



Cable ARP Filtering

This document describes the Cable ARP Filtering feature for the Cisco Cable Modem Termination System (CMTS). This feature enables service providers to filter Address Resolution Protocol (ARP) request and reply packets, to prevent a large volume of such packets from interfering with the other traffic on the cable network.

Feature History for Cable ARP Filtering

Release	Modification
12.2(15)BC2	This feature was introduced for the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.
12.2(15)BC2b	The ip-requests-filtered option was added to the service divert-rate-limit command to display the specific Service IDs (SIDs) that are generating or forwarding a minimum number of ARP packets.
12.3(9a)BC	Introduced optional syntax for the cable arp filter command, where <i>number</i> and <i>window-size</i> values are optional for reply-accept and request-send settings.
12.3(17a)BC	The show cable arp-filter command was introduced for the PXF ARP Filter feature. The service divert-rate-limit command was introduced. Default settings changed for two commands to result as follows: <ul style="list-style-type: none">• cable arp filter request-send 3 2• cable arp filter reply-accept 3 2

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Contents

- [Prerequisites for Cable ARP Filtering, page 2](#)
- [Restrictions for Cable ARP Filtering, page 2](#)
- [Information About Cable ARP Filtering, page 3](#)
- [How to Configure Cable ARP Filtering, page 7](#)
- [Configuration Examples for Cable ARP Filtering, page 19](#)
- [Additional References, page 22](#)
- [Command Reference, page 23](#)

Prerequisites for Cable ARP Filtering

- The Cisco uBR7246VXR or Cisco uBR10012 router must be running Cisco IOS Release 12.2(15)BC2 or a later release.

Restrictions for Cable ARP Filtering

Cisco uBR7100 Series Restrictions

- The Cable ARP Filtering feature is not supported on the Cisco uBR7100 series universal broadband routers.

Cisco uBR10012 Router Restrictions

- The Cisco uBR10012 router maintains ARP filtering statistics on the Performance Routing Engine (PRE) module. Statistics are viewed with the **show cable arp-filter** command for a specified interface. When a switchover event occurs, as in RPR+ Redundancy, these ARP filtering statistics are reset to zero.

Cisco uBR10012 PRE modules support the Route Processor Redundancy Plus (RPR+) feature in several Cisco IOS releases. Refer to the following document for additional information:

Route Processor Redundancy Plus for the Cisco uBR10012 Universal Broadband Router

http://www.cisco.com/en/US/products/hw/cable/ps2209/products_feature_guide09186a00801a24e0.html

- The Cable ARP Filter feature is not configurable per subinterface.

PXF ARP Filter Restrictions

- The PXF microcode must be enhanced to provide the rate limiting functionality for ARP filtering in PXF.
- ARP filtering in PXF is only supported on the Performance Routing Engine 2 (PRE2). For more information, refer to the “[ARP Filtering in PXF](#)” on page 5.
- The ARP Filter in PXF feature is not configurable per subinterface.

Information About Cable ARP Filtering

To configure the Cable ARP Filtering feature, you should understand the following concept:

- [Cable ARP Filtering Overview, page 3](#)
- [Filtering ARP Traffic, page 4](#)
- [Monitoring Filtered ARP Traffic, page 4](#)
- [Linksys Wireless-Broadband Router \(BEFW11S4\), page 4](#)
- [ARP Filtering in PXF, page 5](#)
- [PXF Divert-Rate-Limit, page 6](#)

Cable ARP Filtering Overview

Theft-of-service and denial-of-service (DNS) attacks have become increasingly common in cable broadband networks. In addition, virus attacks are becoming more common, and users are often unaware that their computers have become infected and are being used to continue the attacks on the network.

One sign that often appears during these attacks is an unusually high volume of Address Resolution Protocol (ARP) packets. The user or virus repeatedly issues ARP requests, trying to find the IP addresses of additional computers that might be vulnerable to attack.

ARP requests are broadcast packets, so they are broadcast to all devices on that particular network segment. In some cases, a router can also forward ARP broadcasts to an ARP proxy for further processing.

This problem is also made worse because some low-end routers commonly used by subscribers for home networks can also incorrectly respond to all ARP requests, which generates even more traffic. Until these customer premises equipment (CPE) devices can be upgraded with firmware that is compliant to the appropriate Request for Comments (RFC) specifications, service providers need to be able to deal with the incorrectly generated or forwarded traffic.

In addition, the Cisco CMTS router automatically monitors ARP traffic and enters the IP addresses found in ARP requests into its own ARP table, in the expectation that a device will eventually be found with that IP address. Unacknowledged IP addresses remain in the router's ARP table for 60 seconds, which means that a large volume of ARP traffic can fill the router's ARP table.

This process can create a large volume of ARP traffic across the network. In some situations, the volume of ARP requests and replies can become so great that it can throttle other traffic and occupy most of the Cisco CMTS router's processing time, hampering efforts by technicians to recover their network.

The router cannot use fast-switching to process ARP packets, but must instead forward them to the route processor (RP). Because of this, processing a large volume of ARP traffic can also prevent the router from handling normal traffic.

Filtering ARP Traffic

To control the volume of ARP traffic on a cable interface, you can configure the **cable arp filter** command to specify how many ARP packets are allowed per Service ID (SID) during a user-specified time period. You can configure separate thresholds for ARP request packets and for ARP reply packets.

When a cable interface is configured to filter ARP packets, it maintains a table of the number of ARP request or reply packets that have been received for each SID. If a SID exceeds the maximum number of packets during the window time period, the Cisco CMTS drops the packets until a new time period begins.

**Note**

If using bundled cable interfaces, the Cable ARP Filtering feature is configured on the master and slave interfaces separately. This allows you to configure the feature only on the particular interfaces that require it. In addition, you can configure the feature with different threshold values, allowing you to customize the feature for each interface's traffic patterns.

Monitoring Filtered ARP Traffic

After ARP filtering has been enabled on a cable interface, you can then use the **service divert-rate-limit** command to display the devices that are generating excessive amounts of ARP traffic. These devices could be generating this traffic for any of the following reasons:

- Cable modems that are running software images that are either not DOCSIS-compliant or that have been hacked to allow theft-of-service attacks.
- CPE devices that are either performing a theft-of-service or denial-of-service attack, or that have been infected with a virus that is searching for other computers that can be infected.
- Routers or other devices that mistakenly reply to or forward all ARP requests.

After identifying the specific devices that are generating this traffic, you can use whatever techniques are allowed by your service level agreements (SLAs) to correct the problem.

Linksys Wireless-Broadband Router (BEFW11S4)

The Linksys Wireless-B Broadband Router, Model number BEFW11S4 version 4 with 1.44.2 firmware, incorrectly sends its own ARP reply packet for every ARP request packet it receives, instead of replying only to the ARP requests that are specifically for itself. Customers with these routers should upgrade the firmware to the latest revision to fix this bug. To upgrade the firmware, please go to the download section on the Linksys website, at the following URL:

<http://www.linksys.com/Download>

For the release notes for the latest revision of the firmware, see the following URL on the Linksys website:

http://www.linksys.com/servlet/Satellite?childpagename=US%2FLayout&packedargs=c%3DL_Download_C2%26cid%3D1115417109974%26sku%3D1115416826220&pagename=Linksys%2FCommon%2FVisitorWrapper

**Note**

It is extremely important that non-compliant CPE devices be updated to firmware that correctly handles ARP and other broadcast traffic. Even one or two non-compliant devices on a segment can create a significant problem with dropped packets, impacting all of the other customers on that segment.

ARP Filtering in PXF

Cisco Release 12.3(17a)BC introduces a PXF component to the ARP filter feature. When enabled, this PXF component filters ARP packets for identified ARP offenders, decreasing the ARP punt rate and RP CPU usage. It also provides the user with clearer separation in ARP filtering by utilizing source MAC addresses instead of SIDs.

The filter logic now filters by source MAC address instead of by SID. Currently, the modem MAC addresses are excluded from having their ARPs filtered, but Multimedia Terminal Adapters (MTAs) and other non-offending CPEs can still (statistically) have ARPs filtered because all ARPs appear to come from the same SID. Therefore, filtering by source MAC address will isolate the filtering to the offensive devices. By doing so, a customer who has Voice-over-IP (VoIP) service via an MTA and an infected CPE will not have MTA issues while being contacted by the service provider in regards to the infected CPE.

ARP offenders will still be allowed to use ARP to avoid complete loss of Internet connectivity through their configured or provisioned gateway address. Because of this, it is expected that the “ARP Input” process will still show a few percentage points of CPU usage, but the net interrupt CPU usage will decrease.

