



Filtering Cable DHCP Lease Queries

Document Revision History

| Date | Revision | Reason |
|------------|------------|---|
| 02/13/2006 | OL-2818-06 | Added Document Revision History table. Incorporated Cisco IOS Release 12.3(17a)BC enhancements. |

This document describes the Dynamic Host Configuration Protocol (DHCP) LEASEQUERY filter feature, which enables the Cisco Cable Modem Termination System (CMTS) router to filter excessive numbers of DHCP LEASEQUERY messages on either the upstream or the downstream cable interface, or both.

Feature History for Filtering Cable DHCP Lease Queries

| Release | Modification |
|---|---|
| Release 12.2(15)BC1d, Release 12.2(15)BC2b | This feature was introduced for the Cisco uBR7100 series, Cisco uBR7246VXR, and Cisco uBR10012 universal broadband routers. |
| Release 12.3(13)BC | Support for the MAC Address Exclusion List added for the cable-source verify dhcp command. |
| Release 12.3(17a)BC | Support for Configurable Leasequery Server using the cable source-verify dhcp server ipaddress command. |

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 Filtering Cable DHCP Lease Queries, page 2](#)
- [Restrictions for Filtering Cable DHCP Lease Queries, page 2](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- [Information About Filtering Cable DHCP Lease Queries, page 2](#)
- [How to Configure Filtering Cable DHCP LEASEQUERY Requests, page 3](#)
- [How to Configure the DHCP MAC Address Exclusion List for the cable-source verify dhcp Command, page 6](#)
- [Configuration Examples for Filtering Cable DHCP Lease Queries, page 7](#)
- [Additional References, page 7](#)
- [Command Reference, page 9](#)

Prerequisites for Filtering Cable DHCP Lease Queries

- The Cisco uBR7100 series, Cisco uBR7246VXR, or Cisco uBR10012 router must be running Cisco IOS Release 12.2(15)BC1d, 12.2(15)BC2b, or later release.
- You must configure a cable interface with the **cable source-verify dhcp** command and the **no cable arp** command before the Cisco CMTS router can begin filtering DHCP lease queries. Lease queries will be sent to the DHCP server (or configured alternate server).

To divert DHCP lease queries to a server other than the DHCP server, you must use the **cable source-verify dhcp server ipaddress** command and the **no cable arp** command before the Cisco CMTS router can begin filtering DHCP lease queries. Only one alternate server may be configured.

Restrictions for Filtering Cable DHCP Lease Queries

- Lease queries are sent to the DHCP server unless an alternate server is configured.
- Only one alternate server may be configured.
- Users are responsible for the synchronization of the DHCP server and configured alternate server.
- If the configured alternate server fails, lease query requests will *not* be diverted back to the DHCP server.

Information About Filtering Cable DHCP Lease Queries

To configure the Cisco CMTS router to send DHCP LEASEQUERY requests to the DHCP server, use the **cable source-verify dhcp** and **no cable arp** commands. Unknown IP addresses that are found in packets for customer premises equipment (CPE) devices that use the cable modems on the cable interface will be verified. The DHCP server returns a DHCP ACK message with the MAC address of the CPE device that has been assigned this IP address, if any.

To configure the Cisco CMTS router to divert DHCP LEASEQUERY requests to a server other than the DHCP server, use the **cable source-verify dhcp server ipaddress** and **no cable arp** commands.

Regardless of which server is configured, the router can then use this information to verify that this CPE device is authorized to use this IP address. This prevents users from assigning unauthorized IP addresses to their CPE devices, without interfering with valid traffic on the upstream or downstream.

Problems can occur, though, when viruses, denial of service (DoS) attacks, and theft-of-service attacks begin scanning a range of IP addresses, in an attempt to find unused addresses. When the Cisco CMTS router is verifying unknown IP addresses, this type of scanning generates a large volume of DHCP lease queries, which can result in the following problems:

- High CPU utilization on the Cisco CMTS router
- High utilization on the DHCP server (or configured alternate server), resulting in a slow response time or no response at all
- Packets can be dropped by the Cisco CMTS router or DHCP server (or configured alternate server)
- Lack of available bandwidth for other customers on the cable interface

To prevent such a large volume of LEASEQUERY requests on cable interfaces, you can enable filtering of these requests on upstream interfaces, downstream interfaces, or both. When this feature is enabled, the Cisco CMTS allows only a certain number of DHCP LEASEQUERY requests for each service ID (SID) on an interface within the configured interval time period. If a SID generates more lease queries than the maximum, the router drops the excess number of requests until the next interval period begins.

