



Junos[®] OS

IGMP Feature Guide for Subscriber Management

Release

14.1



Published: 2014-04-25

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos[®] OS IGMP Feature Guide for Subscriber Management

14.1

Copyright © 2014, Juniper Networks, Inc.

All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	vii
	Documentation and Release Notes	vii
	Supported Platforms	vii
	Using the Examples in This Manual	vii
	Merging a Full Example	viii
	Merging a Snippet	viii
	Documentation Conventions	ix
	Documentation Feedback	xi
	Requesting Technical Support	xi
	Self-Help Online Tools and Resources	xi
	Opening a Case with JTAC	xii
Part 1	Overview	
Chapter 1	IGMP in Subscriber Access Networks	3
	Dynamic IGMP and Subscriber Access	3
Part 2	Configuration	
Chapter 2	Configuration Overview	7
	Dynamic IGMP Configuration Overview	7
Chapter 3	Configuration Tasks for Dynamic IGMP	9
	Configuring Dynamic IGMP	9
Chapter 4	Configuration Statements	11
	[edit dynamic-profiles] Hierarchy Level	11
	accounting (Dynamic IGMP Interface)	19
	disable (Dynamic IGMP)	20
	group (Dynamic IGMP Interface)	21
	group-policy (Dynamic IGMP Interface)	22
	group-limit (Dynamic IGMP Interface)	22
	igmp (Dynamic Profiles)	23
	immediate-leave (Dynamic IGMP Interface)	24
	interface (Dynamic IGMP)	25
	no-accounting	26
	oif-map (Dynamic IGMP Interface)	26
	passive (Dynamic IGMP Interface)	27
	promiscuous-mode (Protocols IGMP)	28
	protocols (Dynamic Profiles)	29
	source (Dynamic IGMP Interface)	30
	ssm-map (Dynamic IGMP Interface)	31

	static (Dynamic IGMP Interface)	31
	version (Dynamic IGMP Interface)	32
Part 3	Administration	
Chapter 5	Monitoring Commands	35
	clear igmp membership	36
	clear igmp statistics	39
	show igmp group	41
	show igmp interface	45
	show igmp statistics	49
Part 4	Troubleshooting	
Chapter 6	Acquiring Troubleshooting Information	55
	Collecting Subscriber Access Logs Before Contacting Juniper Technical Support	55
Part 5	Index	
	Index	61

List of Tables

	About the Documentation	vii
	Table 1: Notice Icons	ix
	Table 2: Text and Syntax Conventions	ix
Part 3	Administration	
Chapter 5	Monitoring Commands	35
	Table 3: show igmp group Output Fields	41
	Table 4: show igmp interface Output Fields	45
	Table 5: show igmp statistics Output Fields	49

About the Documentation

- Documentation and Release Notes on page vii
- Supported Platforms on page vii
- Using the Examples in This Manual on page vii
- Documentation Conventions on page ix
- Documentation Feedback on page xi
- Requesting Technical Support on page xi

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Supported Platforms

For the features described in this document, the following platforms are supported:

- MX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:


```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page ix defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page ix defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none">Introduces or emphasizes important new terms.Identifies guide names.Identifies RFC and Internet draft titles.	<ul style="list-style-type: none">A policy <i>term</i> is a named structure that defines match conditions and actions.<i>Junos OS CLI User Guide</i>RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>

- Search technical bulletins for relevant hardware and software notifications:
<http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

Overview

- [IGMP in Subscriber Access Networks on page 3](#)

CHAPTER 1

IGMP in Subscriber Access Networks

- [Dynamic IGMP and Subscriber Access on page 3](#)

Dynamic IGMP and Subscriber Access

Subscriber access supports the configuration of the Internet Group Management Protocol (IGMP) at the **[edit dynamic-profiles *profile-name* protocols]** hierarchy level. Statements configured at this hierarchy level are identical in function to those same statements used for static IGMP configuration.

- | | |
|------------------------------|---|
| Related Documentation | <ul style="list-style-type: none">• For general information about IGMP, see the <i>Multicast Protocols Feature Guide for Routing Devices</i>. |
|------------------------------|---|

PART 2

Configuration

- [Configuration Overview on page 7](#)
- [Configuration Tasks for Dynamic IGMP on page 9](#)
- [Configuration Statements on page 11](#)

CHAPTER 2

Configuration Overview

- [Dynamic IGMP Configuration Overview on page 7](#)

Dynamic IGMP Configuration Overview

The Internet Group Management Protocol (IGMP) is a host to router signaling protocol for IPv4 used to support IP multicasting. This protocol manages the membership of hosts and routers in multicast groups. IP hosts use IGMP to report their multicast group memberships to any immediately neighboring multicast routers. Multicast routers use IGMP to learn, for each of their attached physical networks, which groups have members.

Subscriber access supports the configuration of IGMP within the **dynamic profiles** hierarchy. By specifying IGMP statements within a dynamic profile, you can dynamically apply IGMP configuration when a subscriber connects to an interface using a particular access technology (DHCP), enabling the subscriber to access a carrier (multicast) network.

Related Documentation

- *Dynamic Profiles Overview*
- *Configuring a Dynamic Profile for Client Access*
- *Configuring IGMP*

CHAPTER 3

Configuration Tasks for Dynamic IGMP

- [Configuring Dynamic IGMP on page 9](#)

Configuring Dynamic IGMP

Configuration for Dynamic IGMP is identical to that performed for static IGMP, with the exception of their being configured at the `[edit dynamic-profiles profile-name protocols igmp]` hierarchy level.

Related Documentation

- For specific IGMP configuration tasks, see the *Multicast Protocols Feature Guide for Routing Devices*.

CHAPTER 4

Configuration Statements

- [\[edit dynamic-profiles\] Hierarchy Level](#) on page 11
- [accounting \(Dynamic IGMP Interface\)](#) on page 19
- [disable \(Dynamic IGMP\)](#) on page 20
- [group \(Dynamic IGMP Interface\)](#) on page 21
- [group-policy \(Dynamic IGMP Interface\)](#) on page 22
- [group-limit \(Dynamic IGMP Interface\)](#) on page 22
- [igmp \(Dynamic Profiles\)](#) on page 23
- [immediate-leave \(Dynamic IGMP Interface\)](#) on page 24
- [interface \(Dynamic IGMP\)](#) on page 25
- [no-accounting](#) on page 26
- [oif-map \(Dynamic IGMP Interface\)](#) on page 26
- [passive \(Dynamic IGMP Interface\)](#) on page 27
- [promiscuous-mode \(Protocols IGMP\)](#) on page 28
- [protocols \(Dynamic Profiles\)](#) on page 29
- [source \(Dynamic IGMP Interface\)](#) on page 30
- [ssm-map \(Dynamic IGMP Interface\)](#) on page 31
- [static \(Dynamic IGMP Interface\)](#) on page 31
- [version \(Dynamic IGMP Interface\)](#) on page 32

[\[edit dynamic-profiles\] Hierarchy Level](#)