**Note**

ARP filtering in PXF is only supported on the PRE2 and is enabled by default.

Filtering ARP Traffic in PXF

When ARP traffic in PXF is enabled, a lightweight algorithm executing on the RP is used to identify ARP offenders by the source MAC address or the SID. All offending source MAC addresses or SIDs are then programmed by the ARP Filter control module into the PXF ucode divert rate limiting module (ARP offenders are still allowed to perform ARP transactions, but only at the configured filtering rate).

Offending source MAC addresses or SIDs are filtered in PXF for a minimum of 50 minutes (ten 5-minute intervals with no occurring offenses). Utilizing the existing ARP Filter CLI tools, the cable operator can obtain enough information about the modem and CPE to contact the end user to request the necessary anti-virus software installation or firmware upgrade for the CPE.

**Note**

If the offending device is not “repaired” or shut off, it will remain in the PXF ARP Filter indefinitely.

The PXF ARP rate limiter is designed to filter a maximum of 16,000 ARP offenders. If this pool of 16,000 filterable entities is exhausted, then the entity is filtered on the RP. The CLI statistics will distinguish mac addresses filtered on the RP versus PXF.

Because of possible mac address hash collisions, ARP offenders that cannot be programmed into the PXF ARP rate limiter will still be filtered in PXF by SID. Since the hash is done by source mac address and SID, such devices can actually moved back to mac address filtering by deleting the associated modem and forcing it back online with a new SID (this merely a possibility and is not expected to be a common practice).

ARP packets with a source mac address that is not “known” to the CMTS as a modem or CPE will be filtered by their SID in PXF. Therefore, there will never be an unusual ARP packet source that will NOT be filtered in PXF. False ARP packets with invalid operation codes will be filtered as if they are an ARP Reply.



Note

ARP filtering in PXF is only supported on the PRE2.

PXF Divert-Rate-Limit

Diverted packets sent from the forwarding processor (FP) to the route processor (RP), via the FP-to-RP interface, may encounter congestion when packets requiring diversion arrive at the FP at a faster rate than they can be transmitted to the RP. When congestion occurs, valid packets in the FP-to-RP queues will be dropped. This situation can be deliberately caused by attacks directed at the CMTS or inadvertently by faulty external hardware.

PXF Divert-Rate-Limit identifies packet streams that will cause congestion of the FP-to-RP interface. Packets in the stream are dropped according to the configured rate-limiting parameters. Rate-limiting occurs before the packets are placed in the FP-to-RP queues, preventing valid packets in other streams from being dropped.

The following diverted packets will be rate-limited:

- fwd-glean—Packets that hit a glean adjacency in the Forwarding Information Base (FIB).
- rpf-glean—Packets that hit a glean adjacency during the Reverse Path Forwarding (RPF) check.

Packets that pass rate-limiting are diverted as they normally would be. Packets that fail rate-limiting are dropped.

Rate-limiting is implemented by a token-bucket algorithm. The token-bucket algorithm requires two variables: rate and limit. Both the rate and limit are configurable via the CLI. The rate is the average number of packets-per-second that pass the rate-limiting code. The limit can be thought of as the number of packets that will pass during an initial burst of packets.



Note

The Divert-Rate-Limit feature is always on and cannot be turned off. Using the **no** form of the configuration CLI returns the rate-limiting parameters to their default values. During a PXF and CPU switchover or reload, the configuration is retained, but not the statistics. Therefore, after switchover, the statistics shown by the **show pxf cpu statistics drl** command will show zero.

fwd-glean

IP packets that hit a glean adjacency in the FIB are diverted. There are three requirements:

- RPF-check has passed (if required).
- SV-check has passed (if required).
- Forward adjacency is glean.

Packets are rate-limited based on the destination IP address. A hash on the destination IP address is used to create an index that stores state information for rate-limiting. In the event of a hash collision, the pre-existing state information will be used and updated. The table that stores state information is large enough to make collisions rare.

rpf-glean

The RPF feature is modified to divert packets that hit a glean adjacency during the RPF check. A new `divert_code` will be created for this type of diverted packet. Currently, these packets are dropped.

There are four requirements:

- SV-check has passed (if required).
- RPF is enabled.
- The packet is from a non-load-balanced interface.
- RPF-adjacency is glean.

Packets are rate-limited based on the source IP address. A hash on the source IP address is used to create an index that stores state information for rate-limiting. In the event of a hash collision, the pre-existing state information will be updated. The table that stores state information is large enough to make collisions rare.

How to Configure Cable ARP Filtering

Use the following procedures to determine whether ARP filtering is required and to configure ARP filtering on one or more cable interfaces.

- [Monitoring ARP Processing, page 7](#)
- [Enabling ARP Filtering, page 9](#)
- [Identifying the Sources of Major ARP Traffic, page 10](#)
- [Clearing the Packet Counters, page 14](#)
- [Identifying ARP Offenders in PXF, page 15](#)
- [Configuring PXF Divert-Rate-Limit, page 17](#)

Monitoring ARP Processing

Use the following steps to monitor how the router is processing ARP traffic and whether the volume of ARP packets is a potential problem.

- Step 1** To discover the CPU processes that are running most often, use the **show process cpu sorted** command and look for the ARP Input process:

```
Router# show process cpu sorted
```

```
CPU utilization for five seconds: 99%/28%; one minute: 93%; five minutes: 90%
PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min  TTY Process
 19   139857888   44879804    3116  31.44% 28.84% 28.47% 0 ARP Input
 154   74300964   49856254    1490  20.29% 19.46% 15.78% 0 SNMP ENGINE
 91    70251936   1070352    65635   8.92%  9.62%  9.59% 0 CEF process
 56   17413012   97415887     178   3.01%  3.67%  3.28% 0 C10K BPE IP Enqu
 78   24985008   44343708     563   3.68%  3.47%  3.24% 0 IP Input
 54    6075792    6577800     923   0.90%  0.67%  0.65% 0 CMTS SID mgmt ta
...
```

In this example, the ARP Input process has used 31.44 percent of the CPU for the past five seconds. Total CPU utilization is also at 99 percent, indicating that a major problem exists on the router.

**Note**

As a general rule, the ARP Input process should use no more than one percent of CPU processing time during normal operations. The ARP Input process could use more processing time during certain situations, such as when thousands of cable modems are registering at the same time, but if it uses more than one percent of processing time during normal operations, it probably indicates a problem.

Step 2 To monitor only the ARP processes, use the **show process cpu | include ARP** command:

```
Router# show process cpu | include ARP

 19  139857888  44879804          3116 31.44% 28.84% 28.47%    0 ARP Input
110           0           1           0  0.00%  0.00%  0.00%    0 RARP Input
```

Step 3 To monitor the number of ARP packets being processed, use the **show ip traffic** command.

```
Router# show ip traffic | begin ARP

ARP statistics:
  Rcvd: 11241074 requests, 390880354 replies, 0 reverse, 0 other
  Sent: 22075062 requests, 10047583 replies (2127731 proxy), 0 reverse
```

Repeat this command to see how rapidly the ARP traffic increases.

Step 4 If ARP traffic appears to be excessive, use the **show cable arp-filter** command to display ARP traffic for each cable interface, to identify the interfaces that are generating the majority of the traffic.

```
Router# show cable arp-filter Cable5/0/0

ARP Filter statistics for Cable5/0/0:
  Rcvd Replies: 177387 total, 0 unfiltered, 0 filtered
  Sent Requests For IP: 68625 total, 0 unfiltered, 0 filtered
  Sent Requests Proxied: 7969175 total, 0 unfiltered, 0 filtered
```

In the above example, the unfiltered and filtered counters show zero, which indicates that ARP filtering has not been enabled on the cable interface. After ARP filtering has been enabled with the **cable arp filter** command, you can identify the specific devices that are generating excessive ARP traffic by using the **service divert-rate-limit** command (see the “Identifying the Sources of Major ARP Traffic” section on page 10).

Enabling ARP Filtering

Use the following procedure to enable ARP filtering on a particular cable interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *x/y*
4. **cable arp filter reply-accept** *number window-size*
5. **cable arp filter request-send** *number window-size*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface cable <i>x/y</i> Example: Router(config)# interface cable 5/1	Enters interface configuration mode for the specified cable interface.
Step 4	cable arp filter reply-accept <i>number window-size</i> Example: Router(config-if)# cable arp filter reply-accept 2 2	Configures the cable interface to accept only the specified <i>number</i> of ARP reply packets every <i>window-size</i> seconds for each active Service ID (SID) on that interface. The cable interface drops ARP reply packets for a SID that would exceed this number. (The default behavior is to accept all ARP reply packets.) <ul style="list-style-type: none"> • <i>number</i> = Number of ARP reply packets that is allowed for each SID within the window time period. The allowable range is 0 to 20 packets, with a default of 4 packets. If <i>number</i> is 0, the cable interface drops all ARP reply packets. • <i>window-size</i> = Size of the window time period, in seconds, in which to monitor ARP replies. The valid range is 1 to 5 seconds, with a default of 2 seconds.

