Chapter 2
SRC Components

This chapter provides a general overview of the components provided in the SRC software. Topics include:

Component Overview

The SRC software is a dynamic system. It contains many components that you use to build a subscriber management environment. You can use these tools to customize and extend the SRC software for your use and to integrate the SRC software with other systems. The SRC software also provides the operating system and management tools for C-series platforms.

Table 5 gives a brief description of the components that make up the SRC software and shows which components run on C-series platforms and Solaris platforms. For more information, see the following sections.

Table 5: Descriptions of SRC Components

Component	Description	SRC Software on C-series Platforms	SRC Software on Solaris Platforms
Server Components			
Service activation engine (SAE)	■ Authorizes, activates, and deactivates subscriber and service sessions by interacting with systems such as Juniper Networks routers, cable modem termination system (CMTS) devices, RADIUS servers, and directories. ■ Collects accounting information about subscribers and services from routers, and stores the information in RADIUS accounting servers, flat files, and other accounting databases. ■ Provides plug-ins and application programming interfaces (APIs) for starting and stopping subscriber and service sessions and for integrating with systems that authorize subscriber actions and track resource usage.	X	X
Juniper Policy Server (JPS)	Acts as a policy decision point (PDP) and policy enforcement point (PEP) that manages the relationships between application managers and CMTS devices in a PCMM environment.	X	X
Network information collector (NIC)	Collects information about the state of the network and can provide a mapping from a given type of network data to another type of network data.	X	X
Repository			
Directory	Provides a repository of subscriber information, services, policies, and service portal configurations. The SRC software uses the Lightweight Directory Access Protocol (LDAP) for interactions with the directory.		
Juniper Networks Database	Repository for SRC data on a C-series platform.	X	
Configuration Tools			
Local configuration tools	Generates start scripts and initial local configuration for newly installed SAEs and SNMP agents.		X
Policy Editor and management	Defines how the router or CMTS device treats subscriber traffic. Gives service providers the ability to define and modify policies and to store these policies in the directory.	CLI format	GUI format
SDX Admin	Allows service providers to add, modify, and delete services, network definitions, and advanced configurations within the SRC software.		X
SRC Command line interface (CLI)	Provides a way to configure the SRC software on a C-series platform and SRC components on a Solaris platform from a JUNOS-like CLI. The SRC CLI includes a Policies, Services, and Subscribers CLI which has separate access privileges.	X	X
SDX Configuration Editor	Provides a way to configure several other SRC components through an XML-based application. You can configure properties for SAE, NIC, and logging, as well as other features.		X

Table 5: Descriptions of SRC Components (continued)

Component	Description	SRC Software on C-series Platforms	SRC Software on Solaris Platforms
SRC Management Tools			
C-Web interface	Monitors SRC software on a C-series platform and SRC components on a Solaris platform	X	X
Prepaid Account Administration application	Manages prepaid accounts for the prepaid services demonstration application. (Available in the application library.)		X
Simple Network Management Protocol (SNMP) agent	Monitors system performance and availability. It runs on all the SRC hosts and makes management information available through SNMP tables and sends notifications by means of SNMP traps.	X	X
Traffic Mirroring Administration application	Manages and monitors mirroring tasks. (Available in the application library.)		X
Service Management Applications			
SRC SOAP Gateway (SRC-SG)	Allows a gateway client—an application that is not part of the SRC network—to interact with SRC components through a Simple Object Access Protocol (SOAP) interface. (Available in the application library.)		X
Deep Packet Inspection Integration Application	Integrates Ellacoya Networks Deep Packet Inspection (DPI) platform to provide a traffic management solution that combines the advanced traffic identification and reporting features of the Ellacoya DPI with the SRC software's intelligent service policy enforcement. (Available in the application library.)		X
Enterprise Audit Plug-In	Defines a callback interface, which receives events when IT managers complete specified operations.		X
Enterprise Manager Portal	Allows service providers to provision services for enterprise subscribers on JUNOSe routers and JUNOS routing platforms and that allows IT managers to manage services. Enterprise Manager Portal can be used with NAT Address Management Portal to allows service providers to manage public IP addresses for use with NAT services on JUNOS routing platforms and to all IT managers to make requests about public IP addresses through the Enterprise Manager Portal.		X
Intrusion detection and protection (IDP) integration applications	Integrates IDP into an SRC-managed environment to manage malicious traffic sent to or received by subscribers. (Available in the application library.)		X
Instant Virtual Extranet (IVE) Host Checker integration application	Integrates the IVE Host Checker into an SRC-managed environment to verify that the subscriber systems used to connect to a service provider comply with the service provider's policies. (Available in the application library.)		X
Prepaid service application	Demonstrates how the SRC software might be used to manage prepaid accounts. (Available in the application library.)		X
Sample enterprise service portal	Lets service providers supply an interface to their business customers for managing and provisioning services.		X
Sample IP television (IPTV) application	Demonstrates how the SRC software might be used to manage network resources for IPTV services. (Available in the application library.)	X	X

Table 5: Descriptions of SRC Components (continued)

Component	Description	SRC Software on C-series Platforms	SRC Software on Solaris Platforms
Sample residential service selection portals	Provides a framework for building Web applications that allow residential and enterprise subscribers to manage their own network services. It comes with several full-featured sample Web applications that are easy to customize and suitable for deployment.		X
Threat Mitigation Portal (SRC-TMP)	Manages threats on the SRC-managed network using information provided by Juniper Networks IDP Sensors and Juniper Networks NetScreen-Security Manager. Provides the SRC Threat Mitigation Portal (SRC-TMP) and application to manage the response to attacks. (Available in the application library.)		X
Traffic-Mirroring Application	Mirrors subscriber traffic on any subscriber access platform supported by the SRC software. Provides the Traffic-Mirroring Administration portal to manage the mirroring of subscriber traffic. (Available in the application library.)		X
Workflow application	Automates the process of provisioning and decommissioning primary access services for subscribers. (Available in the application library.)		X
SRC Application Programming Interfaces			
CORBA plug-in service provider interface (SPI)	Tracks sessions and enables linking the rest of the service provider's operations support system (OSS) with the SRC software so that the OSS can be notified of events in the life cycle of SAE sessions.	Applications that use these extensions to the SRC software run on a system other than a C-series platform	
CORBA remote API	Provides remote access to the SAE core API.		
NIC access API	Performs NIC resolutions.		
SAE core API	Controls the behavior of the SRC software.	X	X
Script services	Provides an interface to call scripts that supply custom services such as provisioning policies on a number of systems across a network.	X	X
Authorization and Accounting Applications			
AAA RADIUS servers	Authenticates subscribers and authorizes their access to the requested system or service. Accepts accounting data—time active and volume of data sent—about subscriber and service sessions.		X
SRC Admission Control Plug-In (SRC-ACP)	Authorizes and tracks subscribers' use of network resources associated with services that the SRC application manages. (Available in the application library.)	X	X
Flat file accounting	Stores tracking data to accounting flat files that can be made available to external systems that send the data to a rating and billing system.	X	X