```
dynamic-profiles {  
  profile-name {  
    class-of-service {  
      interfaces {  
        interface-name {  
          unit logical-unit-number {  
            classifiers {  
              type (classifier-name | default);  
            }  
            output-traffic-control-profile (profile-name | $junos-cos-traffic-control-profile);  
            rewrite-rules {  
              dscp (rewrite-name | default);  
            }  
          }  
        }  
      }  
    }  
  }  
}
```

```

        dscp-ipv6 (rewrite-name | default);
        ieee-802.1 (rewrite-name | default) vlan-tag (outer | outer-and-inner);
        inet-precedence (rewrite-name | default);
    }
}
}
}
}
scheduler-maps {
    map-name {
        forwarding-class class-name scheduler scheduler-name;
    }
}
schedulers {
    (scheduler-name) {
        buffer-size (percent percentage | remainder | temporal microseconds |
            $junos-cos-scheduler-bs);
        drop-profile-map loss-priority (any | low | medium-low | medium-high | high)
            protocol (any | non-tcp | tcp) drop-profile (profile-name | predefined-variable);
        excess-priority (low | high | $junos-cos-scheduler-excess-priority);
        excess-rate (percent percentage | percent $junos-cos-scheduler-excess-rate);
        overhead-accounting (shaping-mode) <bytes (byte-value>;
        priority (priority-level | $junos-cos-scheduler-priority);
        shaping-rate (rate | predefined-variable);
        transmit-rate (rate | percent percentage | remainder | percent percentage
            $junos-cos-scheduler-tx) <exact | rate-limit>;
    }
}
traffic-control-profiles profile-name {
    delay-buffer-rate (percent percentage | rate);
    excess-rate (percent percentage | proportion value | percent
        $junos-cos-excess-rate);
    guaranteed-rate (percent percentage | rate);
    overhead-accounting (shaping-mode) <bytes (byte-value>;
    scheduler-map map-name;
    shaping-rate (percent percentage | rate | predefined-variable);
}
}
firewall {
    family family {
        fast-update-filter filter-name {
            interface-specific;
            match-order [match-order];
            term term-name {
                from {
                    match-conditions;
                }
                then {
                    action;
                    action-modifiers;
                }
            }
            only-at-create;
        }
        filter filter-name {
            interface-specific;
            term term-name {
                from {

```



```

        match-conditions;
    }
    then {
        action;
        action-modifiers;
    }
}
policer policer-name {
    filter-specific;
    if-exceeding {
        (bandwidth-limit bps | bandwidth-percent percentage);
        burst-size-limit bytes;
    }
    logical-bandwidth-policer;
    logical-interface-policer;
    physical-interface-policer;
    then {
        policer-action;
    }
}
hierarchical-policer policer-name {
    aggregate {
        if-exceeding {
            bandwidth-limit-limit bps;
            burst-size-limit bytes;
        }
        then {
            policer-action;
        }
    }
    premium {
        if-exceeding {
            bandwidth-limit bps;
            burst-size-limit bytes;
        }
        then {
            policer-action;
        }
    }
}
three-color-policer policer-name {
    action {
        loss-priority high then discard;
    }
    logical-interface-policer;
    single-rate {
        (color-aware | color-blind);
        committed-burst-size bytes;
        committed-information-rate bps;
        excess-burst-size bytes;
    }
    two-rate {
        (color-aware | color-blind);
        committed-burst-size bytes;
        committed-information-rate bps;
        peak-burst-size bytes;
    }
}

```

```

        peak-information-rate bps;
    }
}
}
policy-options {
    prefix-list name {
        ip-addresses;
    }
}
interfaces {
    interface-name {
        unit logical-unit-number {
            family family {
                access-concentrator name;
                address address;
                direct-connect;
                duplicate-protection;
                dynamic-profile profile-name;
                filter {
                    adf {
                        counter;
                        input-precedence precedence;
                        not-mandatory;
                        output-precedence precedence;
                        rule rule-value;
                    }
                    input filter-name {
                        precedence precedence;
                        shared-name filter-shared-name;
                    }
                    output filter-name {
                        precedence precedence;
                        shared-name filter-shared-name;
                    }
                }
            }
            max-sessions number;
            max-sessions-vsa-ignore;
            rpf-check {
                fail-filter filter-name;
                mode loose;
            }
            service {
                input {
                    service-set service-set-name {
                        service-filter filter-name;
                    }
                    post-service-filter filter-name;
                }
                output {
                    service-set service-set-name {
                        service-filter filter-name;
                    }
                }
            }
        }
    }
    service-name-table table-name;
}

```

```

        short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max
            maximum-seconds>;
        unnumbered-address interface-name <preferred-source-address address>;
    }
    ppp-options {
        chap;
        pap;
    }
    vlan-id number;
}
vlan-tagging;
}
interface-set interface-set-name {
    interface interface-name {
        unit logical-unit-number;
    }
}
demux0 {
    unit logical-unit-number {
        demux-options {
            underlying-interface interface-name
        }
        demux-source {
            source-prefix;
        }
        family family {
            access-concentrator name;
            address address;
            direct-connect;
            duplicate-protection;
            dynamic-profile profile-name;
            filter {
                input filter-name;
                output filter-name;
            }
            mac-validate (loose | strict);
            max-sessions number;
            max-sessions-vsa-ignore;
            service-name-table table-name;
            short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max
                maximum-seconds>;
            unnumbered-address interface-name <preferred-source-address address>;
        }
    }
}
}
pp0 {
    unit logical-unit-number {
        keepalives interval seconds;
        no-keepalives;
        pppoe-options {
            underlying-interface interface-name;
            server;
        }
        ppp-options {
            authentication [ authentication-protocols ];
            chap {

```

```
challenge-length minimum minimum-length maximum maximum-length;
}
pap;
}
family inet {
    unnumbered-address interface-name address;
    address address;
    service {
        input {
            service-set service-set-name {
                service-filter filter-name;
            }
            post-service-filter filter-name;
        }
        output {
            service-set service-set-name {
                service-filter filter-name;
            }
        }
    }
    filter {
        input filter-name {
            precedence precedence;
        }
        output filter-name {
            precedence precedence;
        }
    }
}
}
}
}
protocols {
    igmp {
        interface interface-name {
            accounting;
            disable;
            group-policy;
            immediate-leave
            no-accounting;
            promiscuous-mode;
            ssm-map ssm-map-name;
            static {
                group group {
                    source source;
                }
            }
            version version;
        }
    }
    mld {
        interface interface-name {
            disable;
            (accounting | no-accounting);
            group-policy;
            immediate-leave;
            oif-map;
```

