setting.

4 Modify the filter list.

Select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new filter.

If you are modifying an existing filter or adding a filter, specify the following parameters in the Define Filter menu:

- Route to Network (or Route to Network or Zone)—Select All Routes , Non-extended Network , Multiple/Extended Network , or Zone as the type of route or network to be filtered.
- Network Number/Range —Enter a network number or a network range, depending on whether you selected a nonextended or an extended network. If you select an extended network, you can enter a single extended network or a range of extended and nonextended networks.
- Zone Name (Outgoing only)—Enter the zone name of the AppleTalk zone to be filtered.
- Source (or Destination) Type —Press Enter and select Interface , Interface Group , or AURP Tunnel .
- Source (or Destination)—Press Enter and select the interface or interface group from the list. This option does not apply for an AURP tunnel.

  If you specified Interface as the Source Type , select a specific interface on which you want to filter the service. You can select a LAN interface, a WAN interface, the internal network, or all interfaces. The default is All Interfaces .
- Source (or Destination) Circuit —If you selected a WAN circuit, press Enter to modify the following optional circuit information:

  Local Frame Relay DLCI # (for frame relay)—The DLCI circuit number used for calls.

  Remote System ID (for PPP, X.25, ISDN, or ATM)—The name of the remote system server or remote peer associated with this circuit.

  Circuit Parameter Type (for X.25 or ATM)—The type of virtual circuit used to establish a connection.

  Remote DTE Address (for X.25)—The X.121 DTE address assigned to the specific remote DTE.

  Remote ATM Address (for ATM)—The address assigned to the specific remote ATM.
- Comment —Enter an optional short description.

5. Press Esc and save the filter information.
6. Select Exceptions .

   This lists the exceptions to the filter list. Depending on the Action parameter setting, routes that match a filter on this list are always or are never permitted or denied, even if another filter is configured to do the opposite.
7. Modify the exceptions list.

   Select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new filter. Refer to Step 4 and Step 5 to modify or add a filter.
8. Select Status and toggle the choice to read Enabled or Disabled .

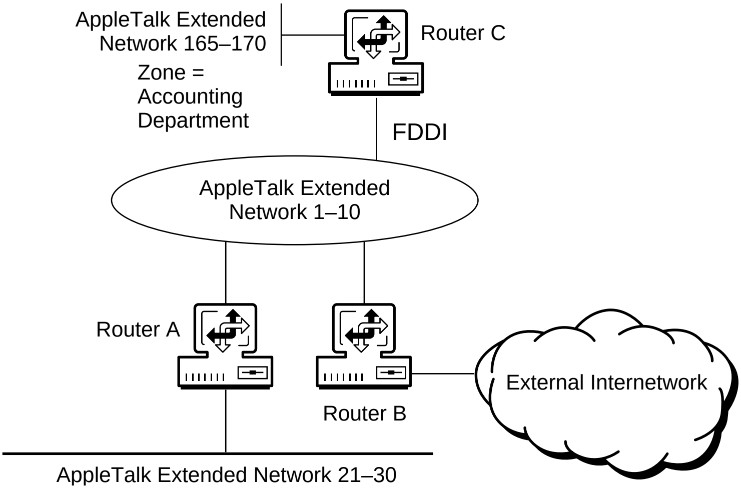
   Any configured filters immediately become active (enabled) or inactive (disabled).
9. Press Esc to save the information and return to the Configure AppleTalk Filters menu.

AppleTalk Outgoing Routing Information Filter Example

In the following example, the Accounting department is connected to the FDDI backbone by Router C. One of the AppleTalk networks within Accounting is 165-170. Because access to this network from outside the Accounting department is not required, the administrator has chosen not to propagate a route to this network outside the Accounting department. Figure 8 on page 69 shows the internetwork topology.

NOTE: When you configure a filter for a primary WAN call, an equivalent filter is automatically generated for the backup call. If the primary call should fail, the backup call is automatically connected.

Figure 8 AppleTalk Routing Information Filter Example



Extended network 165-170 can be hidden from the rest of the organization if an outgoing route filter is configured on Router C.

