## Chapter 16

# Providing Services in IMS Networks

This chapter describes the SRC application's support for IP multimedia subsystem (IMS). Topics include:

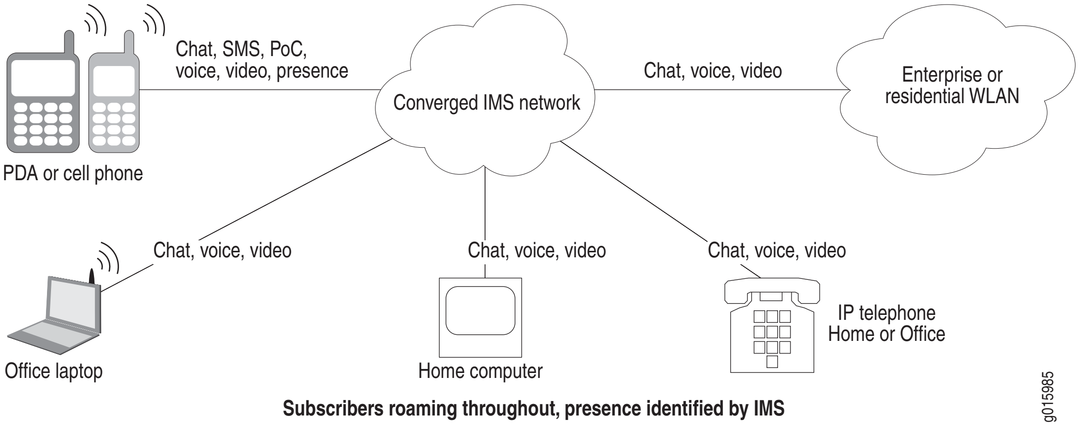
## Overview of an IMS Environment

IP multimedia subsystem (IMS) is a flexible network architecture that allows providers to introduce rich multimedia services across both next-generation packet-switched and traditional circuit-switched networks. It uses open interfaces and functional components that can be assembled flexibly to support real-time interactive services and applications.

Third Generation Partnership Project (3GPP) developed IMS to provide a standards-based architecture for mobile carriers to migrate to their next-generation networks that will support applications that combine voice, video, and data functionality. The European Telecommunications Standards Institute (ETSI) created Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN) to extend IMS support to fixed-line carriers. This extension is commonly called fixed mobile convergence (FMC). IMS/FMC allows subscribers to access any network (wireless or fixed) from any device (computer, PDA, or cell phone) and be able to move seamlessly from one network to another.

Figure 17 shows, at a high level, a converged IMS network that manages and controls the movement of subscribers between fixed and wireless networks.

**Figure 17: A Simplified IMS Converged Network (Service Focus)**



By itself, IMS does not specify new services; rather, it provides a framework for network operators to build and launch their services regardless of access method. The IMS architecture simplifies network operations and allows providers to focus on service introduction and business opportunities. For example, an IMS architecture could allow fixed and mobile users to communicate using voice, video, chat, and online gaming, and to take advantage of functionality such as Push-to-Talk over Cellular (PoC; the ability to quickly arrange meetings through a walkie-talkie mechanism), instant messaging, and presence (whether and how a subscriber is available, and how the subscriber wants to be contacted).

## IMS and ETSI References

For more information about IMS and TISPAN, consult the following specifications:

- ETSI ES 283 026 V0.0.7 (2005-10) *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specification.*

- ETSI TS 183 017 V.0.0.8 (2005-10) *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol specification.*

- ETSI ES 283 034 V0.0.5 (2005-10) *Telecommunications and Internet converged Services and Protocols for Advanced Networks (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol.*

### *Abbreviations*

Table 9 identifies abbreviations used in the IMS and ETSI-TISPAN environments.