Table 5: Descriptions of SRC Components (continued)

Component	Description	SRC Software on C-series Platforms	SRC Software on Solaris Platforms
SRC-Volume-Tracking Application (SRC-VTA)	Monitors subscriber resource usage to allow service providers to offer flexible usage quotas, limit bandwidth to subscribers that overuse network resources, and to notify subscribers who may have been compromised by viruses or worms that overuse network resources. (Available in the application library.)		X
Accessory Components			
Monitoring Agent Application	Integrates IP address managers, such as a DHCP server or a RADIUS server, into an SRC-managed network so that the SAE is notified about subscriber events. (Available in the application library.)		X
Redirect Server	Redirects HTTP requests received from IP Filter to a captive portal page.	X	X
Auxiliary Applications			
Application server	Enables J2EE applications, including Web applications, to be used with the SRC software.	These third-party applications run on a system other than a C-series platform	
IP Filter	Filters traffic as specified by configured rules.		
Other applications	Third-party applications created to run in an SRC environment.		

Server Components

This section describes the SRC server components.

Service Activation Engine

The Service Activation Engine (SAE) is the core manager of an SRC network. It interacts with other systems, such as Juniper Networks routers, CMTS devices, directories, Web application servers, and RADIUS servers to retrieve and disseminate data in the SRC environment. The SAE authorizes, activates and deactivates, and tracks sessions during which a subscriber is logged in to the network and during which a service is active. The SAE can track more than one service session for a subscriber at a time.

Policy and Service Management

The SAE makes decisions about the deployment of policies on JUNOSe routers and JUNOS routing platforms. When a subscriber's IP interface comes up on the router, the SAE determines whether it manages the interface. If the interface is managed—or controlled by—the SAE, the SAE sends the subscriber's default policy configuration to the router. These default policies define the subscriber's initial network access. When the subscriber activates an SAE service (a service that supplements a subscriber's standard services), the SAE translates the service into lists of policies and sends them to the router. This process lets subscribers manage their own subscriptions, typically through a Web page.

Accounting Support

The SAE also collects usage information about subscribers and services and passes the information to the appropriate rating and billing system. The SRC software allows a variety of accounting deployments, and provides a standard deployment that incorporates a RADIUS server. You can also create deployments that do not require a RADIUS server.

SAE Extensions

The SAE provides plug-ins and APIs that extend the capabilities of the SRC software. Plug-ins are software programs that augment existing programs and make them more flexible. SRC plug-ins provide authentication, authorization, and tracking capabilities. The SAE APIs let you create customized programs to integrate with the SAE.

Juniper Policy Server

The Juniper policy Server (JPS) is a PCMM-compliant policy server. In a PCMM environment, the policy server acts as a policy decision point (PDP) and policy enforcement point (PEP) that manages the relationships between application managers and cable management termination system (CMTS) devices.

Network Information Collector

The Network Information Collector (NIC) is the component that locates which SAE manages a subscriber or an interface. The NIC uses information that identifies the subscriber or the interface to identify the managing SAE. The NIC collects information about the state of the network and can provide a mappings from a given type of network data, known as a key, to another type of network data, known as a value.

For services to be activated for a subscriber session, applications such as the SRC-VTA, Dynamic Service Activator, Enterprise Manager Portal, or a residential portal need to locate the SAE that manages the subscriber. An application such as the SRC-TMP needs to locate the SAE that manages interfaces through which traffic destined for a specified IP address enters the network. The NIC component includes a Web administration application to monitor and inspect the state of NIC servers. Other SRC components such as an enterprise service portal and the sample residential portal use NIC.

Table 6 shows the NIC resolutions that the standard SRC software can perform. For customized NIC implementations that provide other resolutions, contact Juniper Networks Professional Services.

Table 6: Available NIC Resolutions

Key	Value
Accounting ID of a subscriber	SAE reference
Enterprise's distinguished name (DN	SAE reference
Subscriber's IP address	Subscriber's login name
Subscriber's IP address	Accounting ID

Table 6: Available NIC Resolutions (continued)

Key	Value
Subscriber's IP address for situations in which the SAE manages the subscriber	SAE reference
Subscriber's IP address for situations in which the SAE manages the interface that the subscriber uses, but not the subscriber	SAE reference
Subscriber's login name	SAE reference
Subscriber's primary username	SAE reference

The NIC comprises a set of software components that work together to collect, process, and provide data.

Repository for Data

The Juniper Networks database on a C-series platform or a directory configured for use with the SRC software running on s Solaris platform contains most SRC configuration data, including license information, service definitions, policies, and SAE configurations, as well as user profile data. You use user profiles to categorize groups of users, allowing you to keep your user data separate in your own directory.

We provide sample data LDAP Data Interchange Format (LDIF) to demonstrate how to provision the directory for different application scenarios. You can use the sample data as a starting place when developing or configuring specified applications of the SRC software. The SRC documentation provides references to the sample data to show sample implementations.

Many SRC components, such as the SAE and the policy engine are designed to run nonstop. These components get most of their configuration and provisioning data from the directory. If the data in the directory changes, it is not necessary to manually reload the data into affected components. The SRC directory client running in each of these components detects changes that affect the component, and the appropriate updates are made.

The directory client is configured with a list of directory servers to use: one primary and any number of backups. If connectivity to the primary directory is lost, the directory client switches to an available backup directory server. If connectivity to the primary directory is restored, the directory client detects the connection and switches back to the primary directory. This capability makes it possible to fine tune SRC deployments for added levels of availability and performance.

Juniper Networks Database as a Data Repository on C-series Platforms

The Juniper Networks database is a robust data repository that keeps your data highly available. It supports data distribution to other Juniper Networks databases and redundancy between Juniper Networks databases. Client applications control which database they connect to as their primary database and as their backup database. You can configure particular SRC components, such as SAE, NIC, and SAE to use a specified database to provide load sharing.

The Juniper Networks database also can also be run standalone to use in demonstrations or for testing purposes.

Directory as Repository for SRC Data

For the SRC software running on a Solaris platform to work with a third-party directory, all the information must be provisioned in the directory. We provide tools, such as SRC CLI, SDX Admin, and Policy Editor, to help provision the information into the directory. An external OSS can also provision all or part of the information directly through the LDAP interface.

LDAP Version 3

The SRC software on Solaris platforms employs LDAP version 3 to interact with third-party directories. The SRC software is compatible with any LDAP version 3–compliant directory, but some integration work might be necessary, such as for the following requirements:

- Schema extension—This mandatory requirement must be completed as outlined in *Integrating Directories* in the *SRC Integration Guide: Network Devices, Directories, and RADIUS Servers*.
- Access control—This is an important function for wholesale/retail applications and for enterprise scenarios.
- Virtual list view control—Requirements are described in LDAP Extensions for Scrolling View Browsing of Search Results—draft-ietf-ldapext-ldapv3-vlv-09.txt (June 2003 expiration). This requirement is important when you run the eventing system.