The route being hidden from the rest of the network is extended network 165-170. Router C's connection to the departments outside Accounting is through the FDDI backbone. The destination from which to hide the Accounting network is most easily defined as the interface to the backbone. Note that no node or server in the internetwork can see the Accounting network 165-170. However, nodes in Accounting can see the internetwork routes, but cannot see any devices on the internetwork.

When configuring this example, set the parameters as shown in Table 8.

Table 8 Parameters for AppleTalk Routing Information Filter Example

Parameter	Value
Action	Deny
Filtered Route:	.
Route to Network or Zone	Multiple/Extended Network
Network Number/Range	165-170
Destination Type	Interface
Destination	FDDI

Configuring Source Route Bridge Filters

Source route bridge supports the following two types of filters:

- Protocol ID filters
- Ring number filters

Refer to Chapter 1, “Understanding,” on page 9 for more information.

NOTE: When you configure a filter for a primary WAN call, an equivalent filter is automatically generated for the backup call. If the primary call fails, the backup call is automatically connected.

This section contains the following topics:

- “Configuring Protocol ID Filters” on page 70
- “Configuring Ring Number Filters” on page 71

Configuring Protocol ID Filters

To configure protocol ID filters, complete the following steps:

1. Load FILTCFG, then select the following parameter path:

   Select Configure Source Route Bridge Filters > Protocol ID Filters

2. Select Action and toggle the choice to permit or deny the packets in the filter list.

   This specifies the action taken with a packet that appears in the filter list. If you select to permit packets, the bridge accepts only the packets in the filter list. If you select to deny packets, the bridge does not accept the packets in the filter list.

3. Select Filters .

   This lists the packets that are permitted or denied, according to the Action parameter setting.

4. Modify the packet list.

   Select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new packet.

If you are modifying an existing filter or adding a new filter, specify the following parameters from the Define Filter menu:

- Source Interface —Press Enter and select an interface from the list of configured network interfaces. This specifies the network interface at which incoming data packets are filtered.
- Protocol ID —Press Enter and select a protocol ID from the list.

  Press F3 to modify a protocol ID. Press Ins to define a new protocol ID and supply the following information:

  NOTE: You cannot modify predefined protocol ID entries.

  Select Protocol ID Type —Select either LLC SAP or 802.2 SNAP, where LLC SAP is the original IEEE 802.2 1-byte protocol ID, and 802.2 SNAP is an expanded 5-byte protocol ID used with SNAP SAP.

  Name —Specify a unique name for the protocol ID.

  Value —For LLC SAP, enter a 1-byte (up to two hexadecimal digits) ID. For SNAP SAP, enter up to a 5-byte (10 hexadecimal digits) ID with a minimum value of 600 (hexadecimal).

  Comment —Enter an optional short description for the protocol ID.

  NOTE: All changes to the filter list take place immediately.

- Comment —Enter an optional short description.

5. Press Esc and save the filter information.
6. Select Status and toggle the choice to read Enabled or Disabled to specify the status of the protocol ID filters.

   Any configured filters immediately become active (enabled) or inactive (disabled).

7. Press Esc to return to the Configure Source Route Bridge Filters menu.

Configuring Ring Number Filters

To configure ring number filters, complete the following steps:

1. Load FILTCFG, then select the following parameter path:

   Select Configure Source Route Bridge Filters > Ring Numbers Filters

2. Select Status and toggle the choice to read Enabled or Disabled to specify the status of the ring number filters.

This displays the action taken when a packet matches a filter in the filter list. The only action possible is to select Deny Packets .

3 Select Filters .

This lists the packets that are permitted or denied, according to the Action parameter setting.

4 Modify the filter list.

Select a filter from the list and press Enter to modify the filter or Del to remove it. Press Ins to add a new filter.

If you are modifying an existing filter or adding a new filter, specify the following parameters from the Define Filter menu:

- Source Ring Number —Enter a number in the range of 1 to FFF (hexadecimal).
- Comment —Enter an optional short description.

5 Press Esc and save the filter information.

NOTE: All changes to the filter list take place immediately.

6 Press Esc to return to the Configure Source Route Bridge Filters menu.