

Configuring Triple Play Multicast Services with CLI

This section provides information to configure multicast parameters in a Triple Play network using the command line interface.

Topics in this section include:

- [Configuring IGMP Snooping in the BSA on page 758](#)
 - [Enabling IGMP Snooping in a VPLS Service on page 758](#)
 - [Modifying IGMP Snooping Parameters on page 760](#)
 - [Configuring Static Multicast Groups on a SAP or SDP on page 763](#)
 - [Enabling IGMP Group Membership Report Filtering on page 764](#)
 - [Enabling IGMP Traffic Filtering on page 766](#)
 - [Configuring Multicast VPLS Registration \(MVR\) on page 767](#)
- [Configuring IGMP and PIM in the BSR on page 768](#)

IGMP

- [Enabling IGMP on page 768](#)
- [Configuring IGMP Interface Parameters on page 769](#)
- [Configuring Static Parameters on page 770](#)
- [Configuring SSM Translation on page 771](#)

PIM

- [Enabling PIM on page 772](#)
- [Configuring PIM Interface Parameters on page 773](#)
- [Importing PIM Join/Register Policies on page 776](#)
- [Configuring PIM Join/Register Policies on page 777](#)
- [Configuring Bootstrap Message Import and Export Policies on page 778](#)

Configuring IGMP Snooping in the BSA

- [Enabling IGMP Snooping in a VPLS Service on page 758](#)
 - [Configuring Static Multicast Groups on a SAP or SDP on page 763](#)
 - [Enabling IGMP Group Membership Report Filtering on page 764](#)
 - [Enabling IGMP Traffic Filtering on page 766](#)
 - [Configuring Multicast VPLS Registration \(MVR\) on page 767](#)
-

Enabling IGMP Snooping in a VPLS Service

- [With IGMPv3 Multicast Routers on page 758](#)
 - [With IGMPv3 Multicast Routers on page 758](#)
 - [With IGMPv1/2 Multicast Routers on page 759](#)
 - [Modifying IGMP Snooping Parameters on page 760](#)
 - [Modifying IGMP Snooping Parameters for a SAP or SDP on page 761](#)
-

With IGMPv3 Multicast Routers

When multicast routers use IGMPv3, it is sufficient to just enable IGMP snooping, without any further modification of parameters.

The following displays an example of an IGMP snooping configuration:

```
A:ALA-48>config>service>vpls# info
-----
      igmp-snooping
        no shutdown
      exit
      no shutdown
-----
A:ALA-48>config>service>vpls#
```

With IGMPv1/2 Multicast Routers

When the multicast routers don't support IGMPv3, some timing parameters need to be configured locally in the Alcatel-Lucent SR-Series. Note that all routers in the multicast network must use the same values for these parameters.

The following displays an example of a modified IGMP snooping configuration:

```
A:ALA-48>config>service>vpls# info
-----
      stp
        shutdown
      exit
      igmp-snooping
        query-interval 60
        robust-count 5
        no shutdown
      exit
      no shutdown
-----
A:ALA-48>config>service>vpls#
```

Modifying IGMP Snooping Parameters

For interoperability with some multicast routers, the source IP address of IGMP group reports can be configured. Use the following CLI syntax to customize this IGMP snooping parameter:

The following displays an example of a modified IGMP snooping configuration:

```
A:ALA-48>config>service>vpls# info
-----
      stp
        shutdown
      exit
      igmp-snooping
        query-interval 60
        robust-count 5
        report-src-ip 10.20.20.20
        no shutdown
      exit
      no shutdown
-----
A:ALA-48>config>service>vpls#
```

Modifying IGMP Snooping Parameters for a SAP or SDP

Use the following CLI syntax to customize IGMP snooping parameters on an existing SAP. Commands for spoke or mesh SDPs are identical.