	Command or Action	Purpose
Step 5	<pre>cable arp filter request-send number window-size</pre> <p>Example: Router(config-if)# cable arp filter request-send 3 1</p>	<p>Configures the cable interface to send only the specified <i>number</i> of ARP request packets every <i>window-size</i> seconds for each active SID on that interface. The cable interface drops ARP requests for a SID that would exceed this number. (The default behavior is to send all ARP request packets.)</p> <ul style="list-style-type: none"> <i>number</i> = Number of ARP request packets that is allowed for each SID within the window time period. The allowable range is 0 to 20 packets, with a default of 4 packets. If <i>number</i> is 0, the cable interface does not send any ARP request packets. <i>window-size</i> = Size of the window time period, in seconds, in which to monitor ARP requests. The valid range is 1 to 5 seconds, with a default of 2 seconds.
	<p>Note Repeat Step 3 through Step 5 to enable ARP filtering on other cable interfaces. Master and slave interfaces in a cable bundle must be configured separately.</p>	
Step 6	<pre>end</pre> <p>Example: Router(config-if)# end</p>	<p>Exits interface configuration mode and returns to privileged EXEC mode.</p>

Identifying the Sources of Major ARP Traffic

After you have begun filtering ARP traffic on a cable interface, use the following procedure to identify the cable modems or CPE devices that are generating or forwarding major amounts of ARP traffic.



Tip

The Linksys Wireless-B Broadband Router, Model number BEFW11S4 version 4 with 1.44.2 firmware, has a known problem in which it incorrectly generates an ARP reply for every ARP request packet it receives. See the [“Linksys Wireless-Broadband Router \(BEFW11S4\)”](#) section on page 4 for information on how to resolve this problem.

DETAILED STEPS

- Step 1** To discover the devices that are responsible for generating or forwarding more ARP requests on a specific cable interface than a specified minimum number of packets, use the **show cable arp-filter requests-filtered** command where *number* is the threshold value for the number of packets being generated:

```
show cable arp-filter cable interface requests-filtered number
```

For example, to display the devices that have generated more than 100 ARP request packets, enter the following command:

```
Router# show cable arp-filter cable 5/1/0 requests-filtered 100
```

Sid	MAC Address	IP Address	Req-Filtered	Req-For-IP-Filtered	Rep-Filtered
1	0006.2854.72d7	10.3.81.4	12407	0	0
81	00C0.c726.6b14	10.3.81.31	743	0	0

- Step 2** Repeat this command to show how quickly the devices are generating the ARP packets.
- Step 3** To discover the devices that are responsible for generating or forwarding more ARP replies on a specific cable interface than a specified minimum number of packets, use the **show cable arp-filter replies-filtered** command where *number* is the threshold value for the number of packets being generated:

```
show cable arp-filter cable interface replies-filtered number
```

For example, to display the devices that have generated more than 200 ARP reply packets, enter the following command:

```
Router# show cable arp-filter c5/0/0 replies-filtered 200
```

Sid	MAC Address	IP Address	Req-Filtered	Req-For-IP-Filtered	Rep-Filtered
2	0006.53b6.562f	10.11.81.16	0	0	2358
191	0100.f31c.990a	10.11.81.6	0	0	11290

- Step 4** (Optional) If a particular cable modem is generating or forwarding excessive ARP replies, contact the customer to see if they are using a Linksys Wireless-B Broadband Router, Model number BEFW11S4. If so, this router could be running old firmware that is incorrectly generating excessive ARP packets, and the customer should upgrade their firmware. For more information, see the [“Linksys Wireless-Broadband Router \(BEFW11S4\)”](#) section on page 4.
- Step 5** Repeat this command during each filter period (the time period you entered with the **cable arp filter** command) to show how quickly the devices are generating the ARP packets.
- Step 6** (Optional) The ARP reply and request packet counters are 16-bit counters, so if a very large number of packets are being generated on an interface, these counters could wrap around to zero in a few hours or even a few minutes. Clearing the ARP counters eliminates stale information from the display and makes it easier to see the worst offenders when you suspect ARP traffic is currently creating a problem on the network.

To eliminate the modems that are not currently triggering the ARP filters and to isolate the worst current offenders, use the **clear counters cable interface** command to reset all of the interface counters to zero. Then the **show cable arp-filter** commands clearly identify the SIDs of the modems that are currently forwarding the most ARP traffic.

For example, the following example indicates that a number of modems are forwarding a large enough volume of ARP traffic that they have triggered the ARP packet filters:

```
Router# show cable arp-filter cable 5/1/0 requests-filtered 10
```

Sid	MAC Address	IP Address	Req-Filtered	Req-For-IP-Filtered	Rep-Filtered
1	0006.2854.72d7	10.3.81.4	8	0	0
23	0007.0e02.b747	10.3.81.31	32	0	0
57	0007.0e03.2c51	10.3.81.31	12407	0	0
...					
81	00C0.c726.6b14	10.3.81.31	23	0	0

SID 57 shows the largest number of packets, but it is not immediately apparent if this modem is causing the current problems. After clearing the counters though, the worst offenders are easily seen:

```
Router# clear counter cable 5/1/0
```

```
Clear "show interface" counters on this interface [confirm] y
```

```
08:17:53.968: %CLEAR-5-COUNTERS: Clear counter on interface Cable5/1/0 by console
```

```

Router# show cable arp cable 5/1/0

ARP Filter statistics for Cable3/0:
  Replies Rcvd: 0 total. 0 unfiltered, 0 filtered
  Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered
  Requests Forwarded: 0 total. 0 unfiltered, 0 filtered

Router# show cable arp-filter cable 5/1/0 requests-filtered 10

Sid  MAC Address      IP Address      Req-Filtered  Req-For-IP-Filtered  Rep-Filtered
-----
Router# show cable arp-filter cable 5/1/0 requests-filtered 10

Sid  MAC Address      IP Address      Req-Filtered  Req-For-IP-Filtered  Rep-Filtered
-----
57   0007.0e03.2c51  10.3.81.31     20            0                    0
81   00C0.c726.6b14  10.3.81.31     12            0                    0

Router# show cable arp-filter cable 5/1/0 requests-filtered 10

Sid  MAC Address      IP Address      Req-Filtered  Req-For-IP-Filtered  Rep-Filtered
-----
57   0007.0e03.2c51  10.3.81.31     31            0                    0
81   00C0.c726.6b14  10.3.81.31     18            0                    0

```

Step 7 (Optional) If the Req-For-IP-Filtered column shows the majority of ARP packets, use the **show cable arp-filter ip-requests-filtered** command to display more details about the CPE device that is generating this traffic. Then use the **debug cable mac-address** and **debug cable arp filter** commands to display detailed information about this particular traffic; for example:

```

Router# show cable arp-filter c5/0/0 ip-requests-filtered 100

Sid  MAC Address      IP Address      Req-Filtered  Req-For-IP-Filtered  Rep-Filtered
-----
1    0007.0e03.1f59  50.3.81.3     0              37282              0

Router# debug cable mac-address 0007.0e03.1f59
Router# debug cable arp filter
Router#

Apr 23 23:03:23.565: ARP for IP Filter=F sid 1 s 0000.0000.0049 d 0005.00e5.3610 sip
50.3.81.13 dip 50.3.82.173 prot 6 len 46 SrcP 445 DstP 445

Apr 23 23:03:23.565: ARP for IP Filter=F sid 1 s 0000.0000.0049 d 0005.00e5.3610 sip
50.3.81.13 dip 50.3.82.174 prot 6 len 46 SrcP 445 DstP 445

Apr 23 23:03:23.565: ARP for IP Filter=F sid 1 s 0000.0000.0049 d 0005.00e5.3610 sip
50.3.81.13 dip 50.3.82.175 prot 6 len 46 SrcP 445 DstP 445

[additional output omitted]...

```

This example shows that the CPE device at IP address 50.3.81.13 is sending packets to TCP port 445 to every IP address on the 50.3.82.0 subnet, in a possible attempt to find a computer that has Microsoft Windows file-sharing enabled.

Step 8 After determining the specific devices that are generating excessive ARP traffic, you can take whatever action is allowed by your company's service level agreements (SLAs) to correct the problem.

