

Chapter 14

Multicast Administrative Scoping

You use multicast scoping to limit multicast traffic by configuring it to an administratively defined topological region. Multicast scoping controls the propagation of multicast messages—both multicast group joins upstream toward a source and data forwarding downstream. Scoping can relieve stress on scarce resources, such as bandwidth, and improve privacy or scaling properties.

This section discusses the following topics that provide information about configuring multicast scoping:

- Multicast Scoping Overview on page 123
- Configuring Multicast Scoping on page 124

For multicast scoping configuration examples, see “Example: Configuring Multicast Scoping with the scope Statement” on page 125 and “Example: Configuring Multicast Scoping with the scope-policy Statement” on page 127.

Multicast Scoping Overview

IP multicast implementations can achieve some level of scoping by using the time-to-live (TTL) field in the IP header. However, TTL scoping has proven difficult to implement reliably, and the resulting schemes often are complex and difficult to understand.

Administratively scoped IP multicast provides clearer and simpler semantics for multicast scoping. Packets addressed to administratively scoped multicast addresses do not cross configured administrative boundaries. Administratively scoped multicast addresses are locally assigned, and hence are not required to be unique across administrative boundaries.

The administratively scoped IP version 4 (IPv4) multicast address space is the range 239.0.0.0 through 239.255.255.255.

The structure of the IPv4 administratively scoped multicast space is based loosely on the IP version 6 (IPv6) addressing architecture described in RFC 1884.

There are two well-known scopes:

- IPv4 local scope—This scope comprises addresses in the range **239.255.0.0/16**. The local scope is the minimal enclosing scope and is not further divisible. Although the exact extent of a local scope is site-dependent, locally scoped regions must not span any other scope boundary and must be contained completely within or be equal to any larger scope. If scope regions overlap in an area, the area of overlap must be within the local scope.
- IPv4 organization local scope—This scope comprises **239.192.0.0/14**. It is the space from which an organization should allocate subranges when defining scopes for private use.

The ranges **239.0.0.0/10**, **239.64.0.0/10**, and **239.128.0.0/10** are unassigned and available for expansion of this space.

Two other scope classes already exist in IPv4 multicast space: the statically assigned link-local scope, which is **224.0.0.0/24**, and the static global scope allocations, which contain various addresses.

All scoping is inherently bidirectional in the sense that join messages and data forwarding are controlled in both directions on the scoped interface.

Configuring Multicast Scoping

You can configure multicast scoping with a scoping statement or with a scoping policy statement. To configure multicast address scoping with either option, include the multicast statement:

```

multicast {
  scope scope-name {
    interface [ interface-names ];
    prefix destination-prefix;
  }
  scope-policy policy-name;
}

```

For a list of the hierarchy levels at which you can configure this statement, see the statement summary section for this statement.



NOTE: You cannot apply a scoping policy to a specific routing instance. That is, all scoping policies are applied to all routing instances. However, the **scope** statement does apply individually to a specific routing instance.

For an overview of logical routers and a detailed example of logical router configuration, see the logical routers chapter of the *JUNOS Feature Guide*.

You cannot use the **scope** and **scope-policy** statements together (the configuration does not commit). The policy statement referenced by the **scope-policy** statement must be properly configured at the **policy-options** hierarchy level. For more information about configuring policy statements, see the *JUNOS Policy Framework Configuration Guide*.

If you configure multicast scoping with the `scope` statement, the names of the defined scopes, prefixes, and interfaces are displayed as part of the `show multicast scope` command output. If you configure multicast scoping with the `scope-policy` statement, only the name of the scope policy is displayed as part of the `show multicast scope` command output.

This section discusses the following topics, which provide information about the two ways to configuring multicast scoping:

- Configuring Multicast Scoping with the `scope` Statement on page 125
- Example: Configuring Multicast Scoping with the `scope` Statement on page 125
- Configuring Multicast Scoping with the `scope-policy` Statement on page 126
- Example: Configuring Multicast Scoping with the `scope-policy` Statement on page 127

Configuring Multicast Scoping with the `scope` Statement

To configure multicast scoping with the `scope` statement, specify a name for the scope, the set of router interfaces on which you are configuring scoping, and the scope's address range.

When you configure multicast scoping with the `scope` statement, all scope boundaries must include the `local` scope. If this scope is not configured, it is added automatically at all scoped interfaces. The `local` scope limits the use of the multicast group `239.255.0.0/16` to an attached LAN.

For information about supported standards for multicast scoping, see “IP Multicast Standards” on page 28.

Example: Configuring Multicast Scoping with the `scope` Statement

This example configures multicast scoping with the `scope` statement, creating four scopes: `local`, `organization`, `engineering`, and `marketing`.

If you have a Tunnel Physical Interface Card (PIC) in your router and you configure a tunnel interface to use IP-IP encapsulation, you can configure the `local` scope. For more information about configuring tunnel interfaces, see the *JUNOS Services Interfaces Configuration Guide*.