You can configure both the number of allowable DHCP LEASEQUERY requests and the interval time period, so as to match the capabilities of your DHCP server (or configured alternate server) and cable network.

How to Configure Filtering Cable DHCP LEASEQUERY Requests

Use the following procedures to configure the filtering of DHCP LEASEQUERY requests on both the downstreams and upstreams of a cable interface:

- [Enabling DHCP LEASEQUERY Filtering on Downstreams, page 3](#)
- [Enabling DHCP LEASEQUERY Filtering on Upstreams, page 4](#)

Enabling DHCP LEASEQUERY Filtering on Downstreams

Use the following procedure to start filtering DHCP lease queries on all downstreams in a Cisco CMTS router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable source-verify leasequery-filter downstream *threshold interval***
4. **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 | cable source-verify leasequery-filter downstream threshold interval Example: Router(config)# cable source-verify leasequery-filter downstream 5 10 Router(config)# | Enables leasequery filtering on all downstreams on the Cisco CMTS router, using the specified <i>threshold</i> and <i>interval</i> values: <ul style="list-style-type: none"> <i>threshold</i>—Maximum number of DHCP lease queries allowed per SID for each <i>interval</i> period. The valid range is 0 to 255 lease queries. <i>interval</i>—Time period, in seconds, over which lease queries should be monitored. The valid range is 1 to 10 seconds. |
| Step 4 | end Example: Router(config-if)# end Router# | Exits interface configuration mode and returns to privileged EXEC mode. |

Enabling DHCP LEASEQUERY Filtering on Upstreams

Use the following procedure to start filtering DHCP lease queries on all upstreams on a particular cable interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable *x/y***
or
interface cable *x/y/z*
4. **cable source-verify leasequery-filter upstream *threshold interval***
5. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|---|
| Step 1 | <p>enable</p> <p>Example: Router> enable</p> | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | <p>configure terminal</p> <p>Example: Router# configure terminal</p> | Enters global configuration mode. |
| Step 3 | <p>interface cable x/y or interface cable x/y/z</p> <p>Example: Router(config)# interface cable 5/1 Router(config-if)#</p> | Enters interface configuration mode for the specified cable interface. |
| Step 4 | <p>enable source-verify leasequery-filter upstream <i>threshold interval</i></p> <p>Example: Router(config-if)# cable source-verify leasequery-filter upstream 2 5 Router(config-if)#</p> | <p>Enables leasequery filtering on all upstreams on the specified cable interface, using the specified <i>threshold</i> and <i>interval</i> values:</p> <ul style="list-style-type: none"> • <i>threshold</i>—Maximum number of DHCP lease queries allowed per SID for each <i>interval</i> period. The valid range is 0 to 20 lease queries. • <i>interval</i>—Time period, in seconds, over which lease queries should be monitored. The valid range is 1 to 5 seconds. |
| | <p>Note Repeat Step 3 through Step 4 to enable the filtering of DHCP lease queries on the upstreams for other cable interfaces. Master and slave interfaces in a cable bundle must be configured separately.</p> | |
| Step 5 | <p>end</p> <p>Example: Router(config-if)# end</p> | Exits interface configuration mode and returns to privileged EXEC mode. |

How to Configure the DHCP MAC Address Exclusion List for the cable-source verify dhcp Command

Cisco IOS Release 12.3(13)BC introduces the ability to exclude trusted MAC addresses from standard DHCP source verification checks, as supported in previous Cisco IOS releases for the Cisco CMTS. This feature enables packets from trusted MAC addresses to pass when otherwise packets would be rejected with standard DHCP source verification. This feature overrides the **cable source-verify** command on the Cisco CMTS for the specified MAC address, yet maintains overall support for standard and enabled DHCP source verification processes. This feature is supported on Performance Routing Engine 1 (PRE1) and PRE2 modules on the Cisco uBR10012 router chassis.

To enable packets from trusted source MAC addresses in DHCP, use the **cable trust** command in global configuration mode. To remove a trusted MAC address from the MAC exclusion list, use the **no** form of this command. Removing a MAC address from the exclusion list subjects all packets from that source to standard DHCP source verification.

cable trust *mac-address*

no cable trust *mac-address*

Syntax Description

| | |
|--------------------|--|
| <i>mac-address</i> | The MAC address of a trusted DHCP source, and from which packets will not be subject to standard DHCP source verification. |
|--------------------|--|

Usage Guidelines

This command and capability are only supported in circumstances in which the Cable Source Verify feature is first enabled on the Cisco CMTS.