Prepackaged Integration

For SRC software installed on Solaris platforms, we provide prepackaged integration for:

- DirX directory server—Optional add-on package offered with the SRC software. This directory is based on the Siemens DirX Solutions product.
- eTrust Directory—Optional add-on package offered with the SRC software. The directory server is a product of Computer Associates International, Inc.
- Oracle Internet Directory—Optional add-on package offered with the SRC software. This directory is a software component in the Oracle Application Server 10g.
- Sun ONE Directory Server—Sun Microsystems product included with Solaris 9. The SRC software's Sun ONE Directory Server add-on package also contains the UMC schema for Sun ONE Directory Server.

Third-Party Directory Servers

For information about the directory servers that you can integrate with the SRC software running on a Solaris platform, see the *SRC-PE Release Notes*. The SRC software is designed to work with directory servers that are robust, scalable, and suitable for the carrier market.

Configuration Tools

This section describes the SRC configuration tools:

- SRC CLI—C-series platform and SRC software on a Solaris platform
- Local Configuration Tools—Solaris platform only
- Policy Editor and Management—Solaris platform only

- SDX Admin—Solaris platform only
- SDX Configuration Editor—Solaris platform only

SRC CLI

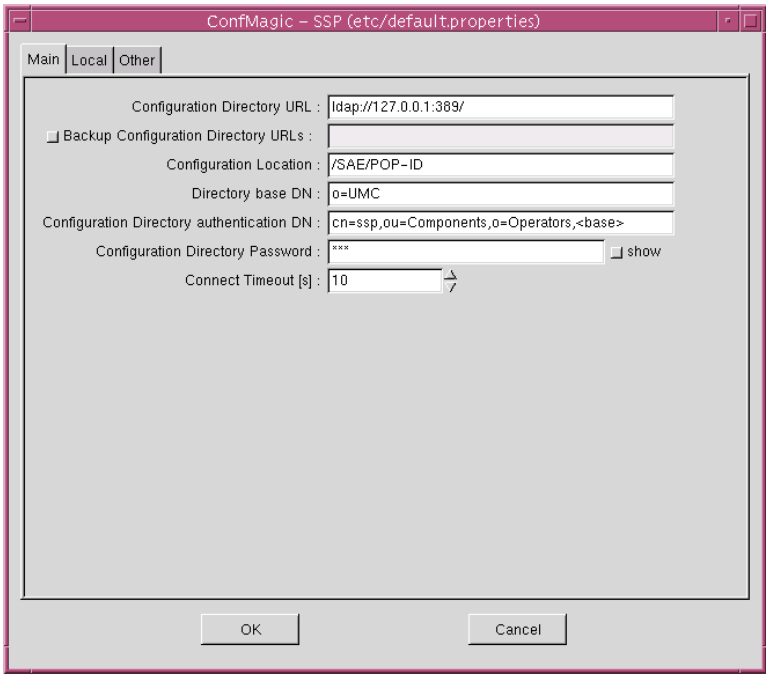
The SRC CLI is the software interface you use to configure a C-series platform. You can also use the CLI to configure supported components for SRC software installed on Solaris platforms.

Local Configuration Tools

The local configuration tool allows administrators to configure local files on the hosts that support SRC components such as the SAE and NIC. For some SRC components, the local configuration tool also reads data from and writes information to the directory.

Figure 3 shows an example of the configuration tool.

Figure 3: Sample Configuration Tool Window



Policy Editor and Management

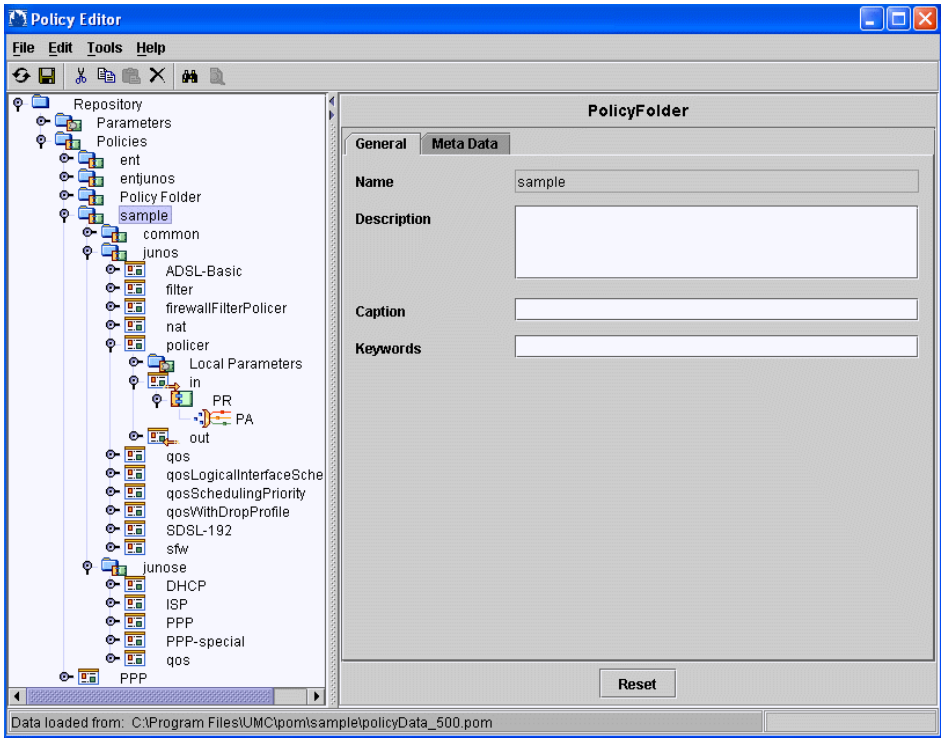
The SRC software works with Juniper Networks routers and PacketCable Multimedia Specification (PCMM) compliant CMTS platforms to provide differentiated QoS. The SRC software uses policies to define how the router or the CMTS device treats subscriber traffic. Policy management is responsible for defining policies and deploying the policies in an SRC network.

On JUNOS routing platforms, the SRC software supports class-of-service (CoS), firewall filters, policing, stateful firewall, stateless firewall, and network address translation (NAT) services.

On JUNOSe routers, the SRC software supports policy routing, rate limiting, QoS classification and marking, packet forwarding, and packet filtering.

The Policy Editor application allows easy specification and validation of policies. Policy Editor stores policies in a central repository, or directory. It works closely with a policy engine, which performs dynamic policy decisions while activating services, leveraging on the directory content to decide which policies to use in a given context. Figure 4 provides an example of Policy Editor.

