

## Chapter 21

# Multicast Reverse Path Forwarding

You use multicast reverse path forwarding (RPF) checks to prevent multicast routing loops. Routing loops are particularly debilitating in multicast applications because packets are replicated with each pass around the routing loop.

In general, a router should forward a multicast packet only if it arrives on the interface closest (as defined by a unicast routing protocol) to the origin of the packet, whether source host or rendezvous point (RP). In other words, if a unicast packet would be sent to the “destination” (the reverse path) on the interface that the multicast packet arrived on, the packet passes the RPF check and is processed. Multicast (or unicast) packets that fail the RPF check are not forwarded (this is the default behavior). For an overview of how a Juniper Networks router implements RPF checks with tables, see “RPF Checks and the RPF Table” on page 14.

However, there are network router configurations where multicast packets that fail the RPF check *should* be forwarded. For example, when point-to-multipoint label-switched paths (LSPs) are used for distributing multicast traffic to PIM “islands” downstream from the egress router, the interface on which the multicast traffic arrives is not always the RPF interface. This is because LSPs do not follow the normal next-hop rules of independent packet routing. For information on LSPs, see the *JUNOS MPLS Applications Configuration Guide*.

In cases such as these, you can configure policies on the PE router to decide which multicast groups and sources should be exempt from the default RPF check.

This chapter discusses the following topics that provide information about configuring multicast RPF policies:

- Configuring RPF Policies on page 140
- Example: Configuring RPF Policies on page 140

For more information about policies, see the *JUNOS Policy Framework Configuration Guide*.

## Configuring RPF Policies

You configure one or more multicast RPF policies to disable RPF checks for a particular multicast (S,G) pair. You usually disable RPF checks on egress routers of a point-to-multipoint LSP.

An RPF policy behaves like an import policy. If no policy term matches the input packet, the default action is to accept (that is, to perform the RPF check).



**NOTE:** Be careful when disabling RPF checks on multicast traffic. If you disable RPF checks in some configurations, multicast loops can result.

To configure multicast RPF policies, include the `rpf-check-policy` statement with a correctly configured policy:

```
multicast {
  rpf-check-policy [ policy-names ];
}
```

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

Changes to an RPF check policy take effect immediately:

- If no policy was previously configured, the policy takes effect immediately.
- If the policy name is changed, the new policy takes effect immediately and any packets no longer filtered are subjected to the RPF check.
- If the policy is deleted, all packets formerly filtered are subjected to the RPF check.
- If the underlying policy is changed, but retains the same name, the new conditions take effect immediately and any packets no longer filtered are subjected to the RPF check.

### Example: Configuring RPF Policies

This example configures an RPF check policy named `disable-RPF-on-PE`, disabling the RPF check on multicast packets for the configured (S,G) source-group pair. This policy will not perform RPF checks on packets arriving for group `228.0.0.0/8` or from source address `196.168.25.6`.

First, configure the policy `disable-RPF-on-PE` at the `[edit policy-options]` hierarchy level:

```
[edit]
policy-options {
  policy-statement disable-RPF-on-PE {
    term first {
      from {
        route-filter 228.0.0.0/8 orlonger;
        source-address-filter 192.168.25.6/32 exact;
      }
    }
  }
}
```

```

    }
    then {
      reject;
    }
  }
}

```

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

Then apply the policy `disable-RPF-on-PE` at the `[edit routing-options]` hierarchy level:

```

[edit]
routing-options {
  multicast {
    rpf-check-policy disable-RPF-on-PE;
  }
}

```

You can also configure each condition as a separate policy and reference both policies in the `rpf-check-policy` statement:

```

[edit]
policy-options {
  policy-statement disable-RPF-on-group {
    term first {
      from {
        route-filter 228.0.0.0/8 orlonger;
      }
      then {
        reject;
      }
    }
  }
}

policy-statement disable-RPF-on-source {
  term first {
    from {
      source-address-filter 192.168.25.6/32 exact;
    }
    then {
      reject;
    }
  }
}
}

[edit]
routing-options {
  multicast {
    rpf-check-policy [ disable-RPF-on-group disable-RPF-on-source ];
  }
}

```

This allows you to associate groups in one policy and source in the other.