Examples

In this example, two cable interfaces, C5/0/0 and C7/0/0, are joined in the same bundle, which means the interfaces share the same broadcast traffic. Separate devices on each interface are generating excessive ARP traffic:

- The device at MAC address 000C.2854.72D7 on interface C7/0/0 is generating or forwarding a large volume of ARP requests. Typically, this device is a cable modem that is forwarding the ARP requests that are being generated by a CPE device behind the modem. The CPE device could be attempting a theft-of-service or denial-of-service attack, or it could be a computer that has been infected by a virus and is trying to locate other computers that can be infected.
- The device at MAC address 000C.53B6.562F on Cable 5/0/0 is responding to a large number of ARP requests, which could indicate that the device is a router that is running faulty software.

The following commands identify the device on the C7/0/0 interface that is generating the excessive ARP requests:

```
Router# show cable arp-filter c7/0/0

ARP Filter statistics for Cable7/0/0:
  Replies Rcvd: 3 total. 3 unfiltered, 0 filtered
  Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered
  Requests Forwarded: 27906 total. 562 unfiltered, 27344 filtered
```

```
Router# show cable arp-filter c7/0/0 requests-filtered 100
```

Sid	MAC Address	IP Address	Req-Filtered	Req-For-IP-Filtered	Rep-Filtered
1	000C.2854.72d7	50.3.81.4	62974	0	0

The following commands identify the device on the C5/0/0 interface that is generating the excessive ARP replies:

```
Router# show cable arp-filter c5/0/0

ARP Filter statistics for Cable5/0/0:
  Replies Rcvd: 2400 total. 456 unfiltered, 1944 filtered
  Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered
  Requests Forwarded: 26 total. 26 unfiltered, 0 filtered
```

```
Router# show cable arp-filter c5/0/0 replies-filtered 100
```

Sid	MAC Address	IP Address	Req-Filtered	Req-For-IP-Filtered	Rep-Filtered
2	000C.53b6.562f	50.3.81.6	0	0	2097

Clearing the Packet Counters

To clear the packet counters on an interface, which includes the ARP packet counters, use the **clear counters cable interface** command. You can also clear the packet counters on all interfaces by using the **clear counters** command without any options. This allows you to use the **show cable arp** commands to display only the CPE devices that are currently generating the most traffic.

The following example shows the ARP packet counters being cleared:

```
Router# show cable arp cable 3/0

ARP Filter statistics for Cable3/0:
  Replies Rcvd: 3278 total. 84 unfiltered, 3194 filtered
  Requests Sent For IP: 941 total. 30 unfiltered, 911 filtered
  Requests Forwarded: 941 total. 37 unfiltered, 904 filtered

Router# show cable arp cable 3/0 replies-filtered 1

Sid  MAC Address      IP Address      Req-Filtered    Req-For-IP-Filtered  Rep-Filtered
2    0006.2854.71e7  50.3.72.2      1815           0                    3194

Router# show cable arp cable 3/0 requests-filtered 1

Sid  MAC Address      IP Address      Req-Filtered    Req-For-IP-Filtered  Rep-Filtered
2    0006.2854.71e7  50.3.72.2      1815           0                    3194

Router# clear counter cable 3/0
Clear "show interface" counters on this interface [confirm] y

22:38:45.875: %CLEAR-5-COUNTERS: Clear counter on interface Cable3/0 by console

Router# show cable arp cable 3/0

ARP Filter statistics for Cable3/0:
  Replies Rcvd: 0 total. 0 unfiltered, 0 filtered
  Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered
  Requests Forwarded: 0 total. 0 unfiltered, 0 filtered

Router# show cable arp cable 3/0 replies-filtered 1

Sid  MAC Address      IP Address      Req-Filtered    Req-For-IP-Filtered  Rep-Filtered

Router# show cable arp cable 3/0 requests-filtered 1

Sid  MAC Address      IP Address      Req-Filtered    Req-For-IP-Filtered  Rep-Filtered
```



Note

The **clear counters** command clears all of the packet counters on an interface, not just the ARP packet counters.

Identifying ARP Offenders in PXF

When the PXF ARP Filter feature is enabled, use the **sho cable arp-filter interface** command to generate a list of ARP offenders.

The following example shows a list of ARP offenders being generated:

```
Router# sho cable arp-filter ?
  Bundle  Cable Virtual bundle interface
  Cable   CMTS interface

uBR-15#sho cable arp-filter Bundle1 ?
  ip-requests-filtered  Show modems with arp request for IP packet filter count
                        at or above x
  replies-filtered     Show modems with arp reply filter count at or above x
  requests-filtered    Show modems with arp request filter count at or above x
  |                    Output modifiers
<cr>
```

The following is a sample output from the CLI:

```
Router# sho cable arp-filter Bundle1 requests-filtered 40

Interface Cable5/0/0 - none
Interface Cable6/0/2
Sid  MAC Address      IP Address      Req-Filtered  Req-For-IP-Filtered  Rep-Filtered
4    0007.0e03.9cad 50.3.81.15     46            0                    0
Interface Cable7/0/0 - none
```

PRE2 Outputs in PXF

When the PXF ARP Filter feature is enabled, the PRE2 output formatting displays the modem and the CPE addresses on a single line, in addition to the following columns:

- **M/S**—This column shows if packets are being filtered by MAC address or SID. A majority of these columns will show MAC address.
- **Rate**—This column shows the packet rate for PXF-filtered packets in the last 5 minutes monitoring time window. Rate is not calculated for RP-filtered packets.
- **Pro**—This column will identify the processor that performed the filtering with either “RP” or “PXF.” On the PRE2, it is expected that 99.9% of Pro fields will show “PXF.”

The following is a sample output for an ARP request on a PRE2 in PXF:

```
Router# sho cable arp-filter Bundle1 requests-filtered 40

Interface Cable5/0/0 - none
Interface Cable6/0/2
Sid  CPE Mac          CPE IP          Modem MAC        Modem IP          M/S Rate Pro REQS
4    00d0.b75a.822a 50.3.81.56      0007.0e03.9cad 50.3.81.15       MAC -   RP 46
5    00d0.b75a.822a 50.3.81.56      0007.0e03.9cad 50.3.81.15       MAC 25  PXF 5012
6    00b0.d07c.e51d 50.3.81.57      0007.0e03.1f59 50.3.81.13       MAC -   RP 64000
7    -                -                0006.2854.7347 50.3.81.4        MAC 101 PXF 5122
8    -                -                0006.2854.72d7 50.3.81.11       SID -   PXF 961205
Interface Cable7/0/0 - none
```

This sample output demonstrates the following:

- SID 4 shows a CPE filtered in PXF. The threshold specified is low enough to show the packets that were filtered on the RP as the offender was being identified. A high enough threshold would not have shown the RP-filtered packets. The ARP packet rate of 25 is shown for PXF-filtered packets.
- SID 5 shows a CPE filtered on the RP. This is extremely unusual and only occurs when the maximum number of PXF-filterable entities has been reached.
- SID 6 shows a modem filtered in PXF (CPE MAC or CPE IP are not shown).
- SID 7 shows ARP packets from an “unknown” source MAC address filtered by SID in PXF.

The counts for requests, replies, and requests for IP will no longer be shown on a single line in order to keep the line concise and less than 90 characters in length.

The “REQs” column is now stated as “REPs” in the case of ARP replies. The column will show “REQ-IP” in cases involving ARP requests for IP.

Requests being sent by the CMTS due to encroaching IP packets, “ip-requests-filtered”, will still be filtered on the RP and not in PXF, with Access Control Lists (ACLs) used to defeat IP-based scanning traffic, and the IP punt rate limiting feature for PRE2 used to decrease the punt rate for such traffic. The ARP Filter can still be used to perform analysis of these IP traffic streams.

PRE1 and Cisco 7246 Outputs in PXF

When the PXF ARP Filter is enabled, the PRE1 and Cisco 7246 output for the **show** commands is simplified to exclude all columns that do not apply.

The following is a sample output for an ARP request on a PRE1 or 7246 in PXF:

```
Router# sho cable arp-filter Bundle1 requests-filtered 40

Interface Cable5/0/0 - none
Interface Cable6/0/2
Sid  CPE Mac          CPE IP          Modem MAC      Modem IP      M/S REQs
4    00d0.b75a.822a    50.3.81.56     0007.0e03.9cad 50.3.81.15    MAC 5058
5    00b0.d07c.e51d    50.3.81.57     0007.0e03.1f59 50.3.81.13    MAC 64000
6    -                 -              0006.2854.7347 50.3.81.4     MAC 5122
7    -                 -              0006.2854.72d7 50.3.81.11    SID 961205
Interface Cable7/0/0 - none
```

Configuring PXF Divert-Rate-Limit


Use the following procedure to configure Divert-Rate-Limit packet streams to identify potential congestion of the FP-to-RP interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *x/y*
4. **service divert-rate-limit** *divert-code rate limit*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface cable <i>x/y</i> Example: Router(config)# interface cable 5/1	Enters interface configuration mode for the specified cable interface.