```

    passive;
    ssm-map ssm-map-name;
    static {
        group mcast-group-address {
            exclude;
            group-count number;
            group-increment increment;
            source ip-address {
                source-count number;
                source-increment increment;
            }
        }
    }
    version version;
}
}
router-advertisement {
    interface interface-name {
        current-hop-limit number;
        default-lifetime seconds;
        (managed-configuration | no-managed-configuration);
        max-advertisement-interval seconds;
        min-advertisement-interval seconds;
        (other-stateful-configuration | no-other-stateful-configuration);
        prefix prefix {
            (autonomous | no-autonomous);
            (on-link | no-on-link);
            preferred-lifetime seconds;
            valid-lifetime seconds;
        }
        reachable-time milliseconds;
        retransmit-timer milliseconds;
    }
}
}
}
}
routing-instances routing-instance-name {
    interface interface-name;
    routing-options {
        access {
            route prefix {
                next-hop next-hop;
                metric route-cost;
                preference route-distance;
                tag route-tag;
            }
        }
    }
    access-internal {
        route subscriber-ip-address {
            qualified-next-hop underlying-interface {
                mac-address address;
            }
        }
    }
}
multicast {

```

```
        interface interface-name {
            no-qos-adjust;
        }
    }
}
rib routing-table-name {
    access {
        route prefix {
            next-hop next-hop;
            metric route-cost;
            preference route-distance;
            tag route-tag;
        }
    }
    access-internal {
        route subscriber-ip-address {
            qualified-next-hop underlying-interface {
                mac-address address;
            }
        }
    }
}
}
routing-options {
    access {
        route prefix {
            next-hop next-hop;
            metric route-cost;
            preference route-distance;
            tag route-tag;
        }
    }
    access-internal {
        route subscriber-ip-address {
            qualified-next-hop underlying-interface {
                mac-address address;
            }
        }
    }
}
multicast {
    interface interface-name {
        no-qos-adjust;
    }
}
}
variables {
    variable-name {
        default-value default-value;
        equals expression;
        mandatory;
        uid;
        uid-reference;
    }
}
}
```

Related Documentation	<ul style="list-style-type: none">• <i>Dynamic Profiles Overview</i>• <i>CoS for Subscriber Access Overview</i>• <i>Configuring a Basic Dynamic Profile</i>• <i>Configuring Static Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access</i>• <i>Two-Color Policer Configuration Overview</i>• <i>Three-Color Policer Configuration Overview</i>• <i>Hierarchical Policer Configuration Overview</i>• <i>Guidelines for Applying Traffic Policers</i>
------------------------------	---

accounting (Dynamic IGMP Interface)

Syntax	(accounting no-accounting);
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>],
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Enable or disable the collection of IGMP join and leave event statistics for dynamically created IGMP interfaces.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring a Dynamic Profile for Client Access</i>• <i>Recording IGMP Join and Leave Events</i>

disable (Dynamic IGMP)

Syntax	"disable:\$junos-igmp-enable";
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>],
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Disable IGMP on the interface.



NOTE: Though the purpose of this statement is to disable IGMP on interfaces, under the dynamic-profiles hierarchy you can use this statement and an enable variable (disable:\$junos-igmp-enable) to ensure that IGMP is not disabled by a AAA-based authentication and management method (RADIUS).

Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring a Dynamic Profile for Client Access</i>• <i>Disabling IGMP</i>

group (Dynamic IGMP Interface)

Syntax For group configuration with a source, use the following syntax:

```
group ip-address {
  source ip-address;
}
```

For group configuration without a source, use the following syntax:

```
group group;
```

Hierarchy Level [edit dynamic-profiles *profile-name* protocols **igmp interface** *interface-name* **static**],

Release Information Statement introduced in Junos OS Release 9.2.

Description When configuring with a source address, configure the IGMP multicast group address that receives data on an interface and a source address for certain packets. For configuration without a source address, configure only the IGMP multicast group address that receives data on an interface.

Options *ip-address*—Group IP address.

group—Name of group.



NOTE: You must specify a unique address for each group.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring a Dynamic Profile for Client Access*
- *Enabling IGMP Static Group Membership*

group-policy (Dynamic IGMP Interface)

Syntax	<code>group-policy <i>policy-name</i>;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Compare the IGMPv2 or IGMPv3 group against the specified group policy, after receiving an IGMP report, and perform the action configured in that policy (for example, reject the report).
Options	<i>policy-name</i> —Name of the group policy.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring a Dynamic Profile for Client Access</i>• <i>Filtering Unwanted IGMP Reports at the IGMP Interface Level</i>

group-limit (Dynamic IGMP Interface)

Syntax	<code>group-limit <i>limit</i>;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>],
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Configure a limit for the number of multicast groups (or [S,G] channels in IGMPv3) allowed on a dynamic logical interface. After this limit is reached, new reports will be ignored and all related flows are not flooded on the logical interface.
Default	By default, there is no limit to the number of multicast groups that can join the interface.
Options	<i>limit</i> —group limit value for the interface. Range: 1 through 32767
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring a Dynamic Profile for Client Access</i>• <i>Limiting the Number of IGMP Multicast Group Joins on Logical Interfaces</i>

igmp (Dynamic Profiles)

Syntax	<pre> igmp { interface <i>interface-name</i> { accounting; disable; group-limit <i>policy-name</i>; group-policy; immediate-leave; no-accounting; oif-map <i>map-name</i>; passive <allow-receive> <send-general-query> <send-group-query>; promiscuous-mode; ssm-map <i>ssm-map-name</i>; static { group <i>group</i> { source <i>source</i>; } } version <i>version</i>; } } </pre>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols], [edit logical-systems <i>logical-system-name</i> protocols], [edit protocols]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Enable IGMP on the router. IGMP must be enabled for the router to receive multicast packets.
Default	IGMP is disabled on the router. IGMP is automatically enabled on all broadcast interfaces when you configure Protocol Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP).
Options	The statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring a Dynamic Profile for Client Access</i> • <i>Understanding IGMP</i> • <i>Enabling IGMP</i>

immediate-leave (Dynamic IGMP Interface)

Syntax	immediate-leave;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>],
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Enable the routing device to leave the multicast group immediately after the last host leaves the multicast group.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring a Dynamic Profile for Client Access</i>• <i>Specifying Immediate-Leave Host Removal for IGMP</i>

interface (Dynamic IGMP)

Syntax	<pre> interface <i>interface-name</i> { accounting; disable; group-policy; immediate-leave no-accounting; oif-map; passive; promiscuous-mode; ssm-map <i>ssm-map-name</i>; static { group <i>group</i> { source <i>source</i>; } } version <i>version</i>; } </pre>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Enable IGMP on an interface and configure interface-specific properties.
Options	<p><i>interface-name</i>—Variable for the interface. Specify the interface variable (\$junos-interface-name) to indicate that the dynamic profile chooses an interface for the accessing DHCP client.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring a Dynamic Profile for Client Access Enabling IGMP


no-accounting

Syntax	no-accounting;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Disable the collection of IGMP join and leave event statistics on a per-interface basis.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring a Dynamic Profile for Client Access</i>• <i>Recording IGMP Join and Leave Events</i>

oif-map (Dynamic IGMP Interface)

Syntax	oif-map <i>map-name</i> ;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Associates an OIF map to the IGMP interface using a dynamic profile. The OIF map is a routing policy statement that can contain multiple terms.
Options	<i>map-name</i> —Name of the OIF map.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring Multicast with Subscriber VLANs</i>• <i>Configuring a Dynamic Profile for Client Access</i>

passive (Dynamic IGMP Interface)

Syntax	<code>passive <allow-receive> <send-general-query> <send-group-query>;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6. allow-receive , send-general-query , and send-group-query options were introduced in Junos OS Release 10.0.
Description	Dynamically specify that IGMP run on the interface and either not send and receive control traffic or selectively send and receive control traffic such as IGMP reports, queries, and leaves.
<div>  <p>NOTE: You can selectively activate up to two out of the three available options for the passive statement while keeping the other functions passive (inactive). Activating all three options would be equivalent to not using the passive statement.</p> </div>	
Options	<p>allow-receive—(Optional) Enables IGMP to receive control traffic on the interface.</p> <p>send-general-query—(Optional) Enables IGMP to send general queries on the interface.</p> <p>send-group-query—(Optional) Enables IGMP to send group-specific and group-source-specific queries on the interface.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring Multicast with Subscriber VLANs</i> • <i>Configuring IGMP</i>

promiscuous-mode (Protocols IGMP)

Syntax	promiscuous-mode;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 9.2 for dynamic profiles. Statement introduced in Junos OS Release 12.1 for the QFX Series.
Description	Specify that the interface accepts IGMP reports from hosts on any subnetwork. Note that when enabling promiscuous-mode, all routing devices on the ethernet segment must be configured with the promiscuous mode statement. Otherwise, only the interface configured with lowest IPv4 address acts as the querier for IGMP for this Ethernet segment.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring a Dynamic Profile for Client Access</i>• <i>Accepting IGMP Messages from Remote Subnetworks</i>

protocols (Dynamic Profiles)