CLI Syntax:

```
config>service# vpls service-id
    sap sap-id
        igmp-snooping
            fast-leave
            import policy-name
            last-member-query-interval interval
            max-num-groups max-num-groups
            mrouter-port
            query-interval interval
            query-response-interval interval
            robust-count count
            send-queries
```

To enable and customize sending of IGMP queries to the hosts:

Example:

```
config>service# vpls 1
config>service>vpls# sap 1/1/3:0
config>service>vpls>sap# igmp-snooping
config>service>vpls>sap>snooping# send-queries
config>service>vpls>sap>snooping# query-interval 100
config>service>vpls>sap>snooping# query-response-interval 60
config>service>vpls>sap>snooping# robust-count 5
config>service>vpls>sap>snooping# exit
config>service>vpls>sap# no shutdown
```

To customize the leave delay:

Example:

```
config>service# vpls 1
config>service>vpls# sap 1/1/1:1
config>service>vpls>sap# igmp-snooping
config>service>vpls>sap>snooping# last-member-query-interval 10
config>service>vpls>sap>snooping# no fast-leave
config>service>vpls>sap>snooping# exit
config>service>vpls>sap# exit
```

Configuring Triple Play Multicast Services with CLI

To enable Fast Leave:

```
Example: config>service# vpls 1
            config>service>vpls# sap 1/1/1:1
            config>service>vpls>sap# igmp-snooping
            config>service>vpls>sap>snooping# no last-member-query-interval
            config>service>vpls>sap>snooping# fast-leave
            config>service>vpls>sap>snooping# exit
            config>service>vpls>sap# exit
```

To limit the number of streams that a host can join:

```
Example: config>service# vpls 1
            config>service>vpls# sap 1/1/1:1
            config>service>vpls>sap# igmp-snooping
            config>service>vpls>sap>snooping# max-num-groups 4
            config>service>vpls>sap>snooping# exit
            config>service>vpls>sap# exit
```

To enable sending group reports on a SAP to standby multicast routers:

```
Example: config>service# vpls 1
            config>service>vpls# sap 1/1/1:1
            config>service>vpls>sap# igmp-snooping
            config>service>vpls>sap>snooping# mrouter-port
            config>service>vpls>sap>snooping# exit
            config>service>vpls>sap# exit
```

The following example displays the modified IGMP snooping configuration on a SAP:

```
A:ALA-48>config>service>vpls>sap>snooping# info detail
-----
                no fast-leave
                no import
                max-num-groups 4
                last-member-query-interval 10
                no mrouter-port
                query-interval 100
                query-response-interval 60
                robust-count 5
                send-queries
-----
A:ALA-48>config>service>vpls>sap>snooping#
```

Configuring Static Multicast Groups on a SAP or SDP

Use the following CLI syntax to add static group membership entries on an existing SAP (commands for spoke or mesh SDPs are identical):

The following displays an example of a static IGMP snooping configuration on a SAP:

```
A:ALA-48>config>service>vpls>sap# info
-----
      max-nbr-mac-addr 4
      igmp-snooping
        fast-leave
        mrouter-port
        static
          group 224.0.10.10
            source 10.10.10.1
            source 10.10.10.2
          exit
        exit
      exit
-----
A:ALA-48>config>service>vpls>sap#
```

Enabling IGMP Group Membership Report Filtering

Routing policies can be defined to limit the multicast channels that can be joined by a host. For example, it is possible to define a policy listing a group of multicast streams (for example, 'basic' containing a basic set of TV channels or 'extended' containing a more extended set of TV channels), and to apply this policy to subscribers of IGMP snooping (SAPs and/or SDPs).

The following displays an example of a configuration to import a routing policy on a SAP:

```
A:ALA-48>config>service>vpls# info
-----
      stp
        shutdown
      exit
      igmp-snooping
        query-interval 60
        robust-count 5
        report-src-ip 10.20.20.20
        no shutdown
      exit
      sap 1/1/3:0 create
        igmp-snooping
          query-interval 100
          query-response-interval 60
          robust-count 5
          send-queries
        exit
      exit
      sap 1/1/3:22 create
        max-nbr-mac-addr 4
        igmp-snooping
          fast-leave
          import "test_policy"
          mrouter-port
          static
            group 224.0.10.10
              source 10.10.10.1
              source 10.10.10.2
          exit
        exit
      exit
      exit
      no shutdown
-----
A:ALA-48>config>service>vpls#
```

For details configuring a routing policy, see the Configuring Route Policies section in the 7750 SR OS Router Configuration Guide.

