

Chapter 10

Configuring the JPS with the SRC CLI

This chapter describes how to use the SRC CLI to configure the Juniper Policy Server (JPS), a component of the SRC software that acts as a policy server in the PacketCable Multimedia Specification (PCMM) environment. You can use the CLI to configure the JPS on a Solaris platform or on a C-series Controller.

Topics in this chapter include:

- Configuration Statements for the JPS on page 81
- Configuring the JPS on page 83
- Modifying the JPS Configuration on page 84
- Modifying the Subscriber Configuration on page 96
- Configuring the SAE to Interact with the JPS on page 98
- Using the NIC Resolver on page 102
- Managing the JPS on page 103

For information about the JPS, see *Chapter 9, Using PCMM Policy Servers*.

Configuration Statements for the JPS

Use the following configuration statements to configure the JPS at the [edit] hierarchy level.

```
slot number jps {  
    java-heap-size java-heap-size;  
    snmp-agent;  
    policy-server-id policy-server-id;  
    use-psid-in-gate-commands;  
    cmts-message-buffer-size cmts-message-buffer-size;  
    am-message-buffer-size am-message-buffer-size;  
}
```

```

slot number jps am-interface {
    pep-id pep-id;
    listening-address listening-address;
    validate-pcmm-objects;
    message-max-length message-max-length;
    message-read-buffer-size message-read-buffer-size;
    message-write-buffer-size message-write-buffer-size;
    open-connection-timeout open-connection-timeout;
}

slot number jps cmts-interface {
    cmts-addresses [cmts-addresses...];
    keepalive-interval keepalive-interval;
    synch-despite-unreachable-pep;
    synch-despite-pre-i03-pep;
    use-ssq-ssc-with-pre-i03-pep;
    local-address local-address;
    message-max-length message-max-length;
    message-read-buffer-size message-read-buffer-size;
    message-write-buffer-size message-write-buffer-size;
    open-connection-timeout open-connection-timeout;
    connection-open-retry-interval connection-open-retry-interval;
    sent-message-timeout sent-message-timeout;
    validate-pcmm-objects;
}

slot number jps cmts-registry cmts cmts-ip ...

slot number jps cmts-registry cmts cmts-ip range-pool pool-index {
    low low;
    high high;
}

slot number jps cmts-registry cmts cmts-ip subnet-pool subnet {
    exclude [exclude];
}

slot number jps logger name ...

slot number jps logger name file {
    filter filter;
    filename filename;
    rollover-filename rollover-filename;
    maximum-file-size maximum-file-size;
}

slot number jps logger name syslog {
    filter filter;
    host host;
    facility facility;
    format format;
}

```

```

slot number jps rks-interface {
    element-id element-id;
    local-address local-address;
    local-port local-port;
    retry-interval retry-interval;
    local-timeout local-timeout;
    mso-data mso-data;
    mso-domain-name mso-domain-name;
    default-rks-pair default-rks-pair;
    pending-rks-event-max-size pending-rks-event-max-size;
    pending-rks-event-max-age pending-rks-event-max-age;
    held-decs-max-size held-decs-max-size;
    held-decs-max-age held-decs-max-age;
    bcid-cache-size bcid-cache-size;
    bcid-cache-age bcid-cache-age;
    use-default-when-am-requests-unconfigured-rks;
}

slot number jps rks-interface am am-name {
    am-id am-id;
    rks-pair-name rks-pair-name;
    trusted;
}

slot number jps rks-interface rks-pair rks-pair-name {
    primary-address primary-address;
    primary-port primary-port;
    secondary-address secondary-address;
    secondary-port secondary-port;
}

```

For detailed information about each configuration statement, see the *SRC-PE CLI Command Reference*.

Configuring the JPS

You can modify the JPS configuration, which includes configuring the logging destinations and connections to the JPS interfaces. Any configuration changes will be applied within 15 seconds.

You can configure the subscriber configuration, which maps a subscriber address to the CMTS address.

The tasks to configure the JPS for a cable network environment are:

- Modifying the JPS Configuration on page 84
- Modifying the Subscriber Configuration on page 96

In addition to configuring the JPS, you might need to perform these tasks:

- Configuring the SAE to Interact with the JPS on page 98
- Using the NIC Resolver on page 102

Modifying the JPS Configuration

To modify the current JPS configuration:

1. Configure general properties for the JPS, including Java heap memory, maximum number of buffered messages for CMTS and application manager destinations, and policy server identifiers.

See *Configuring General Properties for the JPS* on page 84.

See *Specifying Policy Server Identifiers in Messages* on page 85.