```

Syntax protocols {
    igmp {
        interface interface-name {
            accounting;
            disable;
            group-policy;
            immediate-leave
            no-accounting;
            promiscuous-mode;
            ssm-map ssm-map-name;
            static {
                group group {
                    source source;
                }
            }
            version version;
        }
    }
    mld {
        interface interface-name {
            disable;
            (accounting | no-accounting);
            group-policy;
            immediate-leave;
            oif-map;
            passive;
            ssm-map ssm-map-name;
            static {
                group multicast-group-address {
                    exclude;
                    group-count number;
                    group-increment increment;
                    source ip-address {
                        source-count number;
                        source-increment increment;
                    }
                }
            }
            version version;
        }
    }
    router-advertisement {
        interface interface-name {
            current-hop-limit number;
            default-lifetime seconds;
            (managed-configuration | no-managed-configuration);
            max-advertisement-interval seconds;
            min-advertisement-interval seconds;
            (other-stateful-configuration | no-other-stateful-configuration);
            prefix prefix;
            reachable-time milliseconds;
            retransmit-timer milliseconds;
        }
    }
}

```

```
    }  
  }  
}
```

Hierarchy Level	[edit dynamic-profiles <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 9.2. Support at the [edit dynamic-profiles <i>profile-name</i> protocols mld] and [edit dynamic-profiles <i>profile-name</i> protocols router-advertisement] hierarchy levels introduced in Junos OS Release 10.1.
Description	Enable IGMP on the router. IGMP must be enabled for the router to receive multicast packets.
Default	IGMP is disabled on the router. IGMP is automatically enabled on all broadcast interfaces when you configure Protocol Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP). The statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring IGMP</i>• <i>Examples: Configuring MLD</i>

source (Dynamic IGMP Interface)

Syntax	source <i>source</i> ;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i> static]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Specify the IP version 4 (IPv4) unicast address to send data on an interface.
Options	source —IPv4 unicast address.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring a Dynamic Profile for Client Access</i>• <i>Enabling IGMP Static Group Membership</i>

ssm-map (Dynamic IGMP Interface)

Syntax	<code>ssm-map <i>ssm-map-name</i>;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Apply an SSM map to an IGMP interface.
Options	<i>ssm-map-name</i> —Name of SSM map.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring a Dynamic Profile for Client Access</i> • <i>Source-Specific Multicast Groups Overview</i>

static (Dynamic IGMP Interface)

Syntax	<pre>static { group group; group group { source source; } }</pre>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Test multicast forwarding on an interface without a receiver host.
Options	The remaining statements are explained separately.
Required Privilege Level	routing and trace—To view this statement in the configuration. routing-control and trace-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring a Dynamic Profile for Client Access</i> • <i>Enabling IGMP Static Group Membership</i>

version (Dynamic IGMP Interface)

Syntax	<code>version version;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmpinterface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Specify the version of IGMP.
Options	version —IGMP version number. Range: 1, 2, or 3 Default: IGMP version 2



NOTE: Routers running different versions of IGMP negotiate the lowest common version of IGMP that is supported by hosts on their subnet and operate in that version.

If you have already configured the router to use IGMP version 1 and then configure it to use IGMP version 2, the router continues to use IGMP version 1 for up to 6 minutes and then uses IGMP version 2.

Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring a Dynamic Profile for Client Access</i>• <i>Changing the IGMP Version</i>

PART 3

Administration

- [Monitoring Commands on page 35](#)

CHAPTER 5

Monitoring Commands

- `clear igmp membership`
- `clear igmp statistics`
- `show igmp group`
- `show igmp interface`
- `show igmp statistics`

clear igmp membership

Syntax	clear igmp membership <group <i>address-range</i> > <interface <i>interface-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch and the QFX Series)	clear igmp membership <group <i>address-range</i> > <interface <i>interface-name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.3 for the QFX Series.
Description	Clear Internet Group Management Protocol (IGMP) group members.
Options	<p>none—Clear all IGMP members on all interfaces and for all address ranges.</p> <p>group <i>address-range</i>—(Optional) Clear all IGMP members that are in a particular address range. An example of a range is 224.2/16. If you omit the destination prefix length, the default is /32.</p> <p>interface <i>interface-name</i>—(Optional) Clear all IGMP group members on an interface.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show igmp group on page 41 • show igmp interface on page 45
List of Sample Output	clear igmp membership on page 36 clear igmp membership interface on page 37 clear igmp membership group on page 37
Output Fields	See show igmp group for an explanation of output fields.

Sample Output

clear igmp membership

The following sample output displays IGMP group information before and after the **clear igmp membership** command is entered:

```
user@host> show igmp group
Interface      Group           Last Reported   Timeout
so-0/0/0       224.2.127.253   10.1.128.1      186
so-0/0/0       224.2.127.254   10.1.128.1      186
so-0/0/0       239.255.255.255 10.1.128.1      187
```


so-0/0/0	224.1.127.255	10.1.128.1	188
local	224.0.0.6	(null)	0
local	224.0.0.5	(null)	0
local	224.2.127.254	(null)	0
local	239.255.255.255	(null)	0
local	224.0.0.2	(null)	0
local	224.0.0.13	(null)	0

```

user@host> clear igmp membership
Clearing Group Membership Info for so-0/0/0
Clearing Group Membership Info for so-1/0/0
Clearing Group Membership Info for so-2/0/0

```

```

user@host> show igmp group
Interface      Group          Last Reported  Timeout
local         224.0.0.6      (null)         0
local         224.0.0.5      (null)         0
local         224.2.127.254  (null)         0
local         239.255.255.255 (null)         0
local         224.0.0.2      (null)         0
local         224.0.0.13     (null)         0

```

clear igmp membership interface

The following sample output displays IGMP group information before and after the **clear igmp membership interface** command is issued:

```

user@host> show igmp group
Interface      Group          Last Reported  Timeout
so-0/0/0       224.2.127.253  10.1.128.1     210
so-0/0/0       239.255.255.255 10.1.128.1     210
so-0/0/0       224.1.127.255   10.1.128.1     215
so-0/0/0       224.2.127.254   10.1.128.1     216
local         224.0.0.6      (null)         0
local         224.0.0.5      (null)         0
local         224.2.127.254  (null)         0
local         239.255.255.255 (null)         0
local         224.0.0.2      (null)         0
local         224.0.0.13     (null)         0

```

```

user@host> clear igmp membership interface so-0/0/0
Clearing Group Membership Info for so-0/0/0

```

```

user@host> show igmp group
Interface      Group          Last Reported  Timeout
local         224.0.0.6      (null)         0
local         224.0.0.5      (null)         0
local         224.2.127.254  (null)         0
local         239.255.255.255 (null)         0
local         224.0.0.2      (null)         0
local         224.0.0.13     (null)         0

```

clear igmp membership group

The following sample output displays IGMP group information before and after the **clear igmp membership group** command is entered:

```

user@host> show igmp group

```

Interface	Group	Last Reported	Timeout
so-0/0/0	224.2.127.253	10.1.128.1	210
so-0/0/0	239.255.255.255	10.1.128.1	210
so-0/0/0	224.1.127.255	10.1.128.1	215
so-0/0/0	224.2.127.254	10.1.128.1	216
local	224.0.0.6	(null)	0
local	224.0.0.5	(null)	0
local	224.2.127.254	(null)	0
local	239.255.255.255	(null)	0
local	224.0.0.2	(null)	0
local	224.0.0.13	(null)	0

```
user@host> clear igmp membership group 239.225/16
Clearing Group Membership Range 239.225.0.0/16 on so-0/0/0
Clearing Group Membership Range 239.225.0.0/16 on so-1/0/0
Clearing Group Membership Range 239.225.0.0/16 on so-2/0/0
```

```
user@host> show igmp group
```

Interface	Group	Last Reported	Timeout
so-0/0/0	224.1.127.255	10.1.128.1	231
so-0/0/0	224.2.127.254	10.1.128.1	233
so-0/0/0	224.2.127.253	10.1.128.1	236
local	224.0.0.6	(null)	0
local	224.0.0.5	(null)	0
local	224.2.127.254	(null)	0
local	239.255.255.255	(null)	0
local	224.0.0.2	(null)	0
local	224.0.0.13	(null)	0

clear igmp statistics

Syntax	clear igmp statistics <interface <i>interface-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switches)	clear igmp statistics <interface <i>interface-name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.3 for the QFX Series.
Description	Clear Internet Group Management Protocol (IGMP) statistics.
Options	<p>none—Clear IGMP statistics on all interfaces.</p> <p>interface <i>interface-name</i>—(Optional) Clear IGMP statistics for the specified interface only.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show igmp statistics on page 49
List of Sample Output	clear igmp statistics on page 39
Output Fields	See show igmp statistics for an explanation of output fields.

Sample Output

clear igmp statistics

The following sample output displays IGMP statistics information before and after the **clear igmp statistics** command is entered:

```

user@host> show igmp statistics
IGMP packet statistics for all interfaces
IGMP Message type      Received      Sent  Rx errors
Membership Query        8883         459      0
V1 Membership Report    0            0        0
DVMRP                   19784        35476    0
PIM V1                  18310        0        0
Cisco Trace             0            0        0
V2 Membership Report    0            0        0
Group Leave             0            0        0
Mtrace Response         0            0        0
Mtrace Request          0            0        0
Domain Wide Report      0            0        0
V3 Membership Report    0            0        0

```

Other Unknown types	0
IGMP v3 unsupported type	0
IGMP v3 source required for SSM	0
IGMP v3 mode not applicable for SSM	0

IGMP Global Statistics	
Bad Length	0
Bad Checksum	0
Bad Receive If	0
Rx non-local	1227

