

SRC Authentication and Accounting Applications

The following components help to provide accounting or authentication:

- AAA RADIUS Servers on page 1
- SRC Admission Control Plug-In on page 1
- Flat-File Accounting on page 2
- SRC Volume Tracking Application on page 2

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 recommend that service providers use a RADIUS server such the Juniper Networks Steel-Belted Radius/SPE server or integrate the SRC software with another RADIUS server that is already in use. we test and support system integration only with 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

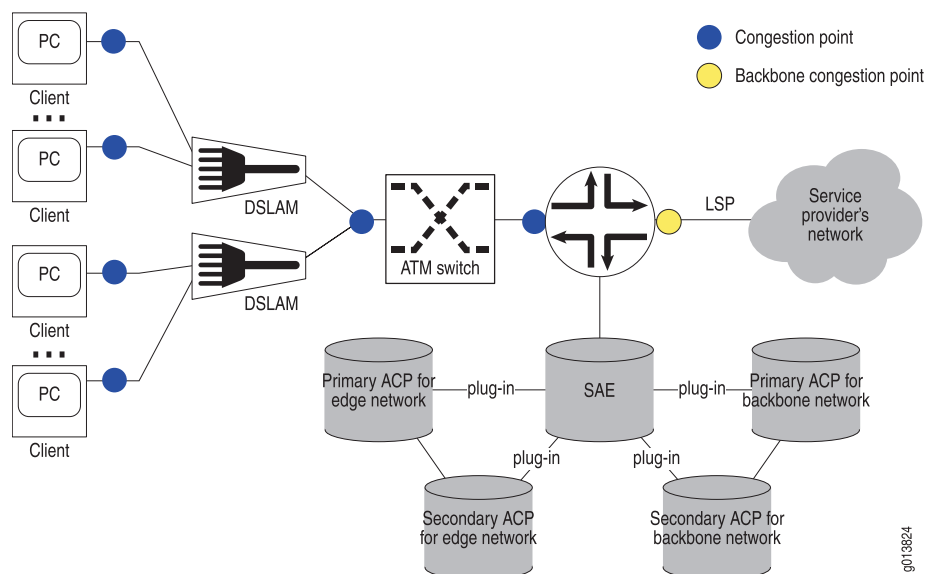
to a router configured as a Broadband Remote Access Server (B-RAS). The backbone network is the region between the router and the service provider's network.

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 1 on page 2 shows a typical network topology.

Figure 1: 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.