2. Configure logging destinations for the JPS.

See *Configuring Logging Destinations for the JPS* on page 86.

3. Configure the connections to the JPS interfaces.

See *Specifying Connections to the Application Managers* on page 87.

See *Specifying Connections to RKs* on page 89.

See *Specifying Connections to CMTS Devices* on page 93.

Configuring General Properties for the JPS

Use the following configuration statements to configure general properties for the JPS:

```
slot number jps {
    java-heap-size java-heap-size;
    snmp-agent;
    cmts-message-buffer-size cmts-message-buffer-size;
    am-message-buffer-size am-message-buffer-size;
}
```

To configure general properties for the JPS:

1. From configuration mode, access the configuration statement that configures the general properties.

```
user@host# edit slot 0 jps
```

2. (Optional) Specify the maximum amount of memory available to the Java Runtime Environment (JRE).

```
[edit slot 0 jps]
user@host# set java-heap-size java-heap-size
```

3. (Optional) Enable the JPS to communicate with the SNMP agent.

```
[edit slot 0 jps]
user@host# set snmp-agent
```

4. (Optional) Specify the maximum number of messages buffered for each CMTS destination.

```
[edit slot 0 jps]
user@host# set cmts-message-buffer-size cmts-message-buffer-size
```

5. (Optional) Specify the maximum number of messages buffered for each application manager destination.

```
[edit slot 0 jps]
user@host# set am-message-buffer-size am-message-buffer-size
```

6. (Optional) Verify your configuration.

```
[edit slot 0 jps]
user@host# show
```

Specifying Policy Server Identifiers in Messages

Use the following configuration statements to configure policy server identifiers for the JPS:

```
slot number jps {
    policy-server-id policy-server-id;
    use-psid-in-gate-commands;
}
```

To configure policy server identifiers for the JPS:

1. From configuration mode, access the configuration statement that configures the policy server identifiers.

```
user@host# edit slot 0 jps
```

2. (Optional) Specify the policy server identifier so that the JPS can be identified in messages sent to CMTS devices.

```
[edit slot 0 jps]
user@host# set policy-server-id policy-server-id
```

3. (Optional) Configure the JPS so that the policy server identifier is specified in messages sent to the RKS.

```
[edit slot 0 jps]
user@host# set use-psid-in-gate-commands
```

When the JPS is communicating only with PCMM I03 CMTS devices, the value must be true. When the JPS is communicating with any pre-PCMM I03 CMTS devices, the value must be false.

4. (Optional) Verify your configuration.

```
[edit slot 0 jps]
user@host# show
```

Configuring Logging Destinations for the JPS

By default, the JPS has four logging destinations.

Use the following configuration statements to configure logging destinations for the JPS:

slot *number* jps logger *name* ...

```
slot number jps logger name file {
    filter filter;
    filename filename;
    rollover-filename rollover-filename;
    maximum-file-size maximum-file-size;
}
```

```
slot number jps logger name syslog {
    filter filter;
    host host;
    facility facility;
    format format;
}
```

Configuring Logging Destinations to Store Messages in a File

To configure logging destinations to store log messages in a file:

1. From configuration mode, access the configuration statement that configures the name and type of logging destination. In this sample procedure, the logging destination called log2 is configured.

```
user@host# edit slot 0 jps logger log2 file
```

2. Specify the properties for the logging destination.

```
[edit slot 0 jps logger log2 file]
user@host# set ?
```

For more information about configuring properties for the logging destination, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 3, Configuring Logging for SRC Components with the CLI*.

3. (Optional) Verify your configuration.

```
[edit slot 0 jps logger log2]
user@host# show
file {
    filter !NoAckRksEvent,/info-;
    filename var/log/jps_info.log;
    rollover-filename var/log/jps_info.alt;
    maximum-file-size 2000000000;
}
```

Configuring Logging Destinations to Send Messages to System Logging Facility

To configure logging destinations to send log messages to the system logging facility:

1. From configuration mode, access the configuration statement that configures the name and type of logging destination. In this sample procedure, the logging destination called log5 is configured.

```
user@host# edit slot 0 jps logger log5 syslog
```

2. Specify the properties for the logging destination.

```
[edit slot 0 jps logger log5 syslog]
user@host# set ?
```

For more information about configuring properties for the logging destination, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 3, Configuring Logging for SRC Components with the CLI*.