**Table 9: Abbreviations in the IMS and ETSI-TISPAN Environments**

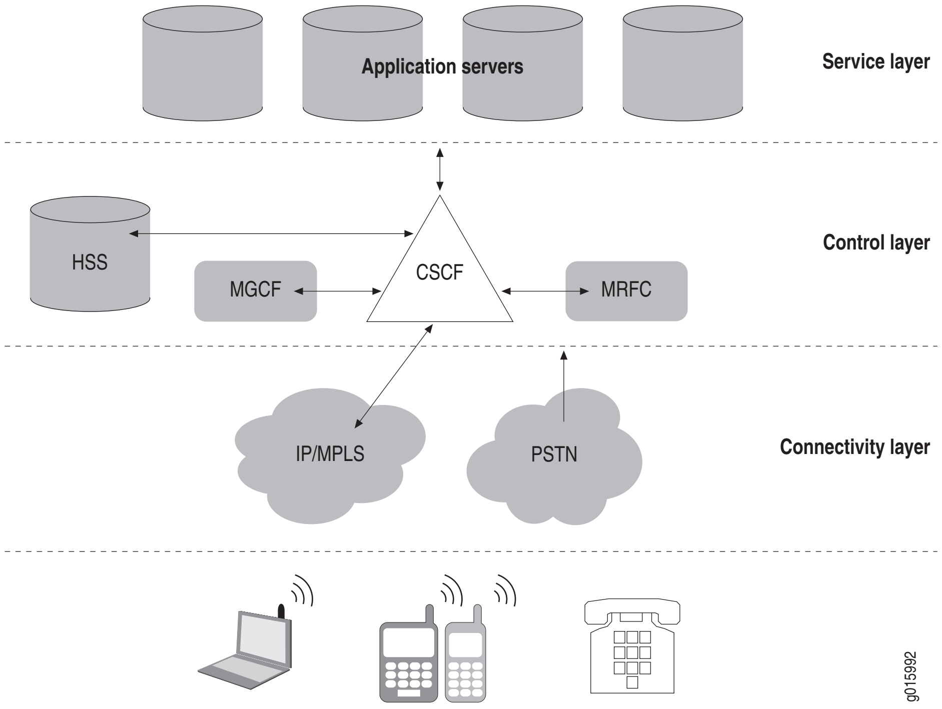
| Abbreviation | Description |
|---|---|
| 3GPP | 3rd Generation Partnership Project, which developed the IMS specifications. |
| A-RACF | Access-resource and admission control function. Provides admission control and network policy assembly. |
| AVP | Attribute value pair |
| BGF | Border gateway function |
| ETSI | European Telecommunications Standards Institute |
| FMC | Fixed mobile convergence |
| IMS | IP multimedia subsystem |
| NGN | Next-generation network |
| RACS | Resource and admission control subsystem. Consists of the A-RACF and the SPDF. |
| RCEF | Resource control enforcement function |
| SPDF | Service policy decision function. The SPDF coordinates the resource reservations requests that it receives from the application function. |
| TISPAN | Telecommunications and Internet Converged Services and Protocols for Advanced Networks |

## IMS Layers

The IMS specifications define functions to handle the signaling and subscriber traffic for multimedia applications. The functions are separated into logical layers, and many of the specified functions often reside in a single platform. Vendors have the flexibility to implement IMS functions in consolidated ways, and it is natural that platforms such as softswitches will combine many logically separate IMS call-processing functions, and that routers will take on some of the session-enforcement and gateway functionality in IMS.

The three layers are the service layer, the control layer, and the transport layer. Figure 18 shows a high-level view of the IMS architecture.

**Figure 18: High-Level View of the IMS Architecture**



- Service layer—Hosts application and content services, including application servers and Web servers. It also includes generic service enablers that manage service elements such as user groups and presence. These service elements connect to subscribers through the control plane. The application layer supports most of the multimedia applications or application enablers, such as presence and location of the subscriber.
- Control layer—Makes the policy decisions that are enforced in the transport layer. This layer provides session control and management, and is responsible for setting up and taking down packet sessions. It also contains information about subscriber authentication, service authorization, and location.
- Connectivity layer—Supports the core network architecture of the General Packet Radio Service (GPRS), which consists of support nodes for data services. This layer is where routers, switches, firewalls, and optical transport reside, along with gateways that translate protocols between packet- and circuit-based traffic.