```
user@host> clear igmp statistics
```

```
user@host> show igmp statistics
```

IGMP packet statistics for all interfaces

IGMP Message type	Received	Sent	Rx errors
Membership Query	0	0	0
V1 Membership Report	0	0	0
DVMRP	0	0	0
PIM V1	0	0	0
Cisco Trace	0	0	0
V2 Membership Report	0	0	0
Group Leave	0	0	0
Mtrace Response	0	0	0
Mtrace Request	0	0	0
Domain Wide Report	0	0	0
V3 Membership Report	0	0	0
Other Unknown types			0
IGMP v3 unsupported type			0
IGMP v3 source required for SSM			0
IGMP v3 mode not applicable for SSM			0
IGMP Global Statistics			
Bad Length	0		
Bad Checksum	0		
Bad Receive If	0		
Rx non-local	0		

show igmp group

Syntax	show igmp group <brief detail> <group-name> <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch and the QFX Series)	show igmp group <brief detail> <group-name>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.3 for the QFX Series.
Description	Display Internet Group Management Protocol (IGMP) group membership information.
Options	<p>none—Display standard information about membership for all IGMP groups.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>group-name—(Optional) Display group membership for the specified IP address only.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear igmp membership on page 36
List of Sample Output	show igmp group (Include Mode) on page 42 show igmp group (Exclude Mode) on page 43 show igmp group brief on page 43 show igmp group detail on page 43
Output Fields	Table 3 on page 41 describes the output fields for the show igmp group command. Output fields are listed in the approximate order in which they appear.

Table 3: show igmp group Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface that received the IGMP membership report. A name of local indicates that the local routing device joined the group itself.	All levels
Group	Group address.	All levels
Group Mode	Mode the SSM group is operating in: Include or Exclude .	All levels
Source	Source address.	All levels

Table 3: show igmp group Output Fields (*continued*)

Field Name	Field Description	Level of Output
Source timeout	Time remaining until the group traffic is no longer forwarded. The timer is refreshed when a listener in include mode sends a report. A group in exclude mode or configured as a static group displays a zero timer.	detail
Last reported by	Address of the host that last reported membership in this group.	All levels
Timeout	Time remaining until the group membership is removed.	brief none
Group timeout	Time remaining until a group in exclude mode moves to include mode. The timer is refreshed when a listener in exclude mode sends a report. A group in include mode or configured as a static group displays a zero timer.	detail
Type	Type of group membership: <ul style="list-style-type: none"> • Dynamic—Host reported the membership. • Static—Membership is configured. 	All levels

Sample Output

show igmp group (Include Mode)

```

user@host> show igmp group
Interface: t1-0/1/0.0
  Group: 232.1.1.1
    Group mode: Include
    Source: 10.0.0.2
    Last reported by: 10.9.5.2
    Timeout:      24 Type: Dynamic
  Group: 232.1.1.1
    Group mode: Include
    Source: 10.0.0.3
    Last reported by: 10.9.5.2
    Timeout:      24 Type: Dynamic
  Group: 232.1.1.1
    Group mode: Include
    Source: 10.0.0.4
    Last reported by: 10.9.5.2
    Timeout:      24 Type: Dynamic
  Group: 232.1.1.2
    Group mode: Include
    Source: 10.0.0.4
    Last reported by: 10.9.5.2
    Timeout:      24 Type: Dynamic
Interface: t1-0/1/1.0
Interface: ge-0/2/2.0
Interface: ge-0/2/0.0
Interface: local
  Group: 224.0.0.2
    Source: 0.0.0.0
    Last reported by: Local
    Timeout:      0 Type: Dynamic
  Group: 224.0.0.22
    Source: 0.0.0.0

```

```

Last reported by: Local
Timeout:          0 Type: Dynamic

```

show igmp group (Exclude Mode)

```

user@host> show igmp group
Interface: t1-0/1/0.0
Interface: t1-0/1/1.0
Interface: ge-0/2/2.0
Interface: ge-0/2/0.0
Interface: local
  Group: 224.0.0.2
    Source: 0.0.0.0
    Last reported by: Local
    Timeout:          0 Type: Dynamic
  Group: 224.0.0.22
    Source: 0.0.0.0
    Last reported by: Local
    Timeout:          0 Type: Dynamic

```

show igmp group brief

The output for the **show igmp group brief** command is identical to that for the **show igmp group** command.

show igmp group detail

```

user@host> show igmp group detail
Interface: t1-0/1/0.0
  Group: 232.1.1.1
    Group mode: Include
    Source: 10.0.0.2
    Source timeout: 12
    Last reported by: 10.9.5.2
    Group timeout:          0 Type: Dynamic
  Group: 232.1.1.1
    Group mode: Include
    Source: 10.0.0.3
    Source timeout: 12
    Last reported by: 10.9.5.2
    Group timeout:          0 Type: Dynamic
  Group: 232.1.1.1
    Group mode: Include
    Source: 10.0.0.4
    Source timeout: 12
    Last reported by: 10.9.5.2
    Group timeout:          0 Type: Dynamic
  Group: 232.1.1.2
    Group mode: Include
    Source: 10.0.0.4
    Source timeout: 12
    Last reported by: 10.9.5.2
    Group timeout:          0 Type: Dynamic
Interface: t1-0/1/1.0
Interface: ge-0/2/2.0
Interface: ge-0/2/0.0
Interface: local
  Group: 224.0.0.2
    Group mode: Exclude
    Source: 0.0.0.0
    Source timeout: 0

```

```
      Last reported by: Local
      Group timeout:      0 Type: Dynamic
Group: 224.0.0.22
      Group mode: Exclude
      Source: 0.0.0.0
      Source timeout: 0
      Last reported by: Local
      Group timeout:      0 Type: Dynamic
```


show igmp interface

Syntax	show igmp interface <brief detail> <interface-name> <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switches and the QFX Series)	show igmp interface <brief detail> <interface-name>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.3 for the QFX Series.
Description	Display information about Internet Group Management Protocol (IGMP)-enabled interfaces.
Options	<p>none—Display standard information about all IGMP-enabled interfaces.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>interface-name—(Optional) Display information about the specified IGMP-enabled interface only.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear igmp membership on page 36
List of Sample Output	show igmp interface on page 47 show igmp interface brief on page 47 show igmp interface detail on page 48 show igmp interface <interface-name> on page 48
Output Fields	Table 4 on page 45 describes the output fields for the show igmp interface command. Output fields are listed in the approximate order in which they appear.

Table 4: show igmp interface Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface.	All levels
Querier	Address of the routing device that has been elected to send membership queries.	All levels
State	State of the interface: Up or Down .	All levels

Table 4: show igmp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
SSM Map Policy	Name of the source-specific multicast (SSM) map policy that has been applied to the IGMP interface.	All levels
Timeout	How long until the IGMP querier is declared to be unreachable, in seconds.	All levels
Version	IGMP version being used on the interface: 1, 2, or 3.	All levels
Groups	Number of groups on the interface.	All levels
Group limit	Maximum number of groups allowed on the interface. Any joins requested after the limit is reached are rejected.	All levels
Group threshold	Configured threshold at which a warning message is generated. This threshold is based on a percentage of groups received on the interface. If the number of groups received reaches the configured threshold, the device generates a warning message.	All levels
Group log-interval	Time (in seconds) between consecutive log messages.	All levels
Immediate Leave	State of the immediate leave option: <ul style="list-style-type: none"> • On—Indicates that the router removes a host from the multicast group as soon as the router receives a leave group message from a host associated with the interface. • Off—Indicates that after receiving a leave group message, instead of removing a host from the multicast group immediately, the router sends a group query to determine if another receiver responds. 	All levels
Promiscuous Mode	State of the promiscuous mode option: <ul style="list-style-type: none"> • On—Indicates that the router can accept IGMP reports from subnetworks that are not associated with its interfaces. • Off—Indicates that the router can accept IGMP reports only from subnetworks that are associated with its interfaces. 	All levels
Passive	State of the passive mode option: <ul style="list-style-type: none"> • On—Indicates that the router can run IGMP on the interface but not send or receive control traffic such as IGMP reports, queries, and leaves. • Off—Indicates that the router can run IGMP on the interface and send or receive control traffic such as IGMP reports, queries, and leaves. <p>The passive statement enables you to selectively activate up to two out of a possible three available query or control traffic options. When enabled, the following options appear after the on state declaration:</p> <ul style="list-style-type: none"> • send-general-query—The interface sends general queries. • send-group-query—The interface sends group-specific and group-source-specific queries. • allow-receive—The interface receives control traffic. 	All levels
OIF map	Name of the OIF map (if configured) associated with the interface.	All levels

Table 4: show igmp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
SSM map	Name of the source-specific multicast (SSM) map (if configured) used on the interface.	All levels
Configured Parameters	Information configured by the user: <ul style="list-style-type: none"> IGMP Query Interval—Interval (in seconds) at which this router sends membership queries when it is the querier. IGMP Query Response Interval—Time (in seconds) that the router waits for a report in response to a general query. IGMP Last Member Query Interval—Time (in seconds) that the router waits for a report in response to a group-specific query. IGMP Robustness Count—Number of times the router retries a query. 	All levels
Derived Parameters	Derived information: <ul style="list-style-type: none"> IGMP Membership Timeout—Timeout period (in seconds) for group membership. If no report is received for these groups before the timeout expires, the group membership is removed. IGMP Other Querier Present Timeout—Time (in seconds) that the router waits for the IGMP querier to send a query. 	All levels

Sample Output

show igmp interface