	Command or Action	Purpose
Step 4	<p>service divert-rate-limit <i>divert-code rate limit</i></p> <p>Example: Router(config-if)# service divert-rate-limit fib-rp-glean 10 limit 20</p> <p>or</p> <p>Router(config-if)# service divert-rate-limit fib-rpf-glean 10 limit 20</p>	<p>Configures the Divert-Rate-Limit for the following packets:</p> <ul style="list-style-type: none"> • fwd-glean—Packets that hit a glean adjacency in the FIB. • rpf-glean—Packets that hit a glean adjacency during the RPF check. <p>The <i>rate</i> is the average number of packets-per-second that pass the rate-limiting code. The minimum rate is 1 packet-per-second and the maximum rate is 255 packets-per-second. The default rate is 20 packets-per-second.</p> <p>The minimum limit is 4 packets, and the maximum limit is 255 packets. The default limit is 5 packets.</p> <p> Note Using the no form of the service divert-rate-limit command will reset the rate and limit to the default values.</p>
Step 5	<p>end</p> <p>Example: Router(config-if)# end</p>	<p>Exits interface configuration mode and returns to privileged EXEC mode.</p>

Configuration Examples for Cable ARP Filtering

This section provides the following examples of how to configure the Cable ARP Filtering feature:

- [ARP Filtering Configuration on an Individual Cable Interface: Example, page 19](#)
- [ARP Filtering Configuration on Bundled Cable Interfaces: Example, page 20](#)

ARP Filtering Configuration on an Individual Cable Interface: Example

The following example shows a typical configuration of a cable interface that is configured for the Cable ARP Filtering feature:

```

!
interface Cable5/0/0
 ip address 192.168.100.1 255.255.255.0 secondary
 ip address 192.168.110.13 255.255.255.0
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream channel-id 0
 cable upstream 0 frequency 6000000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000 200000
 cable upstream 0 minislots-size 16
 cable upstream 0 modulation-profile 6 7
 no cable upstream 0 shutdown
 cable upstream 1 frequency 26000000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000 200000
 cable upstream 1 minislots-size 4
 cable upstream 1 modulation-profile 6 7
 no cable upstream 1 shutdown
 cable upstream 2 frequency 15008000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000 200000
 cable upstream 2 minislots-size 4
 cable upstream 2 modulation-profile 6 7
 cable upstream 2 shutdown
 cable upstream 3 spectrum-group 25
 cable upstream 3 channel-width 3200000 200000
 cable upstream 3 minislots-size 4
 cable upstream 3 modulation-profile 1
 cable upstream 3 shutdown
 cable upstream 4 frequency 21008000
 cable upstream 4 power-level 0
 cable upstream 4 channel-width 3200000 200000
 cable upstream 4 minislots-size 16
 cable upstream 4 modulation-profile 1
 no cable upstream 4 shutdown
 cable upstream 5 spectrum-group 25
 cable upstream 5 channel-width 3200000 200000
 cable upstream 5 minislots-size 4
 cable upstream 5 modulation-profile 1
 cable upstream 5 shutdown
 cable arp filter request-send 4 2
 cable arp filter reply-accept 4 2
end

```

ARP Filtering Configuration on Bundled Cable Interfaces: Example

The following example shows a typical configuration of a cable interface bundle that is also using the Cable ARP Filtering feature. Both the master and slave interface are configured separately, allowing you to configure the feature only on the particular interfaces that require it. In addition, you can configure the feature with different threshold values, allowing you to customize the feature for each interface's traffic patterns.

```

!
interface Cable5/0/0
  description Master cable interface
  ip address 10.3.130.1 255.255.255.0 secondary
  ip address 10.3.131.1 255.255.255.0 secondary
  ip address 10.3.132.1 255.255.255.0 secondary
  ip address 10.3.133.1 255.255.255.0 secondary
  ip address 10.3.81.1 255.255.255.0
  ip helper-address 10.14.0.4
  load-interval 30
  cable bundle 1 master
  cable downstream annex B
  cable downstream modulation 64qam
  cable downstream interleave-depth 32
  cable downstream frequency 441000000
  cable downstream channel-id 0
  cable upstream 0 frequency 5008000
  cable upstream 0 power-level 0
  cable upstream 0 channel-width 1600000
  cable upstream 0 minislots-size 4
  cable upstream 0 modulation-profile 1
  no cable upstream 0 shutdown
  cable upstream 1 channel-width 1600000
  cable upstream 1 minislots-size 4
  cable upstream 1 modulation-profile 1
  cable upstream 1 shutdown
  cable upstream 2 channel-width 1600000
  cable upstream 2 minislots-size 4
  cable upstream 2 modulation-profile 1
  cable upstream 2 shutdown
  cable upstream 3 channel-width 1600000
  cable upstream 3 minislots-size 4
  cable upstream 3 modulation-profile 1
  cable upstream 3 shutdown
  cable arp filter request-send 4 2
  cable arp filter reply-accept 4 2
!
interface Cable7/0/0
  description Slave cable interface--Master is C5/0/0
  no ip address
  cable bundle 1
  cable downstream annex B
  cable downstream modulation 64qam
  cable downstream interleave-depth 32
  cable downstream frequency 562000000
  cable downstream channel-id 0
  no cable downstream rf-shutdown
  cable upstream 0 connector 0
  cable upstream 0 frequency 5008000
  cable upstream 0 power-level 0
  cable upstream 0 channel-width 1600000
  cable upstream 0 minislots-size 4
  cable upstream 0 modulation-profile 21
  no cable upstream 0 shutdown

```

```
cable upstream 1 connector 1
cable upstream 1 channel-width 1600000
cable upstream 1 minislots-size 4
cable upstream 1 modulation-profile 21
cable upstream 1 shutdown
cable upstream 2 connector 2
cable upstream 2 channel-width 1600000
cable upstream 2 minislots-size 4
cable upstream 2 modulation-profile 21
cable upstream 2 shutdown
cable upstream 3 connector 3
cable upstream 3 channel-width 1600000
cable upstream 3 minislots-size 4
cable upstream 3 modulation-profile 21
cable upstream 3 shutdown
cable arp filter request-send 20 5
cable arp filter reply-accept 20 5
end
```

ARP Filtering in PXF Default Configuration: Example

The following example shows the default configuration of a cable interface for the ARP Filtering in PXF feature.

```
interface Bundle1
  cable arp filter request-send 3 2
  cable arp filter reply-accept 3 2
end
```

Additional References

The following sections provide references related to the Cable ARP Filtering feature.

Related Documents

Related Topic	Document Title
CMTS Commands	<i>Cisco Broadband Cable Command Reference Guide</i> , at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/bbcmref/index.htm
Cisco IOS Release 12.2 Commands	<i>Cisco IOS Release 12.2 Configuration Guides and Command References</i> , at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

Standards

Standards	Title
SP-RFIV1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 (http://www.cablemodem.com)

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 826	<i>An Ethernet Address Resolution Protocol (ARP)</i>
RFC 2665	<i>DOCSIS Ethernet MIB Objects Support</i>
RFC 2669	<i>Cable Device MIB</i>

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

- [cable arp filter](#)
- [debug cable arp filter](#)
- [service divert-rate-limit](#)
- [sho cable arp-filter](#)
- [service divert-rate-limit](#)

cable arp filter

To control the number of Address Resolution Protocol (ARP) packets that are allowable for each Service ID (SID) on a cable interface, use the **cable arp** command in cable interface configuration mode. To stop the filtering of ARP broadcasts for CMs, use the **no** form of this command.