3. (Optional) Verify your configuration.

```
[edit slot 0 jps logger log5]
user@host# show
```

Specifying Connections to the Application Managers

Use the following configuration statement to configure the application manager-to-policy server interface (PKT-MM3) so that the policy server can communicate with application managers:

```
slot number jps am-interface {
    pep-id pep-id;
    listening-address listening-address;
    validate-pcmm-objects;
    message-max-length message-max-length;
    message-read-buffer-size message-read-buffer-size;
    message-write-buffer-size message-write-buffer-size;
    open-connection-timeout open-connection-timeout;
}
```

To configure the connections to the application managers:

1. From configuration mode, access the configuration statement that configures the application manager-to-policy server interface.

```
user@host# edit slot 0 jps am-interface
```

2. (Optional) Specify the network-wide unique identifier for this JPS instance.

```
[edit slot 0 jps am-interface]
user@host# set pep-id pep-id
```

Changes apply only to COPS connections that are established after you make the change.

3. (Optional) Specify the local IP address on which the JPS listens for incoming connections from application managers.

```
[edit slot 0 jps am-interface]
user@host# set listening-address listening-address
```

Changes take effect only after you restart the JPS (see *Restarting the JPS* on page 103).

4. (Optional) Specify whether to validate PCMM objects received from PDPs.

```
[edit slot 0 jps am-interface]
user@host# set validate-pcmm-objects
```

5. (Optional) Specify the maximum length of incoming messages.

```
[edit slot 0 jps am-interface]
user@host# set message-max-length message-max-length
```

6. (Optional) Specify the size of message read buffer.

```
[edit slot 0 jps am-interface]
user@host# set message-read-buffer-size message-read-buffer-size
```

7. (Optional) Specify the size of message write buffer.

```
[edit slot 0 jps am-interface]
user@host# set message-write-buffer-size message-write-buffer-size
```

8. (Optional) Specify the maximum time to wait for the initial PCMM messages to be exchanged after a TCP connection is established.

```
[edit slot 0 jps am-interface]
user@host# set open-connection-timeout open-connection-timeout
```

The connection is dropped when initial PCMM messages are not exchanged within this time period.

9. (Optional) Verify your configuration.

```
[edit slot 0 jps am-interface]
user@host# show
pep-id SDX-JPS;
listening-address ;
validate-pcmm-objects;
message-max-length 204800;
message-read-buffer-size 1000000;
message-write-buffer-size 1000000;
open-connection-timeout 5;
```


Specifying Connections to RKSs

To configure the policy server-to-RKS interface (PKT-MM4) so that policy events can be sent to the RKS, you can configure RKS pairs (see *Configuring RKS Pairs* on page 91) and their associated application managers (see *Configuring RKS Pairs for Associated Application Managers* on page 92).

Use the following configuration statement to configure the policy server-to-RKS interface:

```
slot number jps rks-interface {
    element-id element-id;
    local-address local-address;
    local-port local-port;
    retry-interval retry-interval;
    local-timeout local-timeout;
    mso-data mso-data;
    mso-domain-name mso-domain-name;
    default-rks-pair default-rks-pair;
    pending-rks-event-max-size pending-rks-event-max-size;
    pending-rks-event-max-age pending-rks-event-max-age;
    held-decs-max-size held-decs-max-size;
    held-decs-max-age held-decs-max-age;
    bcid-cache-size bcid-cache-size;
    bcid-cache-age bcid-cache-age;
    use-default-when-am-requests-unconfigured-rks;
}
```

To configure the policy server-to-RKS interface:

1. From configuration mode, access the configuration statement that configures the policy server-to-RKS interface.

```
user@host# edit slot 0 jps rks-interface
```

2. Specify the network-wide unique identifier for RKS event origin.

```
[edit slot 0 jps rks-interface]
user@host# set element-id element-id
```

3. (Optional) Specify the source IP address that the plug-in uses to communicate with the RKS.

```
[edit slot 0 jps rks-interface]
user@host# set local-address local-address
```

If no value is specified and there is more than one local address, the JPS randomly selects a local address to be used as the source address.

4. (Optional) Specify the source UDP port or a pool of ports that the plug-in uses to communicate with the RKS.

```
[edit slot 0 jps rks-interface]
user@host# set local-port local-port
```

5. (Optional) Specify the time the JPS waits for a response from an RKS before it resends the packet.

```
[edit slot 0 jps rks-interface]
user@host# set retry-interval retry-interval
```

The JPS keeps sending packets until either the RKS acknowledges the packet or the maximum timeout is reached.