Figure 4: Sample Policy Editor Window



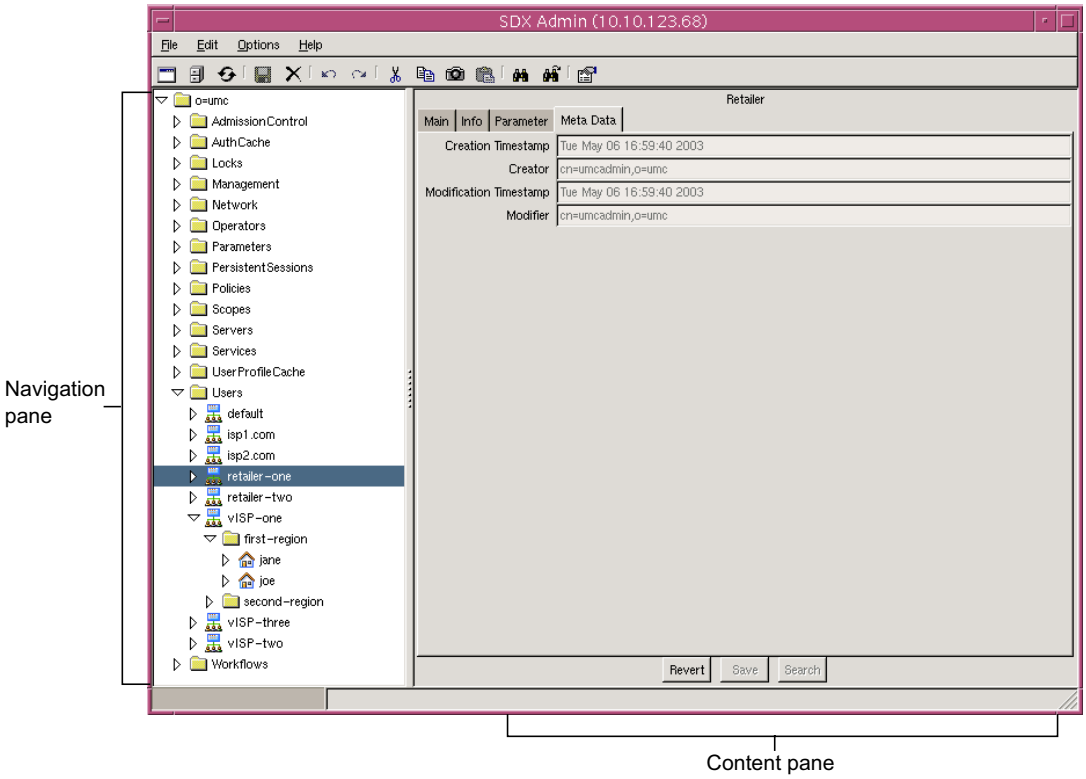
SDX Admin

SDX Admin allows service providers to add, modify, and delete services, network definitions, and advanced configurations within the SRC software. For small installations and demonstrations, you can use SDX Admin to create and modify retailers, subscribers, and subscriptions to services.

Figure 5 shows the two panes that make up the SDX Admin interface:

- Navigation pane—Displays objects in a hierarchical tree. This pane is used to select and navigate through objects or the directory.
- Content pane—Displays details of objects that appear in the navigation pane. This pane is used to display and modify information about objects.

Figure 5: SDX Admin Panes



From SDX Admin, for example, you can create and define a new service, define a grouping of virtual routers, or define a new retailer.

Also, using SDX Admin, administrators can set the language for SRC interfaces so that information can be displayed in the language of choice. The language environment is set globally on the host that is running the SDX Admin software.

SDX Configuration Editor

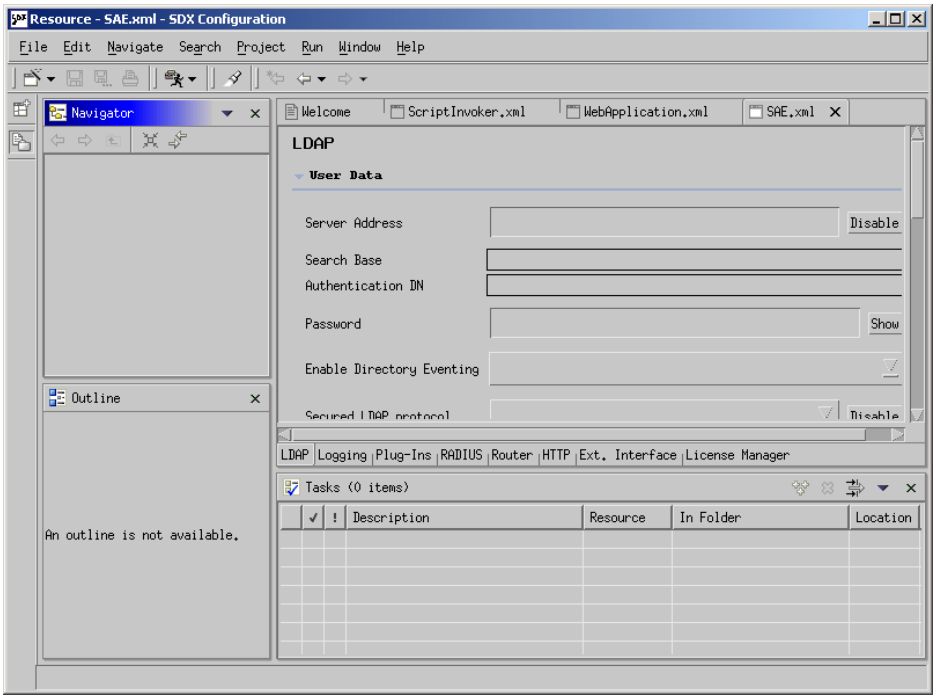
SDX Configuration Editor is an XML-based GUI that administrators can use to configure SRC components that store data in the directory. You can configure SRC components such as the SAE, NIC properties for portals and applications, LDAP connection properties, logging, router access, plug-ins, RADIUS accounting and authentication, Hypertext Transfer Protocol (HTTP) access, the Enterprise Manager Portal, and the license manager.

SDX Configuration Editor is a plug-in to the Eclipse platform and presents Extensible Markup Language (XML) property files as forms in which you edit configuration elements.For information about Eclipse, see

http://www.eclipse.org

Figure 6 shows a sample window for SDX Configuration Editor. The LDAP tab for the *SAE.xml* file is selected to allow configuration of LDAP properties for the SAE.

Figure 6: Sample Window for SDX Configuration Editor



SRC Management Tools

This section describes the SRC management tools.

C-Web Interface

The C-Web interface is an application that allows you to monitor a C-series platform and SRC software on a Solaris platform by means of a Web browser through Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS). The C-Web interface uses the same operational model as the J-Web interface you use to configure and monitor JUNOS routing platforms.

The C-Web interface provides monitoring for SRC-ACP, JPS, NIC, Network Time Protocol (NTP) and system time, redirect server, SAE, security, and system-level components on a C-series platform. Figure 7 shows the SRC Services page as an example C-Web page.