## Signaling Protocol

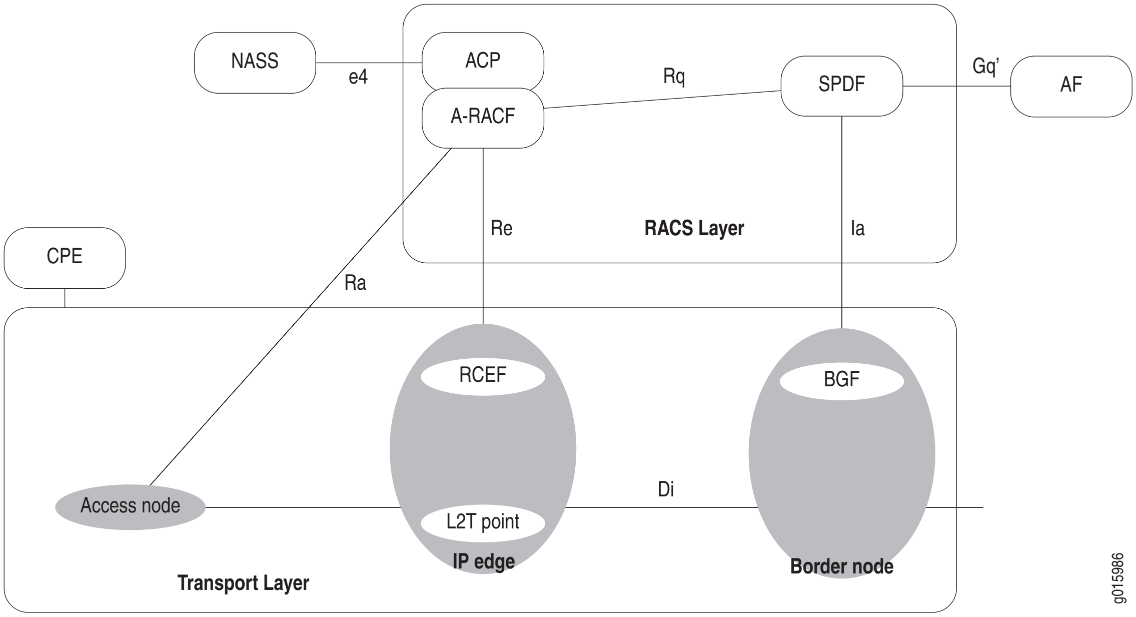
Session Initiation Protocol (SIP) is the main signaling protocol in IMS. SIP is the proposed standard for multimedia communication between subscribers interacting with voice, video, and instant messaging. In IMS, the use of SIP facilitates interconnectivity between fixed and mobile networks.

## ETSI-TISPAN Architecture

TISPAN is an extension to the IMS architecture developed by ETSI to fit the specific requirements of fixed-line providers.

Figure 19 shows a high-level view of the TISPAN architecture.

**Figure 19: High-Level View of the ETSI-TISPAN Architecture**



### RACS Layer

The RACS layer is the TISPAN next-generation network subsystem that is responsible for elements of policing control, including resource reservation and admission control in the access and aggregation networks. The RACS layer also includes support for NAT in the access, aggregation, and core networks required to support end-to-end application-initiated sessions.

The RACS provides policy-based transport control services to applications. These services enable applications to request and reserve transport resources from transport resources from the transport networks within the scope of the RACS.

### Rq Interface

The Rq interface is the interface between the SPDF and the A-RACF. The SPDF issues requests for resources in the access network through the Rq interface. These requests indicate IP QoS characteristics. The A-RACF uses the IP QoS information to perform admission control and indicates to the SPDF through the Rq interface its admission control decisions.

### SPDF

The SPDF is a functional element that coordinates the resource reservations requests that it receives from the application function (the application-level controller, such as a SIP server). The SPDF performs the following functions:

- Determines whether the request information received from the application function is consistent with the policy rules defined in the SPDF.
- Authorizes the requested resources for the application function session. The SPDF uses the request information received from the application function to calculate the proper authorization (that is, to authorize certain media components).
- Provides the location of the BGF and/or the A-RACF device, in accordance with the required transport capabilities.
- Requests resources of the A-RACF.
- Requests services from the BGF.
- Hides the details of the RACS and the core transport layer from the control architecture.
- Provides resource mediation by mapping requests from application functions toward an appropriate A-RACF and/or BGF.

### A-RACF

The A-RACF is a functional element that provides admission control and network policy assembly.

For admission control, the A-RACF receives requests for QoS resources from the SPDF and uses the QoS information received to perform admission control. It then indicates to the SPDF whether or not a request for resources is granted.