When this feature is enabled in addition to cable source verify, a packet's source must belong to the MAC Exclude list on the Cisco CMTS. If the packet succeeds this exclusionary check, then the source IP address is verified against Address Resolution Protocol (ARP) tables as per normal and previously supported source verification checks. The service ID (SID) and the source IP address of the packet must match those in the ARP host database on the Cisco CMTS. If the packet check succeeds, the packet is allowed to pass. Rejected packets are discarded in either of these two checks.

Any trusted source MAC address in the optional exclusion list may be removed at any time. Removal of a MAC address returns previously trusted packets to non-trusted status, and subjects all packets to standard source verification checks on the Cisco CMTS.



Note

When the **cable source-verify dhcp** feature is enabled, and a statically-defined IP address has been added to the CMTS for a CM using the **cable trust** command to override the **cable source-verify dhcp** checks for this device, packets from this CM will continue to be dropped until an entry for this CM is added to the ARP database of the CMTS. To achieve this, disable the **cable source-verify dhcp** feature, ping the CMTS from the CM to add an entry to the ARP database, and re-enable the **cable source-verify dhcp** feature.

For additional information about the enhanced Cable Source Verify DHCP feature, and general guidelines for its use, refer to the following documents on Cisco.com:

- *IP Address Verification for the Cisco uBR7200 Series Cable Router*
http://www.cisco.com/en/US/docs/ios/12_0t/12_0t7/feature/guide/sourcver.html
- *Filtering Cable DHCP Lease Queries*
<http://www.cisco.com/en/US/docs/cable/cmts/feature/cblsrcvy.html>

- *Cisco IOS CMTS Cable Command Reference Guide*
http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
- CABLE SECURITY, *Cable Source-Verify and IP Address Security*, White Paper
http://www.cisco.com/en/US/tech/tk86/tk803/technologies_tech_note09186a00800a7828.shtml

Configuration Examples for Filtering Cable DHCP Lease Queries

This section provides the following examples of how to configure the DHCP lease query filtering feature:

- [DHCP Downstream and Upstream DHCP LEASEQUERY Filtering Configuration on an Individual Cable Interface: Example, page 7](#)

DHCP Downstream and Upstream DHCP LEASEQUERY Filtering Configuration on an Individual Cable Interface: Example

The following example shows an excerpt from a typical configuration of a cable interface that is configured for filtering DHCP LEASEQUERY requests on both its upstream and downstream interfaces:

**Note**

If an alternate server has been configured to receive lease query requests, **cable source-verify dhcp server *ipaddress*** would display in place of **cable source-verify dhcp** below.

```
!  
cable source-verify leasequery-filter downstream 5 20  
!  
interface Cable8/1/0  
...  
  cable source-verify dhcp  
  cable source-verify leasequery-filter upstream 1 5  
  no cable arp  
...
```

Additional References

The following sections provide references related to the DHCP LEASEQUERY filtering feature.

Related Documents

| Related Topic | Document Title |
|--|--|
| CMTS Command Reference | <i>Cisco IOS CMTS Cable Command Reference Guide</i> , at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html |
| Cisco IOS Release 12.2 Command Reference | Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html |

Standards

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

MIBs

| MIBs | MIBs Link |
|--|--|
| No new or modified MIBs are supported 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> |

Technical Assistance

| Description | Link |
|--|---|
| Technical Assistance Center (TAC) home page, containing 30,000 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/cisco/web/support/index.html |

Command Reference

This section documents the following new or modified commands that are needed to configure the DHCP Lease Query filter feature.

- **[cable source-verify leasequery-filter downstream](#)**
- **[cable source-verify leasequery-filter upstream](#)**
- **[show cable leasequery-filter](#)**

**Note**

Other cable-specific commands are documented in the *Cisco IOS CMTS Cable Command Reference Guide*, at the following URL:

http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

cable source-verify leasequery-filter downstream

To control the number of Dynamic Host Configuration Protocol (DHCP) LEASEQUERY request messages that are sent for unknown IP addresses on all cable downstream interfaces on the Cisco Cable Modem Termination System (CMTS) router, use the **cable source-verify leasequery-filter downstream** command in global configuration mode. To stop the filtering of DHCP lease queries, use the **no** form of this command.