The following shows a sample routing policy configuration accepting IGMP messages for only five multicast channels:

```
A:ALA-48>config>router>policy-options# info
-----
    prefix-list "basic_channels"
      prefix 224.10.0.1/32 exact
      prefix 224.10.0.2/32 exact
      prefix 224.10.0.3/32 exact
      prefix 224.10.0.4/32 exact
      prefix 224.10.0.5/32 exact
    exit
    policy-statement "test_policy"
      description "basic set of 5 multicast channels"
      entry 1
        from
          group-address "basic_channels"
        exit
        action accept
        exit
      exit
      default-action reject
    exit
-----
A:ALA-48>config>router>policy-options#
```

Enabling IGMP Traffic Filtering

For security, it might be advisable to only allow multicast traffic into the SR-Series from recognized multicast routers and servers. Multicast packets arriving on other interfaces (for example, customer-facing SAPs or spoke SDPs) can be filtered out by defining an appropriate IP filter policy.

For details on how to configure a *filter policy*, see section *Creating an IP Filter Policy in the 7750 SR OS Router Configuration Guide*

The following example shows a sample IP filter policy configuration dropping all multicast traffic:

```
A:ALA-48>config>filter>ip-filter# info
-----
ip-filter 1 create
  entry 1 create
    match
      dst-ip 224.0.0.0/24
    exit
    action accept
  exit
  entry 2 create
    match
      dst-ip 224.0.0.0/4
    exit
    action drop
  exit
exit
-----
A:ALA-48>config>filter>ip-filter#
```

The following example shows how to apply this sample IP filter policy to a SAP:

```
A:ALA-48>config>service>vpls # info
-----
sap 1/1/1:1
  ingress
    filter ip 1
  exit
exit
-----
A:ALA-48>config>service>vpls>snooping#
```

Configuring Multicast VPLS Registration (MVR)

Use the following CLI syntax to configure Multicast VPLS Registration. The first step is to register a VPLS as a multicast VPLS.

CLI Syntax: `config>service# vpls service-id
 igmp-snooping
 mvr
 no shutdown
 description description
 group-policy policy-name`

Example: `config>service# vpls 1000
 config>service>vpls# igmp-snooping
 config>service>vpls>snooping# mvr
 config>service>vpls>snooping>mvr# no shutdown
 config>service>vpls>snooping>mvr# description "MVR VPLS"
 config>service>vpls>snooping>mvr# group-policy
 "basic_channels_policy"`

The second step is to configure a SAP to take the multicast channels from the registered multicast VPLS.

CLI Syntax: `config>service# vpls service-id
 sap sap-id
 igmp-snooping
 mvr
 from-vpls vpls-id`

Example: `config>service# vpls 1
 config>service>vpls# sap 1/1/1:100
 config>service>vpls>sap# igmp-snooping
 config>service>vpls>snooping# mvr
 config>service>vpls>snooping>mvr# from-vpls 1000`

For MVR by proxy also the destination SAP for the multicast channels should be configured.

CLI Syntax: `config>service# vpls service-id
 sap sap-id
 igmp-snooping
 mvr
 from-vpls vpls-id
 to-sap sap-id`

Example: `config>service# vpls 1
 config>service>vpls# sap 1/1/1:100
 config>service>vpls>sap# igmp-snooping
 config>service>vpls>snooping# mvr
 config>service>vpls>snooping>mvr# from-vpls 1000
 config>service>vpls>snooping>mvr# to-sap 1/1/1:200`

Configuring IGMP and PIM in the BSR

Refer to the Multicast section in the 7750 SR OS Routing Protocols Guide for information about multicast and the commands required to configure basic IGMP and PIM parameters.

IGMP

- [Enabling IGMP on page 768](#)
- [Configuring IGMP Interface Parameters on page 769](#)
- [Configuring Static Parameters on page 770](#)
- [Configuring SSM Translation on page 771](#)

PIM

- [Enabling PIM on page 772](#)
 - [Configuring PIM Interface Parameters on page 773](#)
 - [Importing PIM Join/Register Policies on page 776](#)
 - [Configuring PIM Join/Register Policies on page 777](#)
 - [Configuring Bootstrap Message Import and Export Policies on page 778](#)
-

Enabling IGMP

The following displays an example of enabled IGMP.

```
A:LAX>>config>router# info detail
...
#-----
echo "IGMP Configuration"
#-----
      igmp
        query-interval 125
        query-last-member-interval 1
        query-response-interval 10
        robust-count 2
        no shutdown
      exit
#-----
...
A:LAX>>config>system#
```