6. (Optional) Specify the maximum time the JPS waits for a response from an RKS.

```
[edit slot 0 jps rks-interface]
user@host# set local-timeout local-timeout
```

7. (Optional) Specify the MSO-defined data in the financial entity ID (FEID) attribute, which is included in event messages.

```
[edit slot 0 jps rks-interface]
user@host# set mso-data mso-data
```

8. (Optional) Specify the MSO domain name in the FEID attribute that uniquely identifies the MSO for billing and settlement purposes.

```
[edit slot 0 jps rks-interface]
user@host# set mso-domain-name mso-domain-name
```

9. (Optional) Specify the default RKS pair that the JPS uses unless an RKS pair is configured for a given application manager.

```
[edit slot 0 jps rks-interface]
user@host# set default-rks-pair default-rks-pair
```

10. (Optional) Specify the maximum number of RKS events waiting for Gate-Set-Ack, Gate-Set-Err, Gate-Del-Ack, and Gate-Del-Err messages.

```
[edit slot 0 jps rks-interface]
user@host# set pending-rks-event-max-size pending-rks-event-max-size
```

11. (Optional) Specify the oldest age of RKS events waiting for Gate-Set-Ack, Gate-Set-Err, Gate-Del-Ack, and Gate-Del-Err messages.

```
[edit slot 0 jps rks-interface]
user@host# set pending-rks-event-max-age pending-rks-event-max-age
```

The maximum age must be greater than sent-message-timeout of the corresponding CMTS interface.

12. (Optional) Specify the maximum number of outstanding Gate-Info requests.

```
[edit slot 0 jps rks-interface]
user@host# set held-decs-max-size held-decs-max-size
```

13. (Optional) Specify the oldest age of outstanding Gate-Info requests.

```
[edit slot 0 jps rks-interface]
user@host# set held-decs-max-age held-decs-max-age
```

The maximum age must be greater than sent-message-timeout of the corresponding CMTS interface.

14. (Optional) Specify the size of billing correlation ID (BCID) cache.

```
[edit slot 0 jps rks-interface]
user@host# set bcid-cache-size bcid-cache-size
```

15. (Optional) Specify the oldest age of billing correlation ID (BCID) in cache.

```
[edit slot 0 jps rks-interface]
user@host# set bcid-cache-age bcid-cache-age
```

16. (Optional) Specify whether the default RKS pair is used when an application manager requests the use of an unconfigured RKS pair.

```
[edit slot 0 jps rks-interface]
user@host# set use-default-when-am-requests-unconfigured-rks
```

17. (Optional) Verify your configuration.

```
[edit slot 0 jps rks-interface]
user@host# show
```

Configuring RKS Pairs

By default, the JPS has four RKS pairs. All parameters that share the same RKS pair name configure the connection to that RKS pair. Any configured RKS pair can be used as the value for the default RKS pair or the RKS pair associated with a specific application manager.



NOTE: When running more than one JPS in a group to provide redundancy, all the JPSs in that group must have same RKS pair configuration (including the default RKS pair and any configured RKS pairs associated with a specific application manager).

Use the following configuration statement to configure the RKS pair:

```
slot number jps rks-interface rks-pair rks-pair-name {
  primary-address primary-address;
  primary-port primary-port;
  secondary-address secondary-address;
  secondary-port secondary-port;
}
```

To configure the RKS pair:

1. From configuration mode, access the configuration statement that configures the RKS pair. In this sample procedure, the RKS pair called pair1 is configured.

```
user@host# edit slot 0 jps rks-interface rks-pair pair1
```

2. Specify the IP address of the primary RKS for this RKS pair.

```
[edit slot 0 jps rks-interface rks-pair pair1]
user@host# set primary-address primary-address
```

If no value is specified, the RKS pair is not defined.

3. (Optional) Specify the UDP port on the primary RKS to which the JPS sends events.

```
[edit slot 0 jps rks-interface rks-pair pair1]
user@host# set primary-port primary-port
```

4. (Optional) Specify the IP address of the secondary RKS for this RKS pair.

```
[edit slot 0 jps rks-interface rks-pair pair1]
user@host# set secondary-address secondary-address
```

5. (Optional) Specify the UDP port on the secondary RKS to which the JPS sends events.

```
[edit slot 0 jps rks-interface rks-pair pair1]
user@host# set secondary-port secondary-port
```

6. (Optional) Verify your configuration.

```
[edit slot 0 jps rks-interface rks-pair pair1]
user@host# show
primary-address ;
primary-port 1813;
secondary-address ;
secondary-port 1813;
```

Configuring RKS Pairs for Associated Application Managers

By default, the JPS has four associated application managers. All parameters that share the same application manager name configure the RKS pair to which events associated with a specific application manager are sent.