cable source-verify leasequery-filter downstream *threshold interval*

no cable source-verify leasequery-filter downstream

| Syntax Description | | |
|--------------------|------------------|--|
| | <i>threshold</i> | Maximum number of DHCP lease queries allowed per SID for each <i>interval</i> period. The valid range is 0 to 255 lease queries. |
| | <i>interval</i> | Time period, in seconds, over which lease queries should be monitored. The valid range is 1 to 10 seconds. |

Defaults Filtering of DHCP lease queries is disabled.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-------------------------------|---|
| | 12.2(15)BC1d, 12.2(15)BC2b | This command was introduced for the Cisco uBR7100 series, Cisco uBR7246VXR, and Cisco uBR10012 universal broadband routers. |

Usage Guidelines When the **cable source-verify dhcp** (or **cable source-verify dhcp server ipaddress**) and **no cable arp** commands are configured on a cable interface, the Cisco CMTS router sends a DHCP LEASEQUERY request to the DHCP server (or configured alternate server) to verify unknown IP addresses that are found in packets to and from customer premises equipment (CPE) devices that are using the cable modems on the cable interface. The DHCP server (or configured alternate server) returns a DHCP ACK message with the MAC address of the CPE device that has been assigned this IP address, if any. The router can then verify that this CPE device is authorized to use this IP address, which prevents users from assigning unauthorized IP addresses to their CPE devices.

Problems can occur, though, when viruses, denial of service (DoS) attacks, and theft-of-service attacks scan ranges of IP addresses, in an attempt to find unused addresses. This type of activity can generate a large volume of DHCP LEASEQUERY requests, which can result in high CPU utilization and a lack of available bandwidth for other customers.

To prevent such a large volume of LEASEQUERY requests on all downstreams in the Cisco CMTS router, use the **cable source-verify leasequery-filter downstream** command. After configuring this command, the Cisco CMTS allows only a certain number of DHCP LEASEQUERY requests in the downstream direction within each interval time period.

For example, the **cable source-verify leasequery-filter downstream 5 10** command configures the router so that it allows a maximum of 5 DHCP LEASEQUERY requests every 10 seconds for each SID on the downstream direction. This command applies to all downstream cable interfaces in the router.

**Note**

The **cable source-verify leasequery-filter downstream** command enables DHCP lease query filtering on all downstreams, but the actual filtering does not begin until the **cable source-verify dhcp** (or **cable source-verify dhcp server *ipaddress***) command and the **no cable arp** command are configured on a particular downstream. You can configure these commands on either the downstream's main interface, or on a subinterface for the downstream. If these commands are configured on a subinterface, however, the lease query filtering occurs only for cable modems using that subinterface.

**Tip**

Use the **cable source-verify leasequery-filter upstream** command to filter DHCP LEASEQUERY requests in the upstream direction.

Examples

The following example shows how to configure the Cisco CMTS router so that it allows a maximum of 10 DHCP lease query requests per SID over each five-second interval on all downstream cable interfaces. This example also shows the configuration of **cable source-verify dhcp** and **no cable arp** commands on a cable interface, which are required to use this feature.

**Note**

If an alternate server has been configured to receive lease query requests, the **cable source-verify dhcp server *ipaddress*** command would be used in place of the **cable source-verify dhcp** command below.

```
Router# configure terminal
Router(config)# cable source-verify leasequery-filter downstream 10 5
Router(config)# interface cable 5/1/0
Router(config-if)# cable source-verify dhcp
Router(config-if)# no cable arp
Router(config-if)#
```

Related Commands

| Command | Description |
|---|--|
| cable arp | Activates the cable Address Resolution Protocol (ARP). |
| cable source-verify | Enables verification of IP addresses for cable modems (CMs) and CPE devices on the upstream. |
| cable source-verify leasequery-filter upstream | Controls the number of DHCP lease query messages that are sent for unknown IP addresses per each service ID (SID) on an upstream. |
| show cable leasequery-filter | Displays the number of DHCP lease query messages that have been filtered for all cable modems or for a particular cable interface. |

cable source-verify leasequery-filter upstream

To control the number of Dynamic Host Configuration Protocol (DHCP) LEASEQUERY request messages that are sent for unknown IP addresses per each service ID (SID) on an upstream, use the **cable source-verify leasequery-filter upstream** command in cable interface configuration mode. To disable the filtering of DHCP lease queries, use the **no** form of this command.

cable source-verify leasequery-filter upstream *threshold interval*

no cable source-verify leasequery-filter upstream

| Syntax Description | threshold | Maximum number of DHCP lease queries allowed per SID for each <i>interval</i> period. The valid range is 0 to 20 lease queries. |
|--------------------|-----------|---|
| | interval | Time period, in seconds, over which lease queries should be monitored. The valid range is 1 to 5 seconds. |

Defaults Filtering of DHCP lease queries is disabled.