Configuring IGMP Interface Parameters

The following example displays an IGMP configuration:

```
A:LAX>config>router>igmp# info
-----
    interface "lax-sjc"
    exit
    interface "lax-vls"
    exit
    interface "p1-ix"
    exit
-----
A:LAX>config>router>igmp# exit
```

Configuring Static Parameters

The following example displays a configuration to add IGMP a static multicast source::

```
A:LAX>config>router>igmp# info
-----
    interface "lax-sjc"
    exit
    interface "lax-vls"
        static
            group 229.255.0.2
            source 172.22.184.197
        exit
    exit
    exit
    interface "p1-ix"
    exit
-----
A:LAX>config>router>igmp#
```

The following example displays the configuration to add a IGMP static starg entry:

```
A:LAX>config>router>igmp# info
-----
    interface "lax-sjc"
        static
            group 230.1.1.1
            starg
        exit
    exit
    interface "lax-vls"
        static
            group 229.255.0.2
            source 172.22.184.197
        exit
    exit
    interface "p1-ix"
    exit
-----
A:LAX>config>router>igmp#
```

Configuring SSM Translation

The following displays an SSM translation configuration:

```
A:LAX>config>router>igmp# info
-----
    ssm-translate
      grp-range 229.255.0.1 231.2.2.2
        source 10.1.1.1
      exit
    exit
  interface "lax-sjc"
    static
      group 230.1.1.1
      starg
    exit
  exit
exit
interface "lax-vls"
  static
    group 229.255.0.2
    source 172.22.184.197
  exit
exit
exit
interface "p1-ix"
exit
-----
A:LAX>config>router>igmp# exit
```

Configuring PIM

Enabling PIM

When configuring PIM, make sure to enable PIM on all interfaces for the routing instance, otherwise multicast routing errors can occur.

The following example displays detailed output when PIM is enabled.

```
A:LAX>>config>router# info detail
...
#-----
echo "PIM Configuration"
#-----
    pim
      no import join-policy
      no import register-policy
      apply-to none
      rp
        no bootstrap-import
        no bootstrap-export
        static
        exit
        bsr-candidate
          shutdown
          priority 0
          hash-mask-len 30
          no address
        exit
        rp-candidate
          shutdown
          no address
          holdtime 150
          priority 192
        exit
      exit
    no shutdown
  exit
#-----
...
A:LAX>>config>system#
```


Configuring PIM Interface Parameters

The following displays a PIM interface configuration:

```
A:LAX>config>router>pim# info
-----
interface "system"
exit
interface "lax-vls"
exit
interface "lax-sjc"
exit
interface "p1-ix"
exit
rp
static
address 2.22.187.237
group-prefix 224.24.24.24/32
exit
address 10.10.10.10
exit
exit
bsr-candidate
shutdown
exit
rp-candidate
shutdown
exit
exit
```

```
A:LAX>config>router>pim#
```

```
A:SJC>config>router>pim# info
-----
interface "system"
exit
interface "sjc-lax"
exit
interface "sjc-nyc"
exit
interface "sjc-sfo"
exit
rp
static
address 2.22.187.237
group-prefix 224.24.24.24/32
exit
exit
bsr-candidate
shutdown
exit
rp-candidate
shutdown
exit
exit
```

```
A:SJC>config>router>pim#
```

Configuring Triple Play Multicast Services with CLI

```
A:MV>config>router>pim# info
-----
interface "system"
exit
interface "mv-sfo"
exit
interface "mv-vlc"
exit
interface "p3-ix"
exit
rp
  static
    address 2.22.187.237
    group-prefix 224.24.24.24/32
  exit
  bsr-candidate
    address 2.22.187.236
    no shutdown
  exit
  rp-candidate
    address 2.22.187.236
    no shutdown
  exit
exit
```

```
A:MV>config>router>pim#
```

```
A:SFO>config>router>pim# info
-----
interface "system"
exit
interface "sfo-sjc"
exit
interface "sfo-was"
exit
interface "sfo-mv"
exit
rp
  static
    address 2.22.187.237
    group-prefix 224.24.24.24/32
  exit
  bsr-candidate
    address 2.22.187.239
    no shutdown
  exit
  rp-candidate
    address 2.22.187.239
    no shutdown
  exit
exit
```

```
A:SFO>config>router>pim#
```

```
A:WAS>config>router>pim# info
-----
interface "system"
exit
interface "was-sfo"
exit
interface "was-vlc"
exit
interface "p4-ix"
exit
rp
  static
    address 2.22.187.237
    group-prefix 224.24.24.24/32
  exit
exit
bsr-candidate
  address 2.22.187.240
  no shutdown
exit
rp-candidate
  address 2.22.187.240
  no shutdown
exit
exit
-----
A:WAS>config>router>pim#
```