cable arp filter { **reply-accept** [*number window-size*] | **request-send** [*number window-size*]}

no cable arp filter { **reply-accept** | **request-send** }

default cable arp filter { **reply-accept** | **request-send** }

Syntax Description

reply-accept <i>number window-size</i>	<p>Configures the cable interface to accept only the specified <i>number</i> of ARP reply packets every <i>window-size</i> seconds for each active Service ID (SID) on that interface. The cable interface drops ARP reply packets for a SID that would exceed this number.</p> <ul style="list-style-type: none"> <i>number</i> = (Optional) Number of ARP reply packets that is allowed for each SID within the window time period. The allowable range is 0 to 20 packets, with a default of 4 packets. If <i>number</i> is 0, the cable interface drops all ARP reply packets. <i>window-size</i> = (Optional) Size of the window time period, in seconds, in which to monitor ARP replies. The valid range is 1 to 5 seconds, with a default of 2 seconds. <p>Starting with Cisco IOS Release 12.3(9a)BC and later releases, the values for <i>number</i> and <i>window-size</i> are optional for reply-accept and request-send keywords in the syntax above. In prior supported Cisco IOS releases, these arguments are required for CLI syntax.</p> <p>In Cisco IOS Release 12.3(17a)BC and later releases, the default values for the <i>number</i> and <i>window-size</i> are changed from 4 and 2 respectively to 3 and 2:</p> <ul style="list-style-type: none"> cable arp filter request-send 3 2 cable arp filter reply-accept 3 2 <p>These remain optional for reply-accept and request-send keywords in the syntax above</p>
request-send <i>number window-size</i>	<p>Configures the cable interface to send only the specified <i>number</i> of ARP request packets every <i>window-size</i> seconds for each active SID on that interface. The cable interface drops ARP requests for a SID that would exceed this number.</p> <ul style="list-style-type: none"> <i>number</i> = (Optional) Number of ARP request packets that is allowed for each SID within the window time period. The allowable range is 0 to 20 packets, with a default of 4 packets. If <i>number</i> is 0, the cable interface does not send any ARP request packets. <i>window-size</i> = (Optional) Size of the window time period, in seconds, in which to monitor ARP requests. The valid range is 1 to 5 seconds, with a default of 2 seconds.

Defaults

ARP packets are not filtered by default, which means the Cisco CMTS router accepts all ARP reply packets and sends all ARP request packets.

When ARP filtering is enabled in Cisco IOS Release 12.3(9a)BC and earlier supporting releases, the default values are as follows:

- **cable arp filter request-send 4 2**
- **cable arp filter reply-accept 4 2**

When ARP filtering is enabled in Cisco IOS Release 12.3(17a)BC and later releases, the default values for the *number* and *window-size* are changed from 4 and 2 respectively to 3 and 2:

- **cable arp filter request-send 3 2**
- **cable arp filter reply-accept 3 2**

Command Modes

Cable interface

Command History

Release	Modification
12.2(15)BC2	This command was introduced for the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.
12.3(9a)BC	Introduced optional syntax for the cable arp filter command, where <i>number</i> and <i>window-size</i> values are optional for reply-accept and request-send settings.
12.3(17a)BC	Default settings changed for two commands to result as follows: <ul style="list-style-type: none"> • cable arp filter request-send 3 2 • cable arp filter reply-accept 3 2

Usage Guidelines

Viruses, worms, and theft-of-service attacks can generate a large volume of ARP requests on a cable interface. In some situations, the volume of ARP traffic can become so large that it throttles all other traffic.

To control the number of ARP replies and ARP requests that are allowed for each SID on a cable interface, use the **cable arp filter** command. This command configures the interface so that it accepts only a certain number of ARP reply or request packets per a specified time period. If a SID generates more ARP packets than what is allowed, the cable interface drops the excessive traffic.

By default, no ARP filtering is done. ARP filtering is enabled on individual cable interfaces, and you can choose to filter ARP packets only on the specific cable interfaces that require it. You can further choose to filter only ARP request packets, only ARP reply packets, or both. You can configure different threshold values on each interface, allowing you to customize the feature for each interface's traffic patterns.

If using bundled cable interfaces, the Cable ARP Filtering feature is configured separately on the master and slave interfaces. This allows you to configure the feature only on the particular interfaces that require it.

**Tip**

Disabling the Cable ARP Filtering feature, using the **no cable arp filter** command, does not reset the ARP packet counters. The ARP packet counters do not increment when Cable ARP Filtering is disabled, but the counters retain their current values until the interface counters are specifically cleared using the **clear counters** command.

Linksys Wireless-B BEFW11S4 Router

The Linksys Wireless-B Broadband Router, Model number BEFW11S4 version 4 with 1.44.2 firmware, incorrectly sends its own ARP reply packet for every ARP request packet it receives, instead of replying only to the ARP requests that are specifically for itself. Customers with these routers should upgrade the firmware to the latest revision to fix this bug. To upgrade the firmware, please go to the download section on the Linksys website, at the following URL:

<http://www.linksys.com/Download>

Examples

The following example shows how to filter cable ARP reply packets, so that the cable interface accepts a maximum of 15 ARP replies every three seconds per SID:

```
Router(config)# interface cable 5/1/0
Router(config-if)# cable arp filter reply-accept 15 3
```

The following example shows how to filter cable ARP request packets, so that the cable interface sends a maximum of 10 requests per second per SID:

```
Router(config)# interface cable 6/0
Router(config-if)# cable arp filter request-send 10 1
```

The following example shows how to enable the filtering of cable ARP request and reply packets on a cable interface, using the default values of 4 packets per CPE per every 2 seconds:

```
Router(config)# interface cable 3/0
Router(config-if)# default cable arp filter reply-accept
Router(config-if)# default cable arp filter request-send
Router(config-if)# end
Router# show running-config | include filter
```

```
cable arp filter reply-accept 4 2
cable arp filter request-send 4 2
```

The following example shows how to disable the filtering of cable ARP request and reply packets on a cable interface:

```
Router(config)# interface cable 1/0
Router(config-if)# no cable arp filter reply-accept
Router(config-if)# no cable arp filter request-send
```

Related Commands	Command	Description
	cable arp	Activates cable Address Resolution Protocol (ARP).
	cable proxy-arp	Activates cable proxy ARP on the cable interface.
	clear arp	Clears the ARP table on the router.
	clear counters	Clears the packet counters on all interfaces or on a specific interface.
	debug cable arp filter	Displays debugging messages about the filtering of ARP broadcasts.
	service divert-rate-limit	Displays the total number of ARP replies and requests that have been sent and received, including the number of requests that have been filtered.

debug cable arp filter

To display debugging messages about the filtering of Address Resolution Protocol (ARP) broadcasts, use the **debug cable arp filter** command in privileged EXEC mode. To stop the debugging messages, use the **no** form of this command.

debug cable arp filter

no debug cable arp filter

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(15)BC2	This command was introduced for the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.

Usage Guidelines

If you suspect a particular CM is generating a large volume of ARP traffic, you can enable debugging for that particular CM using the **debug cable arp** command. If the ARP traffic is excessive, you can enable ARP filtering on the associated cable interface using the **cable arp filter** command. To show the results of that ARP filtering, use the **debug cable arp filter** command.

**Tip**

Because this command can produce a large volume of debug information, it does not produce any output until you first limit debugging output to a particular Service ID (SID) or one or more particular CM MAC addresses, using the **debug cable interface sid** or **debug cable mac-address** commands, respectively.

Examples

The following example shows how to enable debugging messages for ARP filtering for a particular MAC address, and samples of the typical messages that can be displayed:

```
Router# debug cable mac-address 000C.0102.0304
Router# debug cable arp filter

CMTS arp filter debugging is ON

Router#

ARP Req Filter = T shdw 000C.0102.0304 sip 10.11.13.1 dhdw 00C0.0809.0A0B dip
192.168.100.14 cnt 2
ARP Req Filter = T src_ip 10.11.13.1 dst_ip 192.168.100.14
```

The following example shows how to enable debugging messages for ARP filtering for a particular SID on a cable interface:

```
Router# debug cable interface cable c5/0 sid 31
Router# debug cable arp filter

CMTS arp filter debugging is ON
```

Related Commands


Command	Description
cable arp	Activates cable Address Resolution Protocol (ARP).
cable arp filter	Controls the number of ARP packets that are allowable for each Service ID (SID) on a cable interface.
cable proxy-arp	Activates cable proxy ARP on the cable interface.
clear arp	Clears the ARP table on the router.
clear counters	Clears the packet counters on all interfaces or on a specific interface.
debug cable arp	Enables debugging of ARP traffic on a cable interface.
debug cable interface sid	Enables debugging for a particular Service ID (SID) on a specific cable interface.
debug cable mac-address	Enables debugging for a particular CM.
service divert-rate-limit	Displays the total number of ARP replies and requests that have been sent and received, including the number of requests that have been filtered.

service divert-rate-limit

To configure PXF Divert-Rate-Limit, use the **service divert-rate-limit** command in interface configuration mode. To reset this feature to the default parameters, use the **no** form of this command.