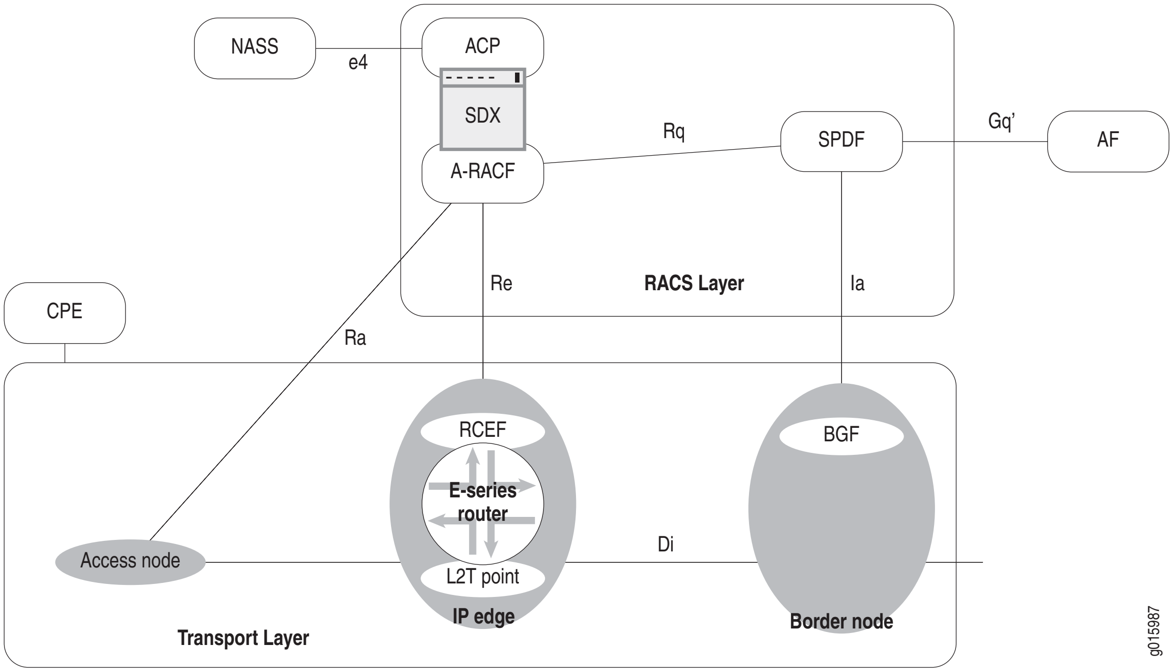
Access network policies are a set of rules that specify the policies that should be applied to an access line. For network policy assembly, the A-RACF:

- Ensures that requests from the SPDF match the access policies because multiple SPDFs can request resources from the A-RACF.
- Combines the requests from the SPDFs that have requested resources and ensures that the total of the requests match the capabilities of the access line.

## SRC Software in the ETSI-TISPAN Architecture

Figure 20 shows the SRC software in the ETSI-TISPAN architecture.

**Figure 20: SRC Software in the ETSI-TISPAN Architecture**



The SAE provides the A-RACF functionality, and the SRC software provides a northbound Rq interface from the A-RACS to the SPDF. This interface is equivalent to the Rq interface defined in the ETSI-TISPAN release 1 architecture. It is a DIAMETER protocol–based interface that allows the SRC software to integrate with services found on the application layer of IMS.