Use the following configuration statement to configure the associated application manager:

```
slot number jps rks-interface am am-name {
    am-id am-id;
    rks-pair-name rks-pair-name;
    trusted;
}
```

To configure the associated application manager:

1. From configuration mode, access the configuration statement that configures the RKS pair for the associated application manager. In this sample procedure, the application manager name called 1 is configured.

```
user@host# edit slot 0 jps rks-interface am 1
```

2. Specify the identifier of the application manager.

```
[edit slot 0 jps rks-interface am 1]
user@host# set am-id am-id
```

If no value is specified, the RKS pair configuration is not defined for this application manager. If you must set `trusted` to true without defining the RKS pair configuration, you must specify a value for `am-id` and not specify a value for `rks-pair-name`.

3. (Optional) Specify the RKS pair that the JPS will send events to when those events are triggered by gate transitions associated with the application manager specified by `am-id` with the same application manager name (`am-name`).

```
[edit slot 0 jps rks-interface am 1]
user@host# set rks-pair rks-pair-name
```

If no value is specified, the RKS pair configuration is not defined for this application manager. Use when you must set `trusted` to true without defining the RKS pair configuration.

4. (Optional) Specify whether this application manager is a trusted network element to the JPS.

```
[edit slot 0 jps rks-interface am 1]
user@host# set trusted
```

5. (Optional) Verify your configuration.

```
[edit slot 0 jps rks-interface am 1]
user@host# show
```

Specifying Connections to CMTS Devices

Use the following configuration statement to configure the policy server-to-CMTS interface (PKT-MM2) so that the policy server can communicate with CMTS devices:

```
slot number jps cmts-interface {
  cmts-addresses [cmts-addresses...];
  keepalive-interval keepalive-interval;
  synch-despite-unreachable-pep;
  synch-despite-pre-i03-pep;
  use-ssq-ssc-with-pre-i03-pep;
  local-address local-address;
  message-max-length message-max-length;
  message-read-buffer-size message-read-buffer-size;
  message-write-buffer-size message-write-buffer-size;
```

```

open-connection-timeout open-connection-timeout;
connection-open-retry-interval connection-open-retry-interval;
sent-message-timeout sent-message-timeout;
validate-pcmm-objects;
}

```

To configure the policy server-to-CMTS interface:

1. From configuration mode, access the configuration statement that configures the policy server-to-CMTS interface.

```
user@host# edit slot 0 jps cmts-interface
```

2. Specify the IP addresses of all the CMTS devices to which the JPS will try to connect.

```

[edit slot 0 jps cmts-interface]
user@host# set cmts-addresses [cmts-addresses...]

```

3. (Optional) Specify the interval between keepalive messages sent from the COPS client (CMTS device) to the COPS server (the JPS). Changes apply only to COPS connections that are established after you make the change.

```

[edit slot 0 jps cmts-interface]
user@host# set keepalive-interval keepalive-interval

```

A value of 0 means that no keepalive messages will be exchanged between the CMTS device and the JPS.

4. (Optional) Specify whether synchronization proceeds when the JPS receives a synchronization request from an application manager (such as the SAE) and the JPS is not connected to a CMTS device to which it should be connected.

```

[edit slot 0 jps cmts-interface]
user@host# set synch-despite-unreachable-pep

```

5. (Optional) Specify whether synchronization proceeds when the JPS receives a synchronization request from an application manager (such as the SAE) and the JPS is connected to a pre-PCMM I03 CMTS device.

```

[edit slot 0 jps cmts-interface]
user@host# set synch-despite-pre-i03-pep

```

6. (Optional) Specify whether synchronization includes both pre-PCMM I03 and PCMM I03 CMTS devices when the JPS receives a synchronization request from an application manager (such as the SAE) and the JPS is connected to a pre-PCMM I03 CMTS device. Relevant only when at least one pre-PCMM I03 CMTS device is connected and synch-despite-pre-i03-pep is specified as true.

```

[edit slot 0 jps cmts-interface]
user@host# set use-ssq-ssc-with-pre-i03-pep

```

7. (Optional) Specify the source IP address that the JPS uses to communicate with CMTS devices.

```
[edit slot 0 jps cmts-interface]
user@host# set local-address local-address
```

If no value is specified and there is more than one local address, a random local address is used as the source address.