```

user@host> show igmp interface
Interface: at-0/3/1.0
  Querier: 10.111.30.1
  State:      Up Timeout:   None Version:  2 Groups:    4
  SSM Map Policy: ssm-policy-A
Interface: so-1/0/0.0
  Querier: 10.111.10.1
  State:      Up Timeout:   None Version:  2 Groups:    2
  SSM Map Policy: ssm-policy-B
Interface: so-1/0/1.0
  Querier: 10.111.20.1
  State:      Up Timeout:   None Version:  2 Groups:    4
  SSM Map Policy: ssm-policy-C
Immediate Leave: On
Promiscuous Mode: Off

Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2

Derived Parameters:
IGMP Membership Timeout: 260.0
IGMP Other Querier Present Timeout: 255.0

```

show igmp interface brief

The output for the **show igmp interface brief** command is identical to that for the **show igmp interface** command. For sample output, see [show igmp interface on page 47](#).

show igmp interface detail

The output for the **show igmp interface detail** command is identical to that for the **show igmp interface** command. For sample output, see [show igmp interface on page 47](#).

show igmp interface <interface-name>

```
user@host# show igmp interface ge-3/2/0.0
Interface: ge-3/2/0.0
Querier: 20.1.1.1
State: Up Timeout:    None Version:  3 Groups:    1
Group limit: 8
Group threshold: 60
Group log-interval: 10
Immediate leave: Off
Promiscuous mode: Off
```

show igmp statistics

Syntax	show igmp statistics <brief detail> <interface <i>interface-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch and the QFX Series)	show igmp statistics <brief detail> <interface <i>interface-name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.3 for the QFX Series.
Description	Display Internet Group Management Protocol (IGMP) statistics.
Options	<p>none—Display IGMP statistics for all interfaces.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>interface <i>interface-name</i>—(Optional) Display IGMP statistics about the specified interface only.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear igmp statistics on page 39
List of Sample Output	show igmp statistics on page 50 show igmp statistics interface on page 51
Output Fields	<p>Table 5 on page 49 describes the output fields for the show igmp statistics command. Output fields are listed in the approximate order in which they appear.</p>

Table 5: show igmp statistics Output Fields

Field Name	Field Description
IGMP packet statistics	Heading for IGMP packet statistics for all interfaces or for the specified interface name.

Table 5: show igmp statistics Output Fields (*continued*)

Field Name	Field Description
IGMP Message type	<p>Summary of IGMP statistics:</p> <ul style="list-style-type: none"> • Membership Query—Number of membership queries sent and received. • V1 Membership Report—Number of version 1 membership reports sent and received. • DVMRP—Number of DVMRP messages sent or received. • PIM V1—Number of PIM version 1 messages sent or received. • Cisco Trace—Number of Cisco trace messages sent or received. • V2 Membership Report—Number of version 2 membership reports sent or received. • Group Leave—Number of group leave messages sent or received. • Mtrace Response—Number of Mtrace response messages sent or received. • Mtrace Request—Number of Mtrace request messages sent or received. • Domain Wide Report—Number of domain-wide reports sent or received. • V3 Membership Report—Number of version 3 membership reports sent or received. • Other Unknown types—Number of unknown message types received. • IGMP v3 unsupported type—Number of messages received with unknown and unsupported IGMP version 3 message types. • IGMP v3 source required for SSM—Number of IGMP version 3 messages received that contained no source. • IGMP v3 mode not applicable for SSM—Number of IGMP version 3 messages received that did not contain a mode applicable for source-specific multicast (SSM).
Received	Number of messages received.
Sent	Number of messages sent.
Rx errors	Number of received packets that contained errors.
IGMP Global Statistics	<p>Summary of IGMP statistics for all interfaces.</p> <ul style="list-style-type: none"> • Bad Length—Number of messages received with length errors so severe that further classification could not occur. • Bad Checksum—Number of messages received with a bad IP checksum. No further classification was performed. • Bad Receive If—Number of messages received on an interface not enabled for IGMP. • Rx non-local—Number of messages received from senders that are not local. • Timed out—Number of groups that timed out as a result of not receiving an explicit leave message. • Rejected Report—Number of reports dropped because of the IGMP group policy. • Total Interfaces—Number of interfaces configured to support IGMP.

Sample Output

show igmp statistics