Figure 7: C-Web Page for SAE Services

Prepaid Account Administration Application

You can use the Prepaid Account Administration application to manage prepaid accounts. From Prepaid Account Administration, you can:

- View or update information about current accounts
- Create new accounts
- Clear expired accounts

The SRC application library includes Prepaid Account Administration application.

SDX SNMP Agent

The SDX SNMP agent monitors system performance and availability, system resources, and SRC processes that are running on the system. The agent obtains information from traps through SNMP. The SNMP agent is preconfigured to monitor SRC processes, such as those associated with infrastructure components (DirX for SRC software on Solaris platforms, and Interlink RADIUS). Additionally, it provides detailed monitoring and configuration of SRC server components such as the residential and enterprise portals, the SAE, NIC hosts, the policy engine, and the Workflow application.

The master agent determines the SNMP version that supports integration with other network management systems. The SRC SNMP agent runs as a subagent to an installed master agent using the Agent Extensibility (AgentX) protocol. The SRC SNMP agent cannot act as a master agent.

Traffic Mirroring Administration Application

You can use the Traffic Mirroring Administration application to manage the mirroring of subscriber traffic. When traffic-mirroring services are activated in an SRC-managed environment, you can:

- Specify the subscriber whose traffic is be mirrored and the IP addresses of the traffic to be mirrored
- Manage currently active mirroring tasks
- Manage pending actions

The SRC application library includes the Traffic Mirroring Administration application.

Service Management Applications

This section describes service management applications in the SRC software and SRC application library.

SRC SOAP Gateway

The SRC SOAP Gateway (SRC-SG) allows a gateway client—an application that is not part of the SRC network—to interact with SRC components through a SOAP interface. This feature is useful for business-to-business situations, such as a wholesaler-retailer environment. Typically, the wholesaler owns and administers the SRC components, and the retailer maintains a database of subscribers. Retailers purchase services from one or more wholesalers and sell the services to their subscribers. Using information provided by the wholesaler, the retailer creates a gateway client to communicate with the components in the SRC software.

The SRC-SG offers the following Web applications:

- Dynamic Service Activator allows a gateway client to dynamically activate and deactivate SRC services for subscribers and to run scripts that manage the SAE.
- Subscriber Manager allows a gateway client to create and modify subscriber data and to manipulate the Workflow application.

Deep Packet Inspection Integration Application

The SRC software has been integrated with the Ellacoya Networks Deep Packet Inspection (DPI) platform to provide a traffic management solution that combines the advanced traffic identification and reporting features of the Ellacoya DPI with the SRC software's intelligent service policy enforcement. With this solution, providers can identify, monitor, and control traffic on a per-application or per-subscriber basis.

Application traffic such as peer-to-peer file sharing or instant messaging, which in many cases originates or terminates outside of a provider's network, can cause abusive or indiscriminate consumption of bandwidth and impact a provider's ability to deliver its own services. In particular, services that require higher, guaranteed levels of performance, such as Voice-over-IP (VoIP) or video-on-demand (VoD), can be impacted. Having visibility into applications that are transported over the network and their associated bandwidth consumption at various times is important as is the ability to control those applications.

The DPI solution allows providers to implement service control policies on specific traffic flows quickly and effectively. Such policies include throttling back, capping volume, or even enhancing bandwidth or service quality for sanctioned peer-to-peer applications.

Benefits of the DPI Integration

By identifying and effectively controlling traffic at the application level, service providers can:

- Put usage controls on applications on a subscriber basis. For example, you can put a quota limit on the amount of peer-to-peer traffic that a subscriber can consume in a month.

  Once subscribers have used their quota, you can apply a policy that throttles back on or blocks a subscriber's peer-to-peer traffic, bill the subscriber for additional usage, or allow the subscriber to purchase additional quota.
- Limit the total percentage of network resources that a specific type of traffic is allowed to consume.
- Provide higher or guaranteed levels of performance for premium services by applying QoS control to application sessions. For example, two subscribers start an Xbox Live session. The Ellacoya DPI platform detects activity for this application, and sends application usage counters to the SRC software. The SRC software pushes policies that deliver a specific level of QoS for this application session to a router or other network device.
- Charge subscribers based on their usage of premium content-based services.

- Offer and charge for tiered Internet services based on both speed and application.
- Better support network planning functions by gaining an in depth understanding of traffic flows and patterns on a per subscriber and per application basis.

Enterprise Audit Plug-In

The Enterprise Service Portal audit plug-in, also referred to as the enterprise service portal IT Manager Audit Plug-In, defines a callback interface, which receives events when IT managers complete specified operations, such as subscribing to a service or changing the parameter substitutions of a subscription. The events report the type of operation, the identity of the IT manager, and other attributes.

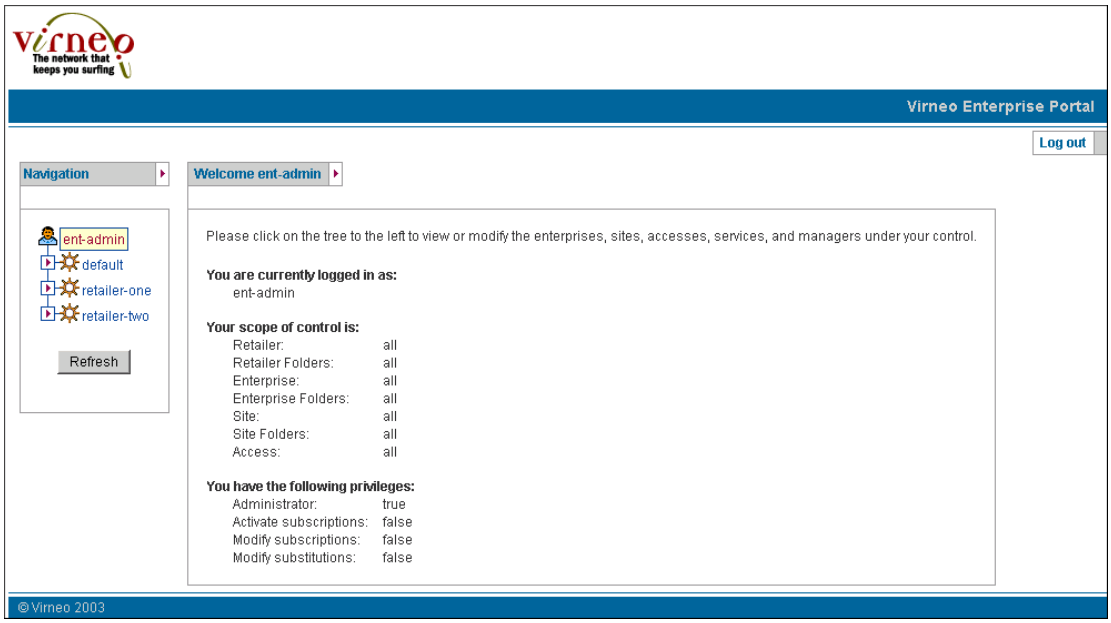
You can write audit plug-in event listeners by implementing the callback interface. A listener performs tasks such as processing received events and then publishing the events to one or more event handlers, such as a log file, system log, or database. Events are sent after the corresponding operations have been completed.