Configure the **organization** scope on an IP-IP encapsulation tunnel interface and a SONET/SDH interface. Configure the **engineering** and **marketing** scopes on an IP-IP encapsulation tunnel interface and two SONET/SDH interfaces. The JUNOS software can scope any user-configurable IPv6 or IPv4 group.

```
[edit]
routing-options {
  multicast {
    scope local {
      interface gr-2/1/0;
      prefix fe00::239.255.0.0/128;
    }
    scope organization {
      interface [gr-2/1/0 so-0/0/0];
      prefix 239.192.0.0/14;
    }
    scope engineering {
      interface [ip-2/1/0 so-0/0/1 so-0/0/2];
      prefix 239.255.255.0/24;
    }
    scope marketing {
      interface [gr-2/1/0 so-0/0/2 so-1/0/0];
      prefix 239.255.254.0/24;
    }
  }
}
```



NOTE: Do not configure the same prefix under multiple **scope** statements. If multiple **scope** statements contain the same prefix, only the last **scope** statement is enforced. If you need to scope the same prefix on multiple interfaces, do not use a separate **scope** statement for each interface. List all interfaces under one **scope** statement instead.

If you configure multicast scoping with the **scope** statement, you cannot use the **scope-policy** statement on the same router and vice versa. Using both statements on the same router prevents you from committing the configuration. To verify that group scoping is in effect, use the `show multicast scope` command:

```
user@host> show multicast scope
```

Scope name	Group prefix	Interface	Resolve Rejects
local	fe00::239.255.0.0/128	gr-2/1/0	0
organization	239.192.0.0/14	gr-2/1/0 so-0/0/0	0
engineering	239.255.255.0/24	ip-2/1/0 so-0/0/1 so-0/0/2	0
marketing	239.255.254.0/24	gr-2/1/0 so-0/0/2 so-1/0/0	0

For more information, see the *JUNOS Routing Protocols Configuration Guide*.

Configuring Multicast Scoping with the **scope-policy** Statement

To configure multicast scoping with the **scope-policy** statement, specify a policy name for the scope. The referenced policy must be correctly configured and contain the set of router interfaces on which you are configuring scoping, and the scope's address range configured as a series of router filters.

Only the `interface`, `route-filter`, and `prefix-list` match conditions are supported for multicast scoping policies. All other configured match conditions are ignored. The only actions supported are `accept`, `reject`, and the policy flow actions `next-term` and `next-policy`. The `reject` action means that joins and multicast forwarding are suppressed in both directions on the configured interfaces. The `accept` action allows joins and multicast forwarding in both directions on the interface. By default, scoping policies apply to all interfaces. The default action is `accept`.

For more information about configuring route filters and policies, see the *JUNOS Policy Framework Configuration Guide*.

In contrast to scoping with the `scope` statement, scoping with `scope-policy` does not automatically add the `local` scope at scope boundaries. You must explicitly configure the local scope boundaries when you use the `scope-policy` statement. The `local` scope limits the use of the multicast group `239.255.0.0/16` to an attached LAN.

For information about supported standards for multicast scoping, see “IP Multicast Standards” on page 28.

Example: Configuring Multicast Scoping with the `scope-policy` Statement

This example configures a `scope-policy` statement named `allow-Auto-RP-on-backbone`, allowing packets for Auto-RP groups `224.0.1.39/32 exact` and `224.0.1.40/32 exact` on backbone-facing interfaces, and rejecting all other addresses in the `224.0.1.0/24` or longer and `239.0.0.0/8` or longer address ranges.

First, configure the policy `allow-Auto-RP-on-backbone` at the `[policy-options]` hierarchy level:

```
[edit]
policy-options {
  policy-statement allow-Auto-RP-on-backbone {
    term allow-Auto-RP {
      from {
        /* backbone-facing interfaces */
        interface [ so-0/0/0.0 so-0/0/1.0 ];
        route-filter 224.0.1.39/32 exact;
        route-filter 224.0.1.40/32 exact;
      }
      then {
        accept;
      }
    }
    term reject-these {
      from {
        route-filter 224.0.1.0/24 orlonger;
        route-filter 239.0.0.0/8 orlonger;
      }
      then reject;
    }
  }
}
```

By default, the scope policy applies to all interfaces. For more information about route filters, see the *JUNOS Policy Framework Configuration Guide*.

Then apply the scope policy `allow-Auto-RP-on-backbone` at the routing-options hierarchy level:

```
[edit]
routing-options {
  multicast {
    scope-policy allow-Auto-RP-on-backbone;
  }
}
```

If you configure multicast scoping with the `scope-policy` statement, you cannot use the `scope` statement on the same router and vice versa. Using both statements on the same router prevents you from committing the configuration. To verify that the scope policy is in effect, use the `show multicast scope` command:

```
user@host> show multicast scope
Scope policy: [ allow-Auto-RP-on-backbone ]
```