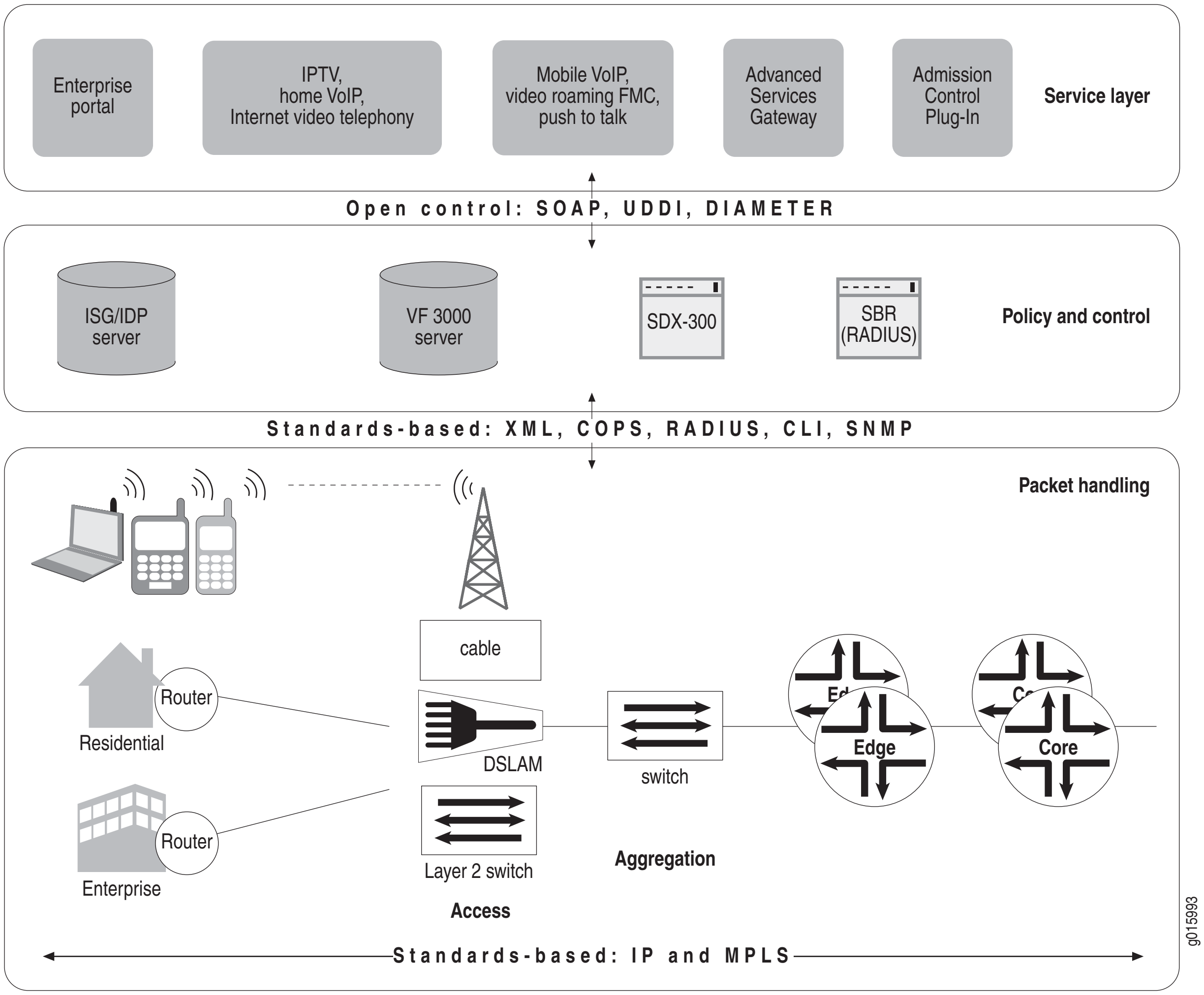
The SRC software uses its COPS and BEEP interfaces as the Re interface to Juniper Networks routers.

## SRC Software in the IMS Environment

Figure 21 shows the Juniper Networks layered IMS architecture.

The northbound Rq interface of the policy and control layer allows integration with SRC applications, such as the portals, the Advanced Services Gateway, and the Admission Control Plug-In.

**Figure 21: Juniper Networks IMS Architecture**


Enterprise portal
IPTV, home VoIP, Internet video telephony
Mobile VoIP, video roaming FMC, push to talk
Advanced Services Gateway
Admission Control Plug-In
Service layer
Open control: SOAP, UDDI, DIAMETER
ISG/IDP server
VF 3000 server
SDX-300
SBR (RADIUS)
Policy and control
Standards-based: XML, COPS, RADIUS, CLI, SNMP
Packet handling
cable
Router
Residential
DSLAM
switch
Edge
Core
Router
Enterprise
Layer 2 switch
Aggregation
Access
g015993
Standards-based: IP and MPLS

## Installing and Configuring the IMS Software

To install and configure the IMS software:

1. On the UNIX host where you will install the IMS software, log in as `root`.
2. Load SRC software disk 1 into the CD drive.
3. Install the UMCims package using the UNIX **pkgadd** tool.