8. (Optional) Specify the maximum length of incoming messages.

```
[edit slot 0 jps cmts-interface]
user@host# set message-max-length message-max-length
```

9. (Optional) Specify the size of message read buffer.

```
[edit slot 0 jps cmts-interface]
user@host# set message-read-buffer-size message-read-buffer-size
```

10. (Optional) Specify the size of message write buffer.

```
[edit slot 0 jps cmts-interface]
user@host# set message-write-buffer-size message-write-buffer-size
```

11. (Optional) Specify the maximum time to wait for the initial PCMM messages to be exchanged after a TCP connection is established.

```
[edit slot 0 jps cmts-interface]
user@host# set open-connection-timeout open-connection-timeout
```

The connection is dropped when initial PCMM messages are not exchanged within this time period.

12. (Optional) Specify the time to wait before the JPS tries to reconnect to CMTS devices.

```
[edit slot 0 jps cmts-interface]
user@host# set connection-open-retry-interval connection-open-retry-interval
```

13. (Optional) Specify the maximum time to wait for the sent messages to be exchanged after a TCP connection is established.

```
[edit slot 0 jps cmts-interface]
user@host# set sent-message-timeout sent-message-timeout
```

This value must be less than the held-decs-max-age and pending-rks-event-max-age values for the corresponding RKS interface.

14. (Optional) Specify whether to validate PCMM objects received from PDPs.

```
[edit slot 0 jps cmts-interface]
user@host# set validate-pcmm-objects
```

15. (Optional) Verify your configuration.

```
[edit slot 0 jps cmts-interface]
user@host# show
cmts-addresses ;
keepalive-interval 60;
synch-despite-unreachable-pep;
synch-despite-pre-i03-pep;
local-address ;
message-max-length 204800;
message-read-buffer-size 1000000;
message-write-buffer-size 1000000;
open-connection-timeout 5;
connection-open-retry-interval 60;
sent-message-timeout 60;
validate-pcmm-objects;
```

Modifying the Subscriber Configuration

To locate the CMTS device associated with a subscriber, the JPS maps the subscriber IP address in a message to the CMTS IP address to which the message must be delivered. This mapping specifies the subscriber IP pools associated with CMTS devices.

Use the following configuration statements to configure a CMTS device to which the JPS can connect and the pools of subscriber IP addresses that are managed by the CMTS device:

```
slot number jps cmts-registry cmts cmts-ip ...

slot number jps cmts-registry cmts cmts-ip range-pool pool-index {
    low low;
    high high;
}

slot number jps cmts-registry cmts cmts-ip subnet-pool subnet {
    exclude [exclude];
}
```


Configuring Subscriber IP Pools as IP Address Ranges

To configure subscriber IP pools that are managed by the CMTS device as IP address ranges:

1. From configuration mode, access the configuration statement that configures the CMTS device to which the JPS can connect.

```
user@host# edit slot 0 jps cmts-registry cmts cmts-ip range-pool pool-index
```

Specify the IP address of the CMTS device and the address range pool index.

2. Specify the first IP address in the IP range for the pool of subscriber IP addresses that are managed by the CMTS device.

```
[edit slot 0 jps cmts-registry cmts cmts-ip range-pool pool-index]
user@host# set low low
```

3. Specify the last IP address in the IP range for the pool of subscriber IP addresses that are managed by the CMTS device.

```
[edit slot 0 jps cmts-registry cmts cmts-ip range-pool pool-index]
user@host# set high high
```

4. (Optional) Verify your configuration.

```
[edit slot 0 jps cmts-registry]
user@host# show
```

Configuring Subscriber IP Pools as IP Subnets

To configure subscriber IP pools that are managed by the CMTS device as IP subnets:

1. From configuration mode, access the configuration statement that configures the CMTS device to which the JPS can connect.

```
user@host# edit slot 0 jps cmts-registry cmts cmts-ip subnet-pool subnet
```

Specify the IP address of the CMTS device and the IP address and mask of the subnet for the pool of subscriber IP addresses.

2. (Optional) Specify the IP addresses of the subnet that are excluded from the subscriber IP pool managed by the CMTS device.

```
[edit slot 0 jps cmts-registry cmts cmts-ip subnet-pool subnet]
user@host# set exclude [exclude...]
```

3. (Optional) Verify your configuration.

```
[edit slot 0 jps cmts-registry]
user@host# show
```

Configuring the SAE to Interact with the JPS

You must configure the SAE as an application manager to allow it to interact with PCMM-compliant policy servers. The policy server acts as a policy decision point that manages the relationships between application managers and CMTS devices. Policy servers that manage the same group of CMTS devices are grouped together and are simultaneously active. The policy server group provides a way for the SAE to communicate with any CMTS device that is managed by a policy server in the policy server group. To provide redundancy, the SAEs are grouped in an SAE community that connects to a policy server group. Only one of the SAEs in the SAE community is active. The active SAE establishes connections to all the policy servers in the policy server group. The active SAE will fail over to a redundant SAE only when it loses the connection to all the policy servers in the policy server group. State synchronization enables the SAE to synchronize its state with all the CMTS devices connected to a policy server group.