```

user@host> show igmp statistics
IGMP packet statistics for all interfaces
IGMP Message type      Received      Sent  Rx errors
Membership Query        8883         459      0
V1 Membership Report     0            0        0

```

DVMRP	0	0	0
PIM V1	0	0	0
Cisco Trace	0	0	0
V2 Membership Report	0	0	0
Group Leave	0	0	0
Mtrace Response	0	0	0
Mtrace Request	0	0	0
Domain Wide Report	0	0	0
V3 Membership Report	0	0	0
Other Unknown types			0
IGMP v3 unsupported type			0
IGMP v3 source required for SSM			0
IGMP v3 mode not applicable for SSM			0
IGMP Global Statistics			
Bad Length	0		
Bad Checksum	0		
Bad Receive If	0		
Rx non-local	1227		
Timed out	0		
Rejected Report	0		
Total Interfaces	2		

show igmp statistics interface

```

user@host> show igmp statistics interface fe-1/0/1.0
IGMP interface packet statistics for fe-1/0/1.0
IGMP Message type      Received      Sent  Rx errors
Membership Query        0           230      0
V1 Membership Report    0           0        0

```


PART 4

Troubleshooting

- [Acquiring Troubleshooting Information on page 55](#)

CHAPTER 6

Acquiring Troubleshooting Information

- [Collecting Subscriber Access Logs Before Contacting Juniper Technical Support on page 55](#)

Collecting Subscriber Access Logs Before Contacting Juniper Technical Support

Problem When you experience a subscriber access problem in your network, we recommend that you collect certain logs before you contact Juniper Technical Support. This topic shows you the most useful logs for a variety of network implementations. In addition to the relevant log information, you must also collect standard troubleshooting information and send it to Juniper Technical Support in your request for assistance.

Solution To collect standard troubleshooting information:

- Redirect the command output to a file.

```
user@host> request support information | save rsi-1
```

To configure logging to assist Juniper Technical Support:

1. Review the following blocks of statements to determine which apply to your configuration.

[edit]

```
set system syslog archive size 100m files 25
set system auto-configuration traceoptions file filename
set system auto-configuration traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions level all
set protocols ppp-service traceoptions flag all
set protocols ppp traceoptions file filename size 100m files 25
set protocols ppp traceoptions level all
set protocols ppp traceoptions flag all
set protocols ppp monitor-session all
set interfaces pp0 traceoptions flag all
set demux traceoptions file filename size 100m files 25
set demux traceoptions level all
set demux traceoptions flag all
set system processes dhcp-service traceoptions file filename
set system processes dhcp-service traceoptions file size 100m
set system processes dhcp-service traceoptions file files 25
set system processes dhcp-service traceoptions flag all
set class-of-service traceoptions file filename
set class-of-service traceoptions file size 100m
set class-of-service traceoptions flag all
set class-of-service traceoptions file files 25
set routing-options traceoptions file filename
set routing-options traceoptions file size 100m
set routing-options traceoptions flag all
set routing-options traceoptions file files 25
set interfaces traceoptions file filename
set interfaces traceoptions file size 100m
set interfaces traceoptions flag all
set interfaces traceoptions file files 25
set system processes general-authentication-service traceoptions file filename
set system processes general-authentication-service traceoptions file size 100m
set system processes general-authentication-service traceoptions flag all
set system processes general-authentication-service traceoptions file files 25
```

2. Copy the relevant statements into a text file and modify the log filenames as you want.
3. Copy the statements from the text file and paste them into the CLI on your router to configure logging.
4. Commit the logging configuration to begin collecting information.



NOTE: The maximum file size for DHCP local server and DHCP relay log files is 1 GB. The maximum number of log files for DHCP local server and DHCP relay is 1000.



BEST PRACTICE: Enable these logs only to collect information when troubleshooting specific problems. Enabling these logs during normal operations can result in reduced system performance.

**Related
Documentation**

- *Compressing Troubleshooting Logs from /var/logs to Send to Juniper Technical Support*

PART 5

Index

- [Index on page 61](#)

Index

Symbols

#, comments in configuration statements.....	x
(), in syntax descriptions.....	x
< >, in syntax descriptions.....	x
[], in configuration statements.....	x
{ }, in configuration statements.....	x
(pipe), in syntax descriptions.....	x

A

accounting statement	
dynamic IGMP	
interface.....	19

B

braces, in configuration statements.....	x
brackets	
angle, in syntax descriptions.....	x
square, in configuration statements.....	x

C

clear igmp membership command.....	36
clear igmp statistics command.....	39
comments, in configuration statements.....	x
conventions	
text and syntax.....	ix
curly braces, in configuration statements.....	x
customer support.....	xi
contacting JTAC.....	xi

D

disable statement	
dynamic IGMP.....	20
documentation	
comments on.....	xi
dynamic IGMP statements	
accounting.....	19
disable.....	20
group	
with source.....	21
without source.....	21
group-limit.....	22

group-policy.....	22
igmp.....	23
immediate-leave.....	24
interface.....	25
no-accounting	
interface.....	26
oif-map	
interface.....	26
passive	
interface.....	27
promiscuous-mode	
interface.....	28
source	
interface.....	30
ssm-map	
interface.....	31
static	
interface.....	31
version	
interface.....	32
dynamic profiles statements	
protocols.....	29
dynamic protocols	
overview.....	7

F

font conventions.....	ix
-----------------------	----

G

group statement	
dynamic IGMP	
with source.....	21
without source.....	21
group-limit statement	
dynamic IGMP.....	22
group-policy statement	
dynamic IGMP.....	22
groups	
IGMP membership, displaying.....	41

I

IGMP	
enabling.....	23, 30
group membership, displaying.....	41
interfaces, displaying.....	45
statistics, displaying.....	49
version.....	32
igmp statement	
dynamic IGMP.....	23

IGMP statements	
promiscuous-mode	
interface.....	28
immediate-leave statement	
dynamic IGMP.....	24
interface statement	
dynamic IGMP.....	25
Internet Group Management Protocol See IGMP	
L	
log files	
collecting for Juniper Technical Support.....	55
M	
manuals	
comments on.....	xi
N	
no-accounting statement	
dynamic IGMP	
interface.....	26
O	
oif-map statement	
dynamic IGMP	
interface.....	26
P	
parentheses, in syntax descriptions.....	x
passive statement	
dynamic IGMP	
interface.....	27
promiscuous-mode statement	
IGMP	
interface.....	28
protocols statement	
dynamic profiles.....	29
S	
show igmp group command.....	41
show igmp interface command.....	45
show igmp statistics command.....	49
source statement	
dynamic IGMP	
interface.....	30
ssm-map statement	
dynamic IGMP	
interface.....	31
static statement	
dynamic IGMP	
interface.....	31
support, technical See technical support	
syntax conventions.....	ix
T	
technical support	
collecting logs for.....	55
contacting JTAC.....	xi
trace operations	
collecting logs for Juniper technical	
support.....	55
troubleshooting subscriber access	
collecting logs for Juniper Technical	
Support.....	55
V	
version statement	
dynamic IGMP	
interface.....	32