   ```
   pkgadd -d /cdrom/cdrom0/SDX_DISK1/solaris10 UMCims
   ```

4. Follow the instructions on your screen to install the IMS software.

   The UMCims package is installed in the */opt/UMC/ims* folder.

5. Run the following command in the */opt/UMC/ims* folder.

   ```
   etc/config -a
   ```

6. Configure the local and remote DIAMETER peers in the */opt/UMC/ims/etc/config.properties* file.

   See *Configuration Fields for DIAMETER Peers* on page 157.

7. Configure logging destinations.

   See *Configuring Logging Destinations* on page 158.

8. Start the process to provide the A-RACF Rq interface.

   See *Starting the IMS Process to Provide the A-RACF Rq Interface* on page 161.

### Configuration Fields for DIAMETER Peers

The properties in this section are in the */opt/UMC/ims/etc/config.properties* file.

#### local.address

- IP address of the local DIAMETER peer that is providing the A-RACF Rq interface.
- Value—IP address of the local host that is running A-RACF
- Default—127.0.0.1
- Property name—/ims/A-RACF/Rq/local.address

#### peer.1.remote.address

- IP address of the remote DIAMETER peer that is providing the SPDF Rq interface.
- Value—IP address of the host that is running SPDF.
- Default—127.0.0.1
- Property name—/ims/A-RACF/Rq/peer.1.remote.address

## Configuring Logging Destinations

The properties in this section are in the */opt/UMC/ims/etc/config.properties* file. By default, the IMS has three logging destinations. To configure the logging destinations, modify the following parameters in the Logging section of the IMS config.properties file, where <loggerName> is a string that groups parameters for the logging destination.

For more information about logging, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 5, Managing SRC Log Files on a Solaris Platform*.

### Logger.<loggerName>.class

- Specifies the type of logging.
- Value
  - file—Event messages are written to a text file.
  - stream—Event messages are written to stderr or stdout output.
  - syslog—Event messages are written to system log (syslog) facilities.

  If you do not fill in this field, the logging destination is disabled, and no logging is performed.
- Default—file

### Logger.<loggerName>.filter

- Specifies the type of messages that this log file contains.
- Value—Filter definition. If you do not fill in this field, filtering is disabled.

  For more information about defining filters, see *Categories and Severity Levels for Event Messages* in the *SRC-PE Monitoring and Troubleshooting Guide, Chapter 2, Configuring Logging for SRC Components*.
- Default
  - For Logger.log1.filter—/debug-
  - For Logger.log2.filter—/info-
  - For Logger.log3.filter—/error-

### Logger.<loggerName>.filename

- Path of the file that contains the current logs for file-based logging.
- Value—Pathname
- Default
  - For Logger.log1.filename—*var/log/ims-a-racf-rq-debug.log*
  - For Logger.log2.filename—*var/log/ims-a-racf-rq-info.log*
  - For Logger.log3.filename—*var/log/ims-a-racf-rq-error.log*

### *Logger.<loggerName>.maxsize*

- Maximum size of the log file for file-based logging.
- Value—Number of kilobytes in the range 0–4294967295
- Guidelines—Do not set the maximum file size to a value greater than the available disk space.
- Default—2000000000

### *Logger.<loggerName>.altfile*

- Path of the alternate file. When the log file exceeds the maximum size specified by the Logger.<loggerName>.maxsize parameter, its contents are saved to this alternate file. If an alternate file already exists, it is overwritten.
- Value—Pathname
- Default
  - For Logger.log1.filename—*var/log/ims-a-racf-rq-debug.alt*
  - For Logger.log2.filename—*var/log/ims-a-racf-rq-info.alt*
  - For Logger.log3.filename—*var/log/ims-a-racf-rq-error.alt*

### *Logger.<loggerName>.stream*

- Stream to use for stream-based logging.
- Value
  - stderr—Event messages are written to stderr output
  - stdout—Event messages are written to stdout output
- Default
  - For Logger.log1.stream—stdout
  - For Logger.log2.stream—stdout
  - For Logger.log3.stream—stderr

### *Logger.<loggerName>.hostname*

- IP address or name of a host that collects event messages by means of a standard system logging daemon.
- Value—IP address or text string
- Default—localhost

### *Logger.<loggerName>.facility*

- Specifies the type of system log in accordance with the system logging protocol.
- Value—Integer in the range 0–23; each integer corresponds to the standard number for a system logging client
- Default—No value

### *Logger.<loggerName>.format*

- Specifies how the information in an event message is printed for syslog-based logging.
- Value—MessageFormat string as specified in

  http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html

  The fields available for events are:

  - 0—Time and date of the event
  - 1—Name of the thread generating the event
  - 2—Text message of the event
  - 3—Category of the event
  - 4—Priority of the event
- Default—No value

## *Bootstrap Properties for IMS*

The properties in this section are in the IMS *bootstrap.properties* file.

