Juniper Networks **Steel-Belted Radius Service Level Manager**

RADIUS/AAA Policy Server for Wholesale Carriers and ISPs

Built on Juniper Networks' market-leading Steel-Belted Radius (SBR) technology, the Steel-Belted Radius Service Level Manager extends Steel-Belted Radius/Service provider Edition (SPE) to provide additional AAA-driven policy controls to wholesale carriers and ISPs.

For ISPs, Service Level Manager lets you enforce concurrent login limits for all your remote users – across all Steel-Belted Radius/SPE servers and network access devices in place on your network.

For wholesale carriers, Service Level Manager ensures that you meet the Service Level Agreements you hold with your ISP customers by letting you track and enforce regional and global port usage – guaranteeing quality of service by controlling different levels of access to port groupings of any size on a per-customer basis.

Internet Service Provider

Every unauthorized connection to your network costs you money – both in terms of lost revenue and incurred bandwidth charges. With SBR SLM, you can block usage which exceeds service limits, detect account sharing, and identify stolen accounts.

Plus, SLM lets you offer popular "family" accounts to your customers – so you can enforce concurrent access for as many unique login IDs on a single shared account as required.

Enforce Concurrent Login Limits Across Your Entire Network

Service Level Manager tracks every user on the network for simultaneous multiple access and enforces every remote user's concurrent login limit as set up within Steel-Belted Radius/SPE.

Here's how the SBR SLM concurrency module works:

- When a subscriber attempts to access the Internet or Intranet through the ISP, the network access server which handles the connection forwards an authentication request to one of the front-end Steel-Belted Radius/SPE servers. Depending on preference, either the concurrency check or the validation of subscriber credentials may be performed first.
- If the concurrency check is first, Steel-Belted Radius/SPE forwards the authentication request along with the user's concurrent login limit to SBR SLM. SBR SLM, which tracks all active sessions, determines if the user is within their concurrent login limit and sends the result back to Steel-Belted Radius/SPE. If the user has not exceeded their limit, processing continues for the validation of credentials. If the user has reached their limit, they are denied access to the network at that time.
- If validation of user credentials is first, Steel-Belted Radius/SPE will either authenticate the user against a subscriber database on the local network or it will proxy forward the request to the appropriate downstream AAA system for authentication. The success/failure result of authentication will determine whether access to the network is denied or whether processing should proceed to the concurrency check phase.
- Once SBR SLM has determined the user is both authorized to connect and is within their concurrent login limit, Steel-Belted Radius/SPE grants the user access to the network.

Family or Group-Based Service Plans

With SBR SLM, you can sell shared "family" accounts of any shape or size. You can sell an account with any number of unique login IDs associated with it, and with a concurrent access limit of any value. This powerful capability gives you the flexibility you need to tailor your service offerings to meet your business requirements.

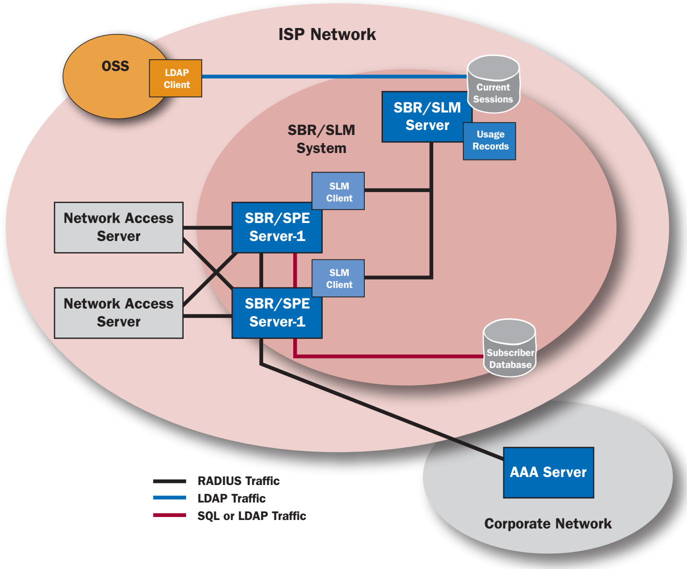
Because different pieces of information that may be needed to properly identify a subscriber or a group alias may reside in different locations across the network, or even off-network, SBR SLM supports the transfer of information across its authentication request path and its concurrency enforcement path to ensure that the necessary information is available to the system.

Management

SBR SLM also lets you:

- Programmatically access its current sessions list via LDAP, to easily determine, for example, if a particular user is connected, which users are connected to a particular network access server, or the IP address that is currently associated with a user's session.
- Elect to accept or reject all remote user connections if the Service Level Manager becomes unavailable.

SBR SLM automatically generates a concurrency log, a complete record of all RADIUS accounting transactions that you can elect to store as a flat file with rollover support or to insert into an SQL database in real time.



Wholesale Carriers

As a carrier, a growing portion of your business depends on complying with Service Level Agreements (SLAs) you've established with your ISP customers, requiring you to demonstrate service delivery at the specified levels and to provide full documentation of compliance.

Allocate Port Usage

For each service provider customer, SBR SLM tracks how many of its contracted ports are in use, and optionally enforces their port usage limit.

Here's how the SBR SLM port allocation module works:

- When a subscriber connects to a network access server, that device forwards an authentication request to Steel-Belted Radius/SPE.
- Depending on how you configure SBR SLM, either of the following sequences of events will occur:
- Steel-Belted Radius/SPE will authenticate the user, and then query SBR SLM to determine the status of the port usage limit; or
- Steel-Belted Radius/SPE will query SBR SLM to determine the status of the port usage limit and, depending on that result, will authenticate the user.
- In either case, once Steel-Belted Radius/SPE has learned that the subscriber is both authorized to connect and is within the port usage limit and enforcement policies set up for their service provider, it grants the subscriber access to the network.

SBR SLM lets you sell usage of a specified number of ports to your customers. Typically, you'll specify the following port usage values in the Service Level Agreements with your customers:

- Soft limit – the port usage you sell
- Hard limit – the port usage you enforce

You can even sell regional port limits. That is, for any customer, you can sell a fixed number of ports for one region of the country and a different number of ports for another region. You can vary these regional distinctions