Enterprise Manager Portal

Enterprise Manager Portal is an application that allows service providers to provision services for enterprise subscribers on JUNOSe routers and JUNOS routing platforms and that allows IT managers to manage services. This Enterprise manager Portal is a complete application that requires little customization.

Figure 8 shows a sample page in the Enterprise Manager Portal.

Figure 8: Sample Page in Enterprise Manager Portal



You can use the Enterprise Manager Portal with the NAT Address Management Portal to allow service providers to manage public IP addresses for use with NAT services on JUNOS routing platforms and to allow IT managers to make requests about public IP addresses through the Enterprise Manager Portal. The NAT Address Management Portal is a complete application that requires little customization.

IDP Integration Applications

The IDP integration applications allow you to use IDP to monitor subscriber traffic for detecting malicious network traffic sent to or received by subscribers. In addition to the actions that IDP can take in response to detected incidents, you can configure the SRC software to respond to these incidents by taking one or more of the following actions for subscribers associated with malicious traffic:

- Applying policies, such as policies that limit subscriber bandwidth, to subscriber interfaces
- Sending e-mail messages that describe the nature of an incident
- Redirecting Web requests to an IDP captive portal where a page provides the source or destination of the problem traffic and a description of the incident

The SRC application library provides robust sample data for IDP integration, a sample e-mail gateway application, and a sample IDP captive portal. You can customize the implementation provided, or create a new one based on the samples.

IVE Host Checker Integration Application

The IVE Host Checker integration application allows you to verify that the subscriber systems used to connect to a service provider comply with the service provider's policies. You can deploy IVE Host Checker in a network so that it is activated according to the service provider's requirements. Based on the host-checking results, the subscriber may be allowed full, limited, or no access to the Internet.

The SRC application library provides sample data for IVE Host Checker integration, a sample Host Check Result portal, and a sample SRC-VTA application for scheduling host checking. You can customize the implementation provided, or create a new one based on the samples.

Prepaid Service Application

The prepaid service application is a demonstration application that illustrates how to integrate prepaid service applications with the SRC software.

The demonstration application consists of two components:

- Prepaid account server—Provides the central data repository for the prepaid services demonstration application. It maintains the different accounts and provides access for the other SRC components.
- Prepaid Account Administration application—Allows you to manage prepaid accounts.

The demonstration supports two types of prepaid service applications, time based and volume based.

Sample Enterprise Service Portal

An enterprise service portal is a Web application that lets service providers supply a management interface to its customers for managing and provisioning services. The sample enterprise service portal provides is an application that illustrates how service providers can make their services available to IT managers in an enterprise and that provides developers with a starting point from which they can create their own enterprise service portals.

Sample IPTV Application

The IPTV application is a sample application that demonstrates how to use extended features of SRC-ACP and the SAE to manage network resources. You can use SRC-ACP to perform call admission control, allocate bandwidth, and initialize and execute applications. You can use the SAE to set up and manage LSP tunnels with router drivers and script service.

Sample Residential Service Selection Portals

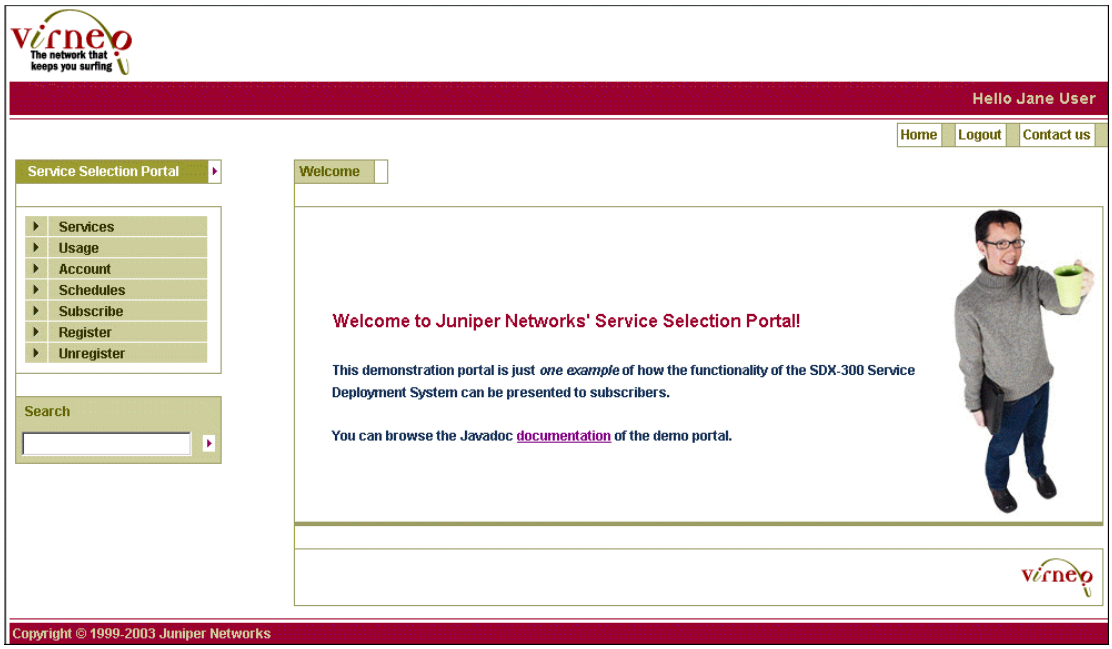
A residential portal is a Web portal application designed for use by individual subscribers to manage their subscriptions to Internet services and to log in to and out of a subscriber session. The portal pages, which are dynamically generated from information stored for subscribers, give subscribers instant access to personalized services, without the need to interact with customer representatives for a service provider. Proprietary client software is not required; subscribers can use a standard Web browser on a workstation or a personal digital assistant (PDA).

A residential portal can locate a specific SAE by using information that is dynamically obtained when subscribers connect. Because the data-processing function of the SRC software is separate from the access function, you can easily integrate the SRC software with existing portals, regardless of the technology used to deliver the portal. If your portal environment provides schemes for checking availability of Web servers and balancing loads between Web servers, you can also take advantage of these schemes for the portal.

The SRC software provides examples of residential portals.

Figure 9 shows a residential Web portal that could be created with the SRC software.

Figure 9: Sample Residential Web Portal



Web-based residential portals that you develop for the SRC software are compatible with PDAs. Figure 10 shows a login page for a sample residential portal that is being accessed from a PDA.

Figure 10: Sample Login Page for a Residential Portal on a PDA

Threat Mitigation Portal

The Threat Mitigation Portal (SRC-TMP) and application allows service providers to respond to threats on the SRC-managed network. The application for the SRC-TMP can be customized based on customer-supplied data to control the description and recommended actions for each type of threat. The application includes the ability to log all user operations to provide an audit trail of actions.