Command Modes Interface configuration (cable interface only)

| Command History | Release | Modification |
|-----------------|-------------------------------|---|
| | 12.2(15)BC1d, 12.2(15)BC2b | This command was introduced for the Cisco uBR7100 series, Cisco uBR7246VXR, and Cisco uBR10012 universal broadband routers. |

Usage Guidelines When the **cable source-verify dhcp** (or **cable source-verify dhcp server ipaddress**) and **no cable arp** commands are configured on a cable interface, the Cisco Cable Modem Termination System (CMTS) router sends a DHCP LEASEQUERY request to the DHCP server (or configured alternate server) to verify unknown IP addresses that are found in packets to and from customer premises equipment (CPE) devices that are using the cable modems on the cable interface. The DHCP server (or configured alternate server) returns a DHCP ACK message with the MAC address of the CPE device that has been assigned this IP address, if any. The router can then verify that this CPE device is authorized to use this IP address, which prevents users from assigning unauthorized IP addresses to their CPE devices.

Problems can occur, though, when viruses, denial of service (DoS) attacks, and theft-of-service attacks scan ranges of IP addresses, in an attempt to find unused addresses. This type of activity can generate a large volume of DHCP LEASEQUERY requests, which can result in high CPU utilization and a lack of available bandwidth for other customers.

To prevent such a large volume of LEASEQUERY requests on the upstreams on a cable interface, use the **cable source-verify leasequery-filter upstream** command. After configuring this command, the Cisco CMTS allows only a certain number of DHCP LEASEQUERY requests in the upstream direction within each interval time period.

For example, the **cable source-verify leasequery-filter upstream 5 5** command configures the router so that it allows a maximum of 5 DHCP LEASEQUERY requests every 5 seconds for each SID on the upstream direction. This command applies to all upstreams on the cable interface.

**Note**

The **cable source-verify leasequery-filter upstream** command enables DHCP lease query filtering on all upstreams on a cable interface, but the actual filtering does not begin until the **cable source-verify dhcp** (or **cable source-verify dhcp server *ipaddress***) command and the **no cable arp** command are configured on the upstream's associated downstream interface. You can configure these commands on either the downstream's main interface, or on a subinterface for the downstream. If these commands are configured on a subinterface, however, the lease query filtering occurs only for cable modems using that subinterface.

**Note**

If using cable interface bundling, configure the **cable source-verify leasequery-filter upstream** command on all master and slave interfaces.

**Tip**

Use the **cable source-verify leasequery-filter downstream** command to filter DHCP LEASEQUERY requests in the downstream direction.

Examples

The following example shows how to configure the Cisco CMTS router so that it allows a maximum of five DHCP lease query requests per SID over each two-second interval on all upstreams on a particular cable interface. This example also shows the configuration of **cable source-verify dhcp** and **no cable arp** commands on the cable interface, which are required to use this feature.

**Note**

If an alternate server has been configured to receive lease query requests, the **cable source-verify dhcp server *ipaddress*** command would be used in place of the **cable source-verify dhcp** command below.

```
Router# configure terminal
Router(config)# interface cable 6/0
Router(config-if)# cable source-verify dhcp
Router(config-if)# cable source-verify leasequery-filter upstream 5 2
Router(config-if)# no cable arp
Router(config-if)#
```

Related Commands

| Command | Description |
|---|--|
| cable arp | Activates the cable Address Resolution Protocol (ARP). |
| cable source-verify | Enables verification of IP addresses for cable modems (CMs) and CPE devices on the upstream. |
| cable source-verify leasequery-filter downstream | Controls the number of DHCP lease query messages that are sent for unknown IP addresses on all cable downstream interfaces on the Cisco CMTS router. |
| show cable leasequery-filter | Displays the number of DHCP lease query messages that have been filtered for all cable modems or for a particular cable interface. |

show cable leasequery-filter

To display the number of Dynamic Host Configuration Protocol (DHCP) LEASEQUERY request messages that have been filtered for all cable modems (CMs) or for a particular cable interface, use the **show cable leasequery-filter** command in privileged EXEC mode.

```
show cable leasequery-filter [cable slot/port [requests-filtered [minimum-requests] ] ]
```

```
show cable leasequery-filter [cable slot/subslot/port [requests-filtered [minimum-requests] ] ]
```