### *Config.java.naming.provider.url*

- URL of the primary directory that stores configuration information.
- Value—ldap:// <host>:<portNumber>
  - <host>—IP address or name of host that supports the Web application
  - <portNumber>—Number of the TCP port
- Default—ldap://127.0.0.1:389/

### *Config.java.naming.security.credentials*

- Password that the Web application server uses to authenticate and authorize gateway clients.
- Value—<password>
- Guidelines—The password can be encoded in base64 and not visible in plain text. To use an encoded value, use the format {BASE64} <encoded-value>.
- Default—conf

### *Config.java.naming.security.principal*

- DN that contains the username that the Web application server uses to authenticate and authorize gateway clients.
- Value—DN of object that contains the username
- Default—*cn=conf, o=Operators, o=umc*

**Config.net.juniper.smgt.lib.config.staticConfigDN**

- Root of the static configuration properties.
- Value—DN of object that contains the username
- Default—*l = OnePop, l = NIC, ou = staticConfiguration, ou = configuration, o = Management, o = umc* (root of static configuration properties of sample data)

**Config.net.juniper.smgt.lib.config.dynamicConfigDN**

- Root of the dynamic configuration properties.
- Value—DN of object that contains the username
- Default—*ou = dynamicConfiguration, ou = configuration, o = Management, o = umc* (root of dynamic configuration properties of sample data)

**Config.net.juniper.smgt.des.<propertySuffix>**

- Set of properties that specify how IMS interacts with the directory.
- Values—See *SRC-PE Getting Started Guide, Chapter 37, Distributing Directory Changes to SRC Components on a Solaris Platform*.
- Defaults—See *SRC-PE Getting Started Guide, Chapter 37, Distributing Directory Changes to SRC Components on a Solaris Platform*.

**Logger.file<propertySuffix>**

- Set of properties that specify how IMS events are logged to files.
- Values—See *SRC-PE Monitoring and Troubleshooting Guide, Chapter 5, Managing SRC Log Files on a Solaris Platform*.
- Defaults—See *SRC-PE Monitoring and Troubleshooting Guide, Chapter 5, Managing SRC Log Files on a Solaris Platform*.

**nic.<propertySuffix>**

- Set of properties that configure the NIC proxy.
- Values—See *SRC-PE Network Guide, Chapter 13, Configuring Applications to Communicate with an SAE*.
- Defaults—See *SRC-PE Network Guide, Chapter 13, Configuring Applications to Communicate with an SAE*.

## Starting the IMS Process to Provide the A-RACF Rq Interface

To start the IMS process to provide the A-RACF Rq interface:

1. On the IMS host, log in as `root` or as an authorized nonroot admin user.
2. Start the process from its installation directory.

   ```
   /opt/UMC/ims/etc/ims start
   ```

   The system responds with a start message.

### Stopping the IMS Process to Provide the A-RACF Rq Interface

To stop the IMS process to provide the A-RACF Rq interface:

1. On the IMS host, log in as `root` or as an authorized nonroot admin user.
2. Stop the process from its installation directory.

   ```
   /opt/UMC/ims/etc/ims stop
   ```

   The system responds with a stop message.

### Cleaning the IMS Log Files

To clean the IMS log files:

1. On the IMS host, log in as `root` or as an authorized nonroot admin user.
2. Enter the following command in the IMS installation directory.

   ```
   /opt/UMC/ims/etc/ims clean
   ```

## Testing and Demonstrating the A-RACF Rq Interface

A sample SPDF that provides the Rq interface is included in the software for testing and demonstrating the A-RACF Rq. The SPDF Rq programs send activation requests, modification requests, and deactivation requests for the News service to the A-RACF Rq interface for various subscribers.