The application uses these components to respond to threats:

- Juniper Networks Intrusion Detection and Prevention (IDP) Sensors to detect the threats.
- Juniper Networks NetScreen-Security Manager to manage the IDP Sensors and to signal the SRC-TMP when a threat is detected.
- The SRC-TMP, which is the user interface for the application, to manage threats and act upon them.

Traffic-Mirroring Application

The traffic-mirroring application allows service providers to mirror subscriber traffic on any subscriber access platform supported by the SRC software. By activating traffic-mirroring services in an SRC-managed environment, service providers can set up SRC policies to:

- Monitor subscriber traffic and intercept traffic from a particular source or to a particular destination.
- Take actions for subscribers with intercepted traffic by applying policies to the subscriber traffic.

The sample data provided with the application illustrates configurations for a network that contains JUNOSe routers and JUNOS routing platforms and includes policies, services, and router definitions.

Workflow Application

The Workflow application allows a service provider to automate the provisioning process for primary access services. Typically, primary access services consist of broadband access, such as DSL or cable, Internet connectivity with a default profile, and possibly some application services, such as e-mail. Once the primary access service is set up, the subscriber can use the dynamic service selection mechanism for SAE services.

As shown in Figure 11, the Workflow application uses APIs, protocols, scripts, and external programs to communicate with the various components of the SRC software.

Figure 11: Workflow APIs, Protocols, and Scripts

Java

The Java API consists of beans developed by the service provider to describe a desired workflow (for example, sending an e-mail to a technician or mail robot provisioning systems). The beans drive the Workflow application. We provide sample beans as well as template beans that help the service provider design workflow beans.

LDAP

The Workflow application can perform LDAP operations (for example, add, delete, search, and modify entries) to an external LDAP server.

Scripts and External Programs

The Workflow application can be designed to run a script or external program that can perform provisioning functions; for example:

- Execute a sequence of configuration commands or SNMP requests on a network element.
- Request an update in a subscriber database.
- Create an e-mail account.
- Allocate file space on a Web server and configure FTP access for the subscriber.

E-Mail Send/Receive Protocols

The following e-mail send and receive protocols are used in the Workflow application:

- Simple Mail Transfer Protocol (SMTP)—Used by an e-mail bean to send an e-mail to an external entity (for example, a provisioning system)
- Post Office Protocol version 3 (POP3)—Used by the Workflow application to receive e-mail responses to e-mail requests sent previously
- Internet Message Access Protocol (IMAP)—An alternative to the SMTP and POP3 protocols

HTTP

The Workflow application also uses HTTP to send and receive messages to and from external provisioning systems. These messages are usually encoded in XML.

XML

The object state manager (OSM) receives messages from the service provider's provisioning system that are encoded in XML. These messages are requests for the OSM to change the state of subscribers and subscriptions according to service provider–defined object life cycle state machines. For instance, a subscription may have several states, such as created, provisioned, and inactive. The state machine defines the valid transitions from state to state and, optionally, a workflow to carry out the provisioning steps to effect the transition between the states.

The workflows themselves can send XML requests and receive XML responses to and from the service provider's provisioning systems to carry out some of the steps in the workflow.

SRC Programming Interfaces

You can use the APIs provided with the SAE to extend SRC capabilities. The SAE provides the following APIs:

- CORBA plug-in SPI
- CORBA remote API
- NIC access API
- SAE core API
- Script Services

Other components within the SRC software may provide programming interfaces. These interfaces are described in the documentation for the associated component.

The SRC software also includes plug-ins, such as plug-ins for accounting and authentication, admission control, customized accounting and authentication, and prepaid access.

CORBA Plug-In SPI

The CORBA-plug-in SPI is an interface that allows you to implement external plug-ins to integrate SAE with OSS software written in a wide variety of languages and distributed across a variety of hardware and operating system platforms. The SPI lets you link the rest of a service provider's OSS with the SRC software so that the OSS is notified of events in the life cycle of SAE sessions. For example, plug-ins can notify the OSS when a subscriber attempts to log in, and the OSS can evaluate general data and resource allocation to make authorization decisions.

CORBA Remote API

The CORBA remote API provides remote access to the SAE. It comprises an interface module manager and the following interface modules:

- SAE access interface module—Provides remote access to the SAE core API
- Java script interface module—Allows you to control the SAE with a Java script
- Python script interface module—Allows you to control the SAE with a Python script
- Event notification interface module—Allows you to integrate the SAE with external IP address managers

Most functions that are available through the SAE core API are also available through the CORBA remote API.

NIC Access API

The NIC access interface module (*nicAccess.idl*) is a simplified CORBA interface used to perform NIC resolutions. Use the NIC access module to develop applications not written in Java.

SAE Core API

The SAE core API is used to control the behavior of the SRC software, including subscribers, services, and subscriptions, as well as the SAE itself. For example, it can be used to provide subscriber credentials information (username and password) or to request subscription activation or deactivation for a subscriber.

Script Services

Script services are SAE services that provide an interface to call scripts that supply custom services. You can use script services to create custom service implementations, such as:

- Provisioning of layer 2 devices, such as digital subscriber line access multiplexers (DSLAMs).
- Setting up of network connections such as MPLS tunnels.
- Provisioning of policies for network devices that do not have a supported SAE router driver.

You can use script services to provision policies on a number of systems across a network, including networks that do not contain a JUNOSe router or JUNOS routing platform.

Authentication and Accounting Applications

This section describes components that help to provide accounting or authentication.

AAA RADIUS Servers

RADIUS enables remote access servers to communicate with a central server to authenticate subscribers and authorize their access to the requested system or service. RADIUS allows a company to maintain subscriber profiles in a central database that all remote servers can share. With a central service, it is easier to track usage for billing and to keep network statistics. The router provides RADIUS accounting and authentication, while the SAE provides SAE accounting and authentication.

We provide the Merit RADIUS application as a convenience to get started. We recommend that service providers move to a more sophisticated RADIUS server, such as the Interlink RAD-Series RADIUS or the Juniper Networks Steel-Belted Radius/SPE server, or integrate the SRC software with some other currently used RADIUS server. The SRC software works with other AAA RADIUS systems; however, we test and support system integration only with Merit, RAD-Series RADIUS Server, and Steel-Belted Radius/SPE server software.

You can use any RADIUS server for authentication and accounting that is compliant with these standards:

- RFC 2882—Network Access Servers Requirements: Extended RADIUS Practices (July 2000)
- RFC 2869—RADIUS Extensions (June 2000)
- RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000)

When a provider uses the SDX schema to integrate the RADIUS server with the directory, the SRC software provides the highest level of subscriber control. For example, when subscriber information is stored in the directory, the SRC software can provide a list of services for each individual subscriber.

The less integration the RADIUS server has with the directory, the less control the SRC software provides for individual subscribers. For example, subscribers may have to be grouped based on criteria such as domain name, router, or interface.