Syntax Description

| | |
|---|---|
| cable slot/port | (Optional) 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 slot/subslot/port | (Optional) 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) |
| requests-filtered [<i>minimum-requests</i>] | (Optional) Displays the number of DHCP LEASEQUERY requests that have been filtered for each particular cable modem on a cable interface. <ul style="list-style-type: none"> • <i>minimum-requests</i>—(Optional) Displays only those cable modems for which the router has filtered at least this minimum number of lease queries. The valid range for <i>minimum-requests</i> is 1 to 65535, with a default of 1. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-------------------------------|---|
| 12.2(15)BC1d, 12.2(15)BC2b | This command was introduced for the Cisco uBR7100 series, Cisco uBR7246VXR, and Cisco uBR10012 universal broadband routers. |

Usage Guidelines

The **show cable leasequery-filter** command displays the total number of DHCP LEASEQUERY requests that have been filtered on a Cisco Cable Modem Termination System (CMTS) router and on a particular cable interface. This command can also optionally display details for each particular cable modem on an interface that has had DHCP lease queries filtered.

Examples

The following example shows how to display the total number of DHCP LEASEQUERY requests that have been filtered on the router and on a particular cable interface:

```
Router# show cable leasequery-filter
```

```
Lease Query Filter statistics for Unknown Sid
```

```
Requests Sent : 138 total. 41 unfiltered, 97 filtered
```

```
Router# show cable leasequery-filter cable 8/1/0
```

```
Lease Query Filter statistics for Cable8/1/0:
```

```
Requests Sent : 35 total. 25 unfiltered, 10 filtered
```

The following example shows how to display a list of cable modems on a cable interface and the number of DHCP LEASEQUERY messages that have been filtered for each:

```
Router# show cable leasequery-filter cable 8/1/0 requests-filtered
```

| Sid | MAC Address | IP Address | Req-Filtered |
|-----|----------------|------------|--------------|
| 1 | 0050.7366.1243 | 92.1.1.20 | 0 |
| 2 | 0007.0e06.953b | 95.1.1.24 | 0 |
| 3 | 0007.0e06.97b5 | 93.1.1.24 | 2 |
| 4 | 00d0.ba45.4bd5 | 91.1.1.35 | 0 |
| 5 | 0007.0e06.9773 | 95.1.1.23 | 12 |
| 6 | 0001.42aa.737d | 94.1.1.23 | 645 |
| 7 | 0001.42aa.738b | 95.1.1.22 | 0 |
| 8 | 00d0.ba45.4955 | 92.1.1.23 | 0 |
| 9 | 0007.0e06.51ef | 94.1.1.25 | 0 |
| 10 | 00d0.ba77.743b | 91.1.1.36 | 3 |
| 11 | 0001.42aa.6e6f | 93.1.1.22 | 2 |
| 12 | 0007.0e06.512f | 91.1.1.23 | 2 |
| 13 | 0007.0e06.5137 | 92.1.1.25 | 0 |
| 14 | 0007.0e06.9be7 | 92.1.1.24 | 0 |
| 15 | 0002.b970.0027 | 92.1.1.22 | 1 |
| 16 | 0001.42aa.738d | 91.1.1.21 | 10 |

```
Router#
```

The following example shows how to display a list of cable modems on a cable interface that have had 10 or more DHCP LEASEQUERY messages that have been filtered:

```
Router# show cable leasequery-filter cable 8/1/0 requests-filtered 10
```

| Sid | MAC Address | IP Address | Req-Filtered |
|-----|----------------|------------|--------------|
| 5 | 0007.0e06.9773 | 95.1.1.23 | 12 |
| 6 | 0001.42aa.737d | 94.1.1.23 | 645 |
| 16 | 0001.42aa.738d | 91.1.1.21 | 10 |

```
Router#
```

Related Commands

| Command | Description |
|---|--|
| cable arp | Activates the cable Address Resolution Protocol (ARP). |
| cable source-verify | Enables verification of IP addresses for cable modems (CMs) and customer premises equipment (CPE) devices on the upstream. |
| cable source-verify leasequery-filter downstream | Controls the number of DHCP lease query messages that are sent for unknown IP addresses on all cable downstream interfaces on the Cisco CMTS router. |
| cable source-verify leasequery-filter upstream | Controls the number of DHCP lease query messages that are sent for unknown IP addresses per each service ID (SID) on an upstream. |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo 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. (0910R)

Copyright © 2004–2009 Cisco Systems, Inc. All rights reserved.