The tasks to configure the SAE as an application manager are:

- Specifying Application Managers for the Policy Server on page 98
- Specifying Application Manager Identifiers for Policy Servers on page 100
- Adding Objects for Policy Servers to the Directory on page 100
- *Configuring Initialization Scripts* on page 101
- Enabling State Synchronization on page 101

Specifying Application Managers for the Policy Server

To specify the SAE community that connects to a policy server group, you need to add an application manager group object to the directory.

Use the following configuration statements to specify the application manager for the policy server:

```
shared network application-manager-group name {
    description description;
    application-manager-id application-manager-id;
    connected-sae [connected-sae...];
    pdp-group pdp-group;
    local-address-pools [local-address-pools...];
    managing-sae-ior managing-sae-ior;
}
```

To add an application manager group:

1. From configuration mode, access the configuration statement that specifies the application managers.

```
user@host# edit shared network application-manager-group name
```

2. (Optional) Specify information about the SAE community.

```
[edit shared network application-manager-group name]
user@host# set description description
```

3. (Optional) Specify the unique identifier within the domain of the service provider for the application manager that handles the service session (Application Manager Tag) as a 2-byte unsigned integer.

```
[edit shared network application-manager-group name]
user@host# set application-manager-id application-manager-id
```

4. (Optional) Specify the SAEs that are connected to the specified policy server group. This list becomes the community of SAEs.

```
[edit shared network application-manager-group name]
user@host# set connected-sae [connected-sae...]
```

When you modify a community, wait for passive session stores of the new community members to be updated before you shut down the current active SAE. Otherwise, a failover from the current active SAE to the new member is triggered immediately, and the new member's session store may not have received all data from the active SAE's session store.

5. (Optional) Specify the name of the policy server group associated with this SAE community.

```
[edit shared network application-manager-group name]
user@host# set pdp-group pdp-group
```

6. (Optional) Specify the list of IP address pools that the specified PDP group currently manages and stores.

```
[edit shared network application-manager-group name]
user@host# set local-address-pools local-address-pools
```

You must configure a local address pool if you are using the NIC so that the NIC can resolve the IP-to-SAE mapping. See *Using the NIC Resolver* on page 102.

7. (Optional) Specify the Common Object Request Broker Architecture (CORBA) reference for the SAE managing this policy server group.

```
[edit shared network application-manager-group name]
user@host# set managing-sae-ior managing-sae-ior
```

The **amIorPublisher** script provides this information when the SAE connects to the policy server. If you do not select this script when configuring initialization scripts, enter a value. For information about configuring initialization scripts, see *Configuring Initialization Scripts* on page 101.

Specifying Application Manager Identifiers for Policy Servers

The application manager identifier (AMID) identifies the application manager (such as the SAE) in messages sent to and from the policy server. The SAE constructs the AMID value by concatenating two fields: Application Manager Tag and Application Type.

The Application Manager Tag value is obtained from the specification of application managers for policy servers. See *Specifying Application Managers for the Policy Server* on page 98.

The Application Type value is obtained during service activation from the specification of the PCMM Application Type value when you configure normal services. For more information about configuring services, see *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI*.

Adding Objects for Policy Servers to the Directory

To communicate with policy servers, the SAE creates and manages pseudointerfaces that it associates with a policy decision point object in the directory. Each policy server in the SRC network must appear in the directory as a policy decision point object.

Use the following configuration statements to specify the policy server as a policy decision point:

```
shared network policy-decision-point name {
    description description;
    pdp-address pdp-address;
    pdp-group pdp-group;
}
```

To add a policy server to the directory with the SRC CLI:

1. From configuration mode, access the configuration statement that configures the policy decision point.

```
user@host# edit shared network policy-decision-point name
```

2. (Optional) Specify information about the policy server.

```
[edit shared network policy-decision-point name]
user@host# set description description
```

3. (Optional) Specify the IP address of the policy server. The SAE uses this address to establish a COPS connection with the policy server.

```
[edit shared network policy-decision-point name]
user@host# set pdp-address pdp-address
```

4. (Optional) Specify the name of the policy server group.

```
[edit shared network policy-decision-point name]
user@host# set pdp-group pdp-group
```

5. Create an SAE community for the policy servers. See *Specifying Application Managers for the Policy Server* on page 98.