The SRC software can work without a RADIUS server. The SRC software can use either LDAP authentication and flat-file accounting, or it can rely on plug-ins to perform authentication and accounting.

SRC Admission Control Plug-In

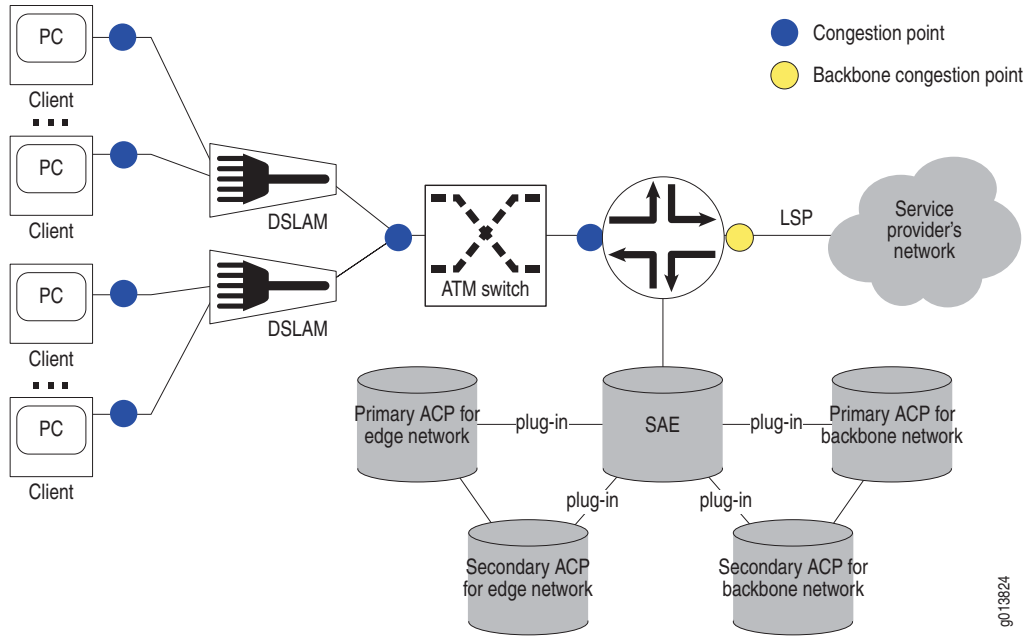
SRC-ACP authorizes and tracks subscribers' use of the network resources that are associated with services that the SRC software manages. SRC-ACP operates in two separate regions of the SRC network: the *edge* network and the *backbone* network. The edge network is the layer 2 access network through which subscribers connect to a router configured as a Broadband Remote Access Server (B-RAS). The backbone network is the region between the router and the service provider's network.

Congestion often occurs in the network at points where connections are aggregated. SRC-ACP monitors congestion points at interfaces between devices in the edge network. In the backbone network, SRC-ACP monitors one congestion point, a point-to-point label-switched path (LSP), between the router and the service provider's network.

Typically, network administrators use their own network management applications and external applications to provide data for SRC-ACP. SRC-ACP first obtains updates from external applications through its remote CORBA interface and then obtains updates from the directory through LDAP. SRC-ACP does not interact directly with the network to assess the capacity of a congestion point or actual use of network resources.

Figure 12 shows a typical network topology.

Figure 12: Position of SRC-ACP in the Network



Flat-File Accounting

The SAE can write tracking data to accounting flat files. External systems can then collect the accounting log files and feed them to a rating and billing system. When the SAE writes data to a flat file, it writes into the first line the headers that identify the attributes in the file. Subsequent lines list the actual data in each field.

SRC Volume Tracking Application

The SRC Volume Tracking Application (SRC-VTA) allows service providers to track and control the network usage of subscribers and services. You can control volume and time usage on a per subscriber or per service basis. This level of control means that service providers can offer tiered services that use volume as a metric, while also controlling abusive subscribers and applications.

When a subscriber or service exceeds bandwidth limits (or quotas), the SRC-VTA can take actions including directing the subscriber to a portal to activate additional services or purchase additional bandwidth, imposing rate limits on traffic, sending an e-mail notification, or charging extra for additional bandwidth consumed.

If you use the SRC-VTA with the SRC deep packet inspection (DPI) feature, you can control the volume of traffic for specific applications, such as peer-to-peer file sharing.

You can use the VTA Configuration Manager to configure the SRC-VTA, including event handlers, events, actions, and processors. You can also use it to configure identifiers for subscribers and sessions and to set up logging for the SRC-VTA. VTA Configuration Manager lets you store your configurations in local files or in a directory.

Managing Subscriber Accounts with Web Portals

We provide two sample portals that manage subscriber accounts. One is an administrator portal that administrators can use to manage SRC-VTA subscriber accounts. The second is a subscriber portal that subscribers can use to manage their own accounts. Before you can use these portal, you need to configure the Web applications for the SRC-VTA.

The suggested billing model for services managed by VTAs is one in which subscribers pay for services when they select them through a Web portal.

Accessory Components

This section describes SRC components that are used with other SRC components to create a solution.

Monitoring Agent Application

The Monitoring Agent application integrates IP address managers into an SRC-managed PCMM environment and provides event notification for the SAE from subscribers who log into CMTS devices.

You can use the Monitoring Agent application to allow IP address managers, such as a DHCP server or a RADIUS server, to notify the SAE about subscriber events. You can use the SRC software to notify the SAE when:

- A subscriber logs in
- An address assignment is terminated

Redirect Server

The redirect server redirects HTTP requests received from IP Filter to a captive portal page. The redirect server examines requested paths and detects proxy HTTP requests. If the requested URL is served by the captive portal server, the redirect server opens a TCP connection to the captive portal and directs traffic to the captive portal rather than the requested URL.

Auxiliary Applications

This section describes applications that integrate with other SRC components or applications.

Application Server

To run a residential portal, the Enterprise Manager portal, or other enterprise portals you need an application server in your SRC environment you need an application server. Typically, you should use a J2EE application servers that includes a Web application server

The Web application server should support JavaServer Pages (JSP) technology. JSP pages are Web pages that contain Java code and JSP tags (similar to HTML tags) embedded in normal HTML. The Java code and JSP tags produce dynamic HTML content and invoke the SAE functionality.

For use on a Solaris platform, the SRC software provides the JBoss application server as a convenience to let you quickly set up an SRC environment. This application server is J2EE compliant and supports the J2EE applications that the SRC software offers.

We have tested the SRC software with other application servers. For a list of the application servers that we have tested with the SRC software, see the release notes.

IP FIlter

For SRC installations on a Solaris platform, IP Filter filters traffic as specified by Network Address Translation (NAT) rules and redirects incoming HTTP requests that meets criteria for the filter to the redirect server. The redirect server can then direct this traffic to a captive portal page.

Other Applications

Other companies have created applications for use with the SRC software. For information about applications created by Juniper partners, see

http://www.juniper.net/partners/content_partners.html