service divert-rate-limit *divert-code rate* [**limit** *limit*]

no service divert-rate-limit *divert-code*

Syntax Description	<i>divert-code rate</i>	<p>Configures the PXF Divert-Rate-Limit for the any of the following packets:</p> <ul style="list-style-type: none"> • fwd-glean—Packets that hit a glean adjacency in the FIB. • rpf-glean—Packets that hit a glean adjacency during the RPF check. <p>The minimum rate is 1 packet-per-second and the maximum rate is 255 packets-per-second.</p> <p>The default rate is 20 packets-per-second.</p>
	limit <i>limit</i>	<p>Sets the limit for the number of packets that will be diverted in an initial burst of packets.</p> <p>The minimum limit is 4 packets and the maximum limit is 255 packets.</p> <p>The default limit is 5 packets.</p>
		<p> Note Setting the limit has a limited effect on the behavior of the algorithm, so this part of the CLI is hidden.</p>

Defaults	<p>Divert-Rate-Limit contains the following default behavior and values:</p> <ul style="list-style-type: none"> • Divert-Rate-Limit is always active. • The default rate is 20 packets-per-second. • The default limit is 5 packets.
-----------------	---

Command Modes	Interface configuration (cable interface only)
----------------------	--

Command History	12.3(17a)BC	The command was introduced for the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.
------------------------	-------------	---

Usage Guidelines	<p>The service divert-rate-limit command is used to configure the PXF Divert-Rate-Limit for fwd-glean and rpf-glean packets in order to identify packet streams that will cause congestion of the FP-to-RP interface.</p>
-------------------------	--

Examples

The following example shows how to configure rate-limiting for fib-rp-glean, with a rate of 10 packets-per-second and a limit of 20 packets:

```
Router(config-if)# service divert-rate-limit fib-rp-glean 10 limit 20
```

The following example shows how to return rate-limiting for fib-rp-glean to the default values:

```
Router(config-if)# no service divert-rate-limit fib-rp-glean
```

Pass and fail counters are kept for fwd-glean, rpf-glean, and cable-ARP packets. To show the statistics for the pass and fail counter, use the **show pxf cpu statistics drl** command:

```
Router(config-if)# show pxf cpu statistics drl
  Divert-Rate-Limit statistics
  code          total          diverted          dropped
  fib_rpf_glean 500            59               441
  fib_rp_glean  500            54               446
  arp_filter     0              0                0
```

**Note**

The arp_filter stats shown above are global stats for PXF ARP Filtering. These stats cannot be cleared by the CLI. However, they will reset to zero upon reload.

Packets dropped by Divert-Rate-Limit and the ARP Filter will be recorded in the regular PXF drop statistics:

```
Router(config-if)# show pxf cpu stat drop c5/0/0
  FP drop statistics for Cable5/0/0
  packets          bytes
  vcci undefined   0                0
  vcci C
  ...
  divert_rate_limit 441             28224
  arp_filter_reply  0                0
  arp_filter_request 0                0
```

Related Commands

There are no related commands.

sho cable arp-filter

To display the total number of Address Resolution Protocol (ARP) offenders, use the **sho cable arp-filter** command in privileged EXEC mode.

```
sho cable arp-filter slot/port [ip-requests-filtered number] [requests-filtered number | replies-filtered number]
```

```
sho cable arp-filter slot/subslot/port [ip-requests-filtered number] [requests-filtered number | replies-filtered number]
```

Syntax Description		
<i>slot/port</i>	Displays information for all CMs on the specified cable interface and downstream port on the Cisco uBR7246VXR router.	On the Cisco uBR7246VXR router, <i>slot</i> can range from 3 to 6, and <i>port</i> can be 0 or 1, depending on the cable interface.
<i>slot/subslot/port</i>	Displays information for all CMs on the specified cable interface on the Cisco uBR10012 router. The following are the valid values:	<ul style="list-style-type: none"> • <i>slot</i> = 5 to 8 • <i>subslot</i> = 0 or 1 • <i>port</i> = 0 to 4 (depending on the cable interface)
[ip-requests-filtered <i>number</i>]	(Optional) Displays the Service IDs (SIDs) that are generating or forwarding more filtered ARP requests for IP packets than the specified minimum <i>number</i> of packets. The valid range for <i>number</i> is 1 to 65535, with no default.	Note This field shows the modems that are forwarding IP traffic that could be an part of a attack, such as TCP SYN floods, ping scans, and so forth.
[requests-filtered <i>number</i>]	(Optional) Displays the Service IDs (SIDs) that are generating or forwarding more filtered ARP requests than the specified minimum <i>number</i> of packets. The valid range for <i>number</i> is 1 to 65535, with no default.	
[replies-filtered <i>number</i>]	(Optional) Displays the Service IDs (SIDs) that are generating or filtering more filtered ARP replies than the specified minimum <i>number</i> of packets. The valid range for <i>number</i> is 1 to 65535, with no default.	

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.3(17a)BC	This command was introduced for the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.

Usage Guidelines

The **sho cable arp-filter** command is used to display the total number of Address Resolution Protocol (ARP) offenders.

Examples

The following example shows how to generate a list of ARP offenders in PXF:

```
Router# sho cable arp-filter ?
  Bundle  Cable Virtual bundle interface
  Cable   CMTS interface

uBR-15#sho cable arp-filter Bundle1 ?
  ip-requests-filtered  Show modems with arp request for IP packet filter count
                        at or above x
  replies-filtered     Show modems with arp reply filter count at or above x
  requests-filtered    Show modems with arp request filter count at or above x
  |                    Output modifiers
<cr>
```

The following is a sample output from the CLI:

```
Router# sho cable arp-filter Bundle1 requests-filtered 40

Interface Cable5/0/0 - none
Interface Cable6/0/2
Sid  MAC Address      IP Address      Req-Filtered Req-For-IP-Filtered Rep-Filtered
4    0007.0e03.9cad 50.3.81.15      46           0                 0
Interface Cable7/0/0 - none
```

Related Commands

Command	Description
cable arp	Activates cable Address Resolution Protocol (ARP).
cable arp filter	Controls the number of ARP packets that are allowable for each Service ID (SID) on a cable interface.
cable proxy-arp	Activates cable proxy ARP on the cable interface.
clear arp	Clears the ARP table on the router.
clear counters	Clears the packet counters on all interfaces or on a specific interface.
debug cable arp filter	Displays debugging messages about the filtering of ARP broadcasts.

show cable arp-filter

To display the total number of Address Resolution Protocol (ARP) replies and requests that have been sent and received, including the number of requests that have been filtered, use the **show cable arp-filter** command in privileged EXEC mode.

```
show cable arp-filter cable slot/port [ip-requests-filtered number] [requests-filtered number | replies-filtered number]
```

```
show cable arp-filter cable slot/subslot/port [ip-requests-filtered number] [requests-filtered number | replies-filtered number]
```

Syntax	Description
cable <i>slot/port</i>	Displays information for all CMs on the specified cable interface and downstream port on the Cisco uBR7246VXR router. On the Cisco uBR7246VXR router, <i>slot</i> can range from 3 to 6, and <i>port</i> can be 0 or 1, depending on the cable interface.
cable <i>slot/subslot/port</i>	Displays information for all CMs on the specified cable interface on the Cisco uBR10012 router. The following are the valid values: <ul style="list-style-type: none"> <i>slot</i> = 5 to 8 <i>subslot</i> = 0 or 1 <i>port</i> = 0 to 4 (depending on the cable interface)
[ip-requests-filtered <i>number</i>]	(Optional) Displays the Service IDs (SIDs) that are generating or forwarding more filtered ARP requests for IP packets than the specified minimum <i>number</i> of packets. The valid range for <i>number</i> is 1 to 65535, with no default. Note This field shows the modems that are forwarding IP traffic that could be a part of an attack, such as TCP SYN floods, ping scans, and so forth.
[requests-filtered <i>number</i>]	(Optional) Displays the Service IDs (SIDs) that are generating or forwarding more filtered ARP requests than the specified minimum <i>number</i> of packets. The valid range for <i>number</i> is 1 to 65535, with no default.
[replies-filtered <i>number</i>]	(Optional) Displays the Service IDs (SIDs) that are generating or filtering more filtered ARP replies than the specified minimum <i>number</i> of packets. The valid range for <i>number</i> is 1 to 65535, with no default.

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.2(15)BC2	This command was introduced for the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.
	12.2(15)BC2b	The ip-requests-filtered option was added to display the specific Service IDs (SIDs) that are generating or forwarding a minimum number of ARP packets.

Usage Guidelines

The **cable arp filter** command enables the filtering of ARP request and reply packets on a cable interface. ARP packets might need to be filtered when a user on the cable network generates a large volume of ARP traffic as part of a theft-of-service or denial-of-service attack, or when a virus is using ARP requests to find other computers that it might infect.