Configuring Initialization Scripts

When the SAE establishes a connection with a policy server, it runs an initialization script to customize the setup of the connection.

Use the following configuration statement to configure the initialization script:

```
shared sae configuration driver scripts {
  pcmm pcmm;
}
```

To configure initialization scripts for the SAE:

1. From configuration mode, access the configuration statement that configures the initialization scripts.

```
user@host# edit shared sae configuration driver scripts
```

2. Specify the initialization script for a PCMM environment.

```
[edit shared sae configuration driver scripts]
user@host# set pcmm pcmm
```

The script is run when the connection between a policy server and the SAE is established and again when the connection is dropped. For the JPS, we recommend setting this value to `amIorPublisher`.

Enabling State Synchronization

State synchronization is achieved when the SAE is required to communicate with the policy server over the COPS connection.

Use the following configuration statement to configure state synchronization:

```
shared sae configuration driver pcmm {
  disable-full-sync;
  disable-pcmm-i03-policy;
  session-recovery-retry-interval session-recovery-retry-interval;
}
```

To enable state synchronization with policy servers:

1. From configuration mode, access the configuration statement that configures the PCMM device driver.

```
user@host# edit shared sae configuration driver pcmm
```

2. Specify whether state synchronization with the PCMM policy servers is disabled.

```
[edit shared sae configuration driver pcmm]
user@host# set disable-full-sync
```

When using other PCMM-compliant policy servers (instead of the JPS), we recommend setting this value to true.

3. Specify whether PCMM I03 policies are disabled when the SAE is deployed with pre-PCMM I03 CMTS devices.

```
[edit shared sae configuration driver pcmm]
user@host# set disable-pcmm-i03-policy
```

When there are pre-PCMM I03 CMTS devices in the network, you must set this value to true.

4. Specify the time interval between attempts by the SAE to restore service sessions that are still being recovered in the background when state synchronization completes with a state-data-incomplete error.

```
[edit shared sae configuration driver pcmm]
user@host# set session-recovery-retry-interval session-recovery-retry-interval
```

We recommend setting this value to 3600000 (1 hour) or longer.

Using the NIC Resolver

If you are using the NIC to map the subscriber IP address to the SAE, you need to configure a NIC host. The NIC system uses IP address pools to map IP addresses to SAEs. You configure the local address pools in the application manager configuration for a policy server group. These pools are published in the NIC. The NIC maps subscriber IP addresses in requests received through the portal or Advanced Services Gateway to the policy server group that currently manages that CMTS device. For information about configuring the SAE for policy servers, see *Specifying Application Managers for the Policy Server* on page 98.

The OnePopPcmm sample configuration data supports this scenario for a PCMM environment in which you use the assigned IP subscriber method to log in subscribers and in which you use the NIC to determine the subscriber's SAE. The OnePopPcmm configuration supports one point of presence (POP). NIC replication can be used to provide high availability. The realm for this configuration accommodates the situation in which IP pools are configured locally on each application manager group object.

The resolution process takes a subscriber's IP address as the key and returns a reference to the SAE managing this subscriber as the value.

The following agents collect information for resolvers in this realm:

- Directory agent PoolVr collects and publishes information about the mappings of IP pools to the policy server group.
- Directory agent VrSaeld collects and publishes information about the mappings of policy server groups to SAEs.

For more information about configuring the NIC, see *SRC-PE Network Guide, Chapter 10, Configuring NIC with the SRC CLI*.

Managing the JPS

After you have installed the JPS and applied the local configuration of the JPS, you can perform these tasks:

- Starting the JPS on page 103
- Restarting the JPS on page 103
- Stopping the JPS on page 104
- Displaying JPS Status on page 104

To modify the JPS configuration, see *Configuring the JPS* on page 83. To monitor the JPS, see *Chapter 12, Monitoring the JPS with the SRC CLI*.

Starting the JPS

You must start the JPS when you install the JPS without rebooting the JPS host.

To start the JPS:

```
user@host> enable component jps
```

The system responds with a start message. If the JPS is already running, the system responds with a warning message.

Restarting the JPS

To restart the JPS:

```
user@host> restart component jps
```

The system responds with a start message. If the JPS is already running, the system responds with a shutdown message and then a start message.

Stopping the JPS

To stop the JPS:

```
user@host> disable component jps
```

The system responds with a shutdown message. If the JPS is not running when you issue the command, the system responds with the command prompt.

To start the JPS, see *Starting the JPS* on page 103.

Displaying JPS Status

To display the JPS status:

```
user@host> show component
```

The system responds with a status message.