Importing PIM Join/Register Policies

The import command provides a mechanism to control the (*,g) and (s,g) state that gets created on a router. Import policies are defined in the **config>router>policy-options** context. See [Configuring PIM Join/Register Policies on page 777](#).

Note, in the import policy, if an action is not specified in the entry then the default-action takes precedence. If no entry matches then the default-action also takes precedence. If no default-action is specified, then the default default-action is executed.

The following example displays the command usage to apply the policy statement will not allow join messages for group 229.50.50.208/32 and source 192.168.0.0/16 but allows join messages for 192.168.0.0/16, 229.50.50.208:

```
Example:    config>router# pim
               config>router>pim# import join-policy "foo"
               config>router>pim# no shutdown
```

The following example displays the PIM configuration:

```
A:LAX>config>router>pim# info
-----
import join-policy "foo"
interface "system"
exit
interface "lax-vls"
exit
interface "lax-sjc"
exit
interface "pl-ix"
exit
rp
  static
    address 2.22.187.237
      group-prefix 224.24.24.24/3
    exit
    address 10.10.10.10
    exit
  exit
  bsr-candidate
    shutdown
  exit
  rp-candidate
    shutdown
  exit
exit
-----
A:LAX>config>router>pim#
```

Configuring PIM Join/Register Policies

Join policies are used in Protocol Independent Multicast (PIM) configurations to prevent the transportation of multicast traffic across a network and the dropping of packets at a scope at the edge of the network. PIM Join filters reduce the potential for denial of service (DoS) attacks and PIM state explosion—large numbers of Joins forwarded to each router on the RPT, resulting in memory consumption.

*.g or s,g is the information used to forward unicast or multicast packets.

- **group-address** matches the group in join/prune messages
group-address 229.55.150.208/32 exact
- **source-address** matches the source in join/prune messages
source-address 192.168.0.0/16 longer
- **interface** matches any join message received on the specified interface
interface port 1/1/1
- **neighbor** matches any join message received from the specified neighbor
neighbor 1.1.1.1

The following configuration example will not allow join messages for group 229.50.50.208/32 and source 192.168.0.0/16 but allows join messages for 192.168.0.0/16, 229.50.50.208.

```
A:ALA-B>config>router>policy-options# info
-----
...
    policy-statement "foo"
      entry 10
        from
          group-address "229.50.50.208/32"
          source-address 192.168.0.0
        exit
        action reject
      exit
    exit
  policy-statement "reg-pol"
    entry 10
      from
        group-address "224.0.0.0/8"
      exit
      action accept
    exit
  exit
exit
...
-----
A:ALA-B>config>router>policy-options#
```

Configuring Bootstrap Message Import and Export Policies

Bootstrap import and export policies are used to control the flow of bootstrap messages to and from the RP.

The following configuration example specifies that no BSR messages received or sent out of interface port 1/1/1.

```
:A:ALA-B>config>router>policy-options# policy-statement pim-import
:A:ALA-B>config>router>policy-options>policy-statement$ entry 10
:A:ALA-B>config>router>policy-options>policy-statement>entry$ from
:A:ALA-B>config>router>policy-options>policy-statement>entry>from$ interface port1/1/1/
:A:ALA-B>config>router>policy-options>policy-statement>entry>from$ exit
:A:ALA-B>config>router>policy-options>policy-statement>entry# action reject
:A:ALA-B>config>router>policy-options>policy-statement>entry# exit
:A:ALA-B>config>router>policy-options>policy-statement# exit

:A:ALA-B>config>router>policy-options# policy-statement pim-export
:A:ALA-B>config>router>policy-options>policy-statement$ entry 10
:A:ALA-B>config>router>policy-options>policy-statement>entry$ to
:A:ALA-B>config>router>policy-options>policy-statement>entry>to$
```