To run this program:

1. Run the following command in the */opt/UMC/ims* folder if you have not already done so.

   ```
   etc/config -a
   ```

2. Enter the following command:

   ```
   etc/SPDF-rq-sample appl [argument…]

   @param arguments
   args[0] address of the local peer, SPDF in this case.
   args[1] address of the remote peer, A-RACF in this case.
   args[2] number of seconds given the local peer to run. When
             the time is up the local will shutdown.
   args[3] number of seconds used in this range to wait before
             sending requests to the remote peer. For example a
             value of 25 means that from 0 to 25 seconds wait
              is inserted between each call (with and average
             delay of 12.5 seconds).
   args[4] number of subscribers to iterate over. The loop
             starts with the subscriber base address and is incremented
              by one in each step of the loop. For example, 100.
   args[5] subscriber base address. For example, 10.20.0.0.
   ```

### Rq Interface Messaging

The following information provides a high-level description of the Rq interface and its messaging:

- A-RACF receives DIAMETER-messages from SPDF:
    - AA-Request for session initiation and for session modification
    - ST-Request for session termination
- In case of an AA-Request, the A-RACF verifies whether Session-Id AVP is new or already known. If new, a session is initiated; otherwise an existing session is modified.
- A-RACF gets the AF-Application-Id AVP within the Media-Component-Description AVPs to determine the service to be activated or modified.
- A-RACF retrieves the Framed-Ip-Address AVP within the Globally-Unique-Ip-Address AVPs to determine the IP address of the subscriber.
- A-RACF checks Flow-Status AVP. If the value is disabled, the session is reserved. If the value is enabled, the session is committed.
- The A-RACF reads the remaining DIAMETER AVPs and maps them according to the SAE external interface requirements.
- The A-RACF requests the required resources from the RCEF via the Re interface.
- A-RACF acknowledges the AA-Request with an AA-Answer back to the SPDF.

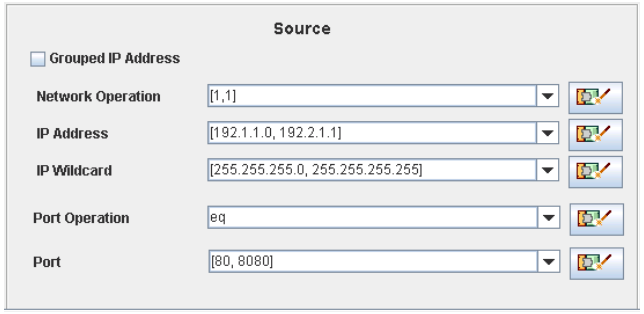
## Configuring Policies for IMS

For IMS environments, you can configure JUNOSe policies. When you configure classify-traffic conditions, you can set up the software so that the SAE expands into multiple classifiers before it installs the policy on the router. If you enter a comma-separated list of values in the source and destination network (IP address, mask, and IP operation) or port fields (for port-related protocols), the software creates a classifier for each possible combination of address and port. Note that the software does not expand classifiers for values that are entered as a range.

For example, the source configuration in the classify-traffic condition in Figure 22 would cause the condition to be expanded into four classifiers that have the following combination of source addresses and source ports:

```
192.1.1.0/255.255.255.0 eq 8
192.1.1.0/255.255.255.0 eq 8080
192.2.1.1/255.255.255.0 eq 8
192.2.1.1/255.255.255.0 eq 80
```

**Figure 22: Classify-Traffic Condition Example for Expanded Classifiers**



Source

☐ Grouped IP Address

Network Operation [1,1]

IP Address [192.1.1.0, 192.2.1.1]

IP Wildcard [255.255.255.0, 255.255.255.255]

Port Operation eq

Port [80, 8080]

## *Enabling Expansion of JUNOSe Classify-Traffic Conditions*

To use the SRC CLI to enable the expansion of JUNOSe classify-traffic conditions:

1. From configuration mode, access the SAE configuration statement for policy management.

```
[edit]
user@host# edit shared sae configuration policy-management-configuration
```

2. Enable the SAE to expand the JUNOSe classify-traffic conditions into multiple classifiers before it installs the policy on the router.

```
[edit shared sae configuration policy-management-configuration]
user@host# set enable-junose-classifier-expansion
```

---

**NOTE:** Because classifier expansion uses processing resources when the policy is created, you should set this property to true only if you are going to use the feature.

---