The **show cable arp-filter** command displays the total number of ARP reply packets that have been received and the number of ARP request packets that have been sent on the cable interface, as well as the number of such packets that have been filtered.

**Tip**

To clear the counters on all interfaces, use the **clear counters** command. To clear the counters on a specific interface, use the **clear counters cable interface** command.

Examples

The following example shows the typical output from the **show cable arp-filter** command on a Cisco uBR10012 router. The displays for other Cisco CMTS platforms are similar.

```
Router# show cable arp-filter Cable5/0/0

ARP Filter statistics for Cable5/0/0:
  Replies Rcvd: 177387 total, 1869 unfiltered, 8824 filtered
  Requests Sent For IP: 68625 total, 964 unfiltered, 36062 filtered
  Requests Forwarded: 7969175 total, 7213 unfiltered, 366167 filtered
```

[Table 1](#) describes the fields shown in the display.

Table 1 *show cable arp-filter Field Descriptions*

Field	Description
Replies Rcvd	
Total	Total number of ARP reply packets received on the cable interface since power-on.
Unfiltered	Number of ARP reply packets that the cable interface received and accepted while filtering was enabled using the cable arp filter reply-accept command.
Filtered	Number of ARP reply packets that the cable interface dropped while filtering was enabled, because they would have otherwise exceeded the allowable threshold value that was configured for the interface using the cable arp filter reply-accept command.
Requests Sent For IP	
Total	Total number of ARP request packets that the cable interface was asked to forward since power-on.
Unfiltered	Number of ARP request packets that the cable interface sent while filtering was enabled using the cable arp filter request-send command.
Filtered	Number of ARP request packets that the cable interface dropped, because they would have otherwise exceeded the allowable threshold value that was configured for the interface using the cable arp filter request-send command.

Table 1 *show cable arp-filter Field Descriptions (continued)*

Field	Description
Requests Forwarded	
Total	Total number of ARP request packets that the cable interface was asked to forward to the ARP proxy since power-on.
Unfiltered	Number of ARP request packets that the cable interface sent to the ARP proxy while filtering was enabled using the cable arp filter request-send command.
Filtered	Number of ARP request packets for the ARP proxy that the cable interface dropped, because they would have otherwise exceeded the allowable threshold value that was configured for the interface using the cable arp filter request-send command.
Note	All counters are 16-bit counters, with a maximum value of 65,535 packets. If the number of packets exceeds this amount, the counter wraps back to zero and begins incrementing again.

**Note**

The Total counts in the **show cable arp-filter** command continue to increment, regardless of whether ARP filtering has been enabled. The Unfiltered and Filtered counts increment only when ARP filtering has been enabled using the **cable arp filter** command. When Cable ARP Filtering is disabled, these counters retain their current values until manually reset, using the **clear counters** command.

The following example shows how to display the devices that are generating or filtering more than 100 ARP requests per reporting period. Repeat the command to see how quickly the device is generating ARP packets.

```
Router# show cable arp-filter c7/0/0 requests-filtered 100
```

```
Sid  MAC Address      IP Address      Req-Filtered    Req-For-IP-Filtered  Rep-Filtered
1    0006.2854.72d7    50.3.81.4      12407           0                     0
```

```
Router# show cable arp-filter c7/0/0 requests-filtered 100
```

```
Sid  MAC Address      IP Address      Req-Filtered    Req-For-IP-Filtered  Rep-Filtered
1    0006.2854.72d7    50.3.81.4      14597           0                     0
```

The following example shows how to display the devices that are generating or filtering more than 200 ARP replies per reporting period. Repeat the command to see how quickly the device is generating ARP packets.

```
Router# show cable arp-filter c5/0/0 replies-filtered 200
```

```
Sid  MAC Address      IP Address      Req-Filtered    Req-For-IP-Filtered  Rep-Filtered
2    0006.53b6.562f    50.3.81.6      0               0                     2358
```

```
Router# show cable arp-filter c5/0/0 replies-filtered 200
```

```
Sid  MAC Address      IP Address      Req-Filtered    Req-For-IP-Filtered  Rep-Filtered
2    0006.53b6.562f    50.3.81.6      0               0                     4016
```

The following example shows how to display the devices that are generating or filtering more than 10 ARP requests for IP packets per reporting period. Repeat the command to see how quickly the device is generating ARP packets.

```
Router# show cable arp-filter c3/0 ip-requests-filtered 10

Sid  MAC Address      IP Address      Req-Filtered    Req-For-IP-Filtered  Rep-Filtered
 2    0006.2854.71e7  50.3.72.4      0                1926                 0
```

Table 2 describes the fields shown in the display.

Table 2 show cable arp-filter Detail Field Descriptions

Field	Description
SID	Service ID (SID) of the device.
MAC Address	Hardware (MAC-layer) address of the cable modem or CPE device.
IP Address	IP address of the cable modem or CPE device.
Req-Filtered	Total number of ARP requests that the device has generated or forwarded.
Req-For-IP-Filtered	Total number of ARP requests that the device has generated or forwarded for IP packets.
Rep-Filtered	Total number of ARP replies that the device has generated or forwarded.

Note The Req-Filter and Rep-Filtered counters are 16-bit counters, with a maximum value of 65,535 packets. If the number of packets exceeds this amount, the counter wraps back to zero and begins incrementing again.

Clearing the ARP Packet Counters

The following example shows the cable ARP counters being cleared by the **clear counters cable interface** command. This can be useful because the ARP counters are 16-bit counters that can wrap around to zero relatively quickly when a large amount of ARP traffic is being generated. Also, the ARP packet counters could include SIDs that had forwarded large amounts of ARP traffic in the past, but that are not currently forwarding such traffic. Clearing the counters allows you to clearly see the SIDS that are currently forwarding the ARP traffic that is triggering the ARP filters.

```
Router# show cable arp cable 3/0

ARP Filter statistics for Cable3/0:
  Replies Rcvd: 3278 total. 84 unfiltered, 3194 filtered
  Requests Sent For IP: 941 total. 30 unfiltered, 911 filtered
  Requests Forwarded: 941 total. 37 unfiltered, 904 filtered

Router# show cable arp-filter cable 5/1/0 requests-filtered 10

Sid  MAC Address      IP Address      Req-Filtered    Req-For-IP-Filtered  Rep-Filtered
 1    0006.2854.72d7  10.3.81.4      8                0                   0
23   0007.0e02.b747  10.3.81.31     32               0                   0
57   0007.0e03.2c51  10.3.81.31    12407            0                   0
...
81   00C0.c726.6b14  10.3.81.31     23               0                   0

Router# clear counter cable 5/1/0
Clear "show interface" counters on this interface [confirm] y

08:17:53.968: %CLEAR-5-COUNTERS: Clear counter on interface Cable5/1/0 by console
```

```
Router# show cable arp cable 5/1/0
```

```
ARP Filter statistics for Cable3/0:
  Replies Rcvd: 0 total. 0 unfiltered, 0 filtered
  Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered
  Requests Forwarded: 0 total. 0 unfiltered, 0 filtered
```

```
Router# show cable arp-filter cable 5/1/0 requests-filtered 10
```

```
Sid  MAC Address      IP Address      Req-Filtered    Req-For-IP-Filtered  Rep-Filtered
```

```
Router# show cable arp-filter cable 5/1/0 requests-filtered 10
```

```
Sid  MAC Address      IP Address      Req-Filtered    Req-For-IP-Filtered  Rep-Filtered
57   0007.0e03.2c51  10.3.81.31     20              0                    0
81   00C0.c726.6b14  10.3.81.31     12              0                    0
```

```
Router# show cable arp-filter cable 5/1/0 requests-filtered 10
```

```
Sid  MAC Address      IP Address      Req-Filtered    Req-For-IP-Filtered  Rep-Filtered
57   0007.0e03.2c51  10.3.81.31     31              0                    0
81   00C0.c726.6b14  10.3.81.31     18              0                    0
```

```
Router#
```

**Note**

The **clear counters** command clears all of the packet counters on an interface, not just the ARP packet counters.

Related Commands

Command	Description
cable arp	Activates cable Address Resolution Protocol (ARP).
cable arp filter	Controls the number of ARP packets that are allowable for each Service ID (SID) on a cable interface.
cable proxy-arp	Activates cable proxy ARP on the cable interface.
clear arp	Clears the ARP table on the router.
clear counters	Clears the packet counters on all interfaces or on a specific interface.
debug cable arp filter	Displays debugging messages about the filtering of ARP broadcasts.
sho cable arp-filter	Displays a list of ARP offenders on the cable interface when ARP Filtering in PXF is enabled.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2006 Cisco Systems, Inc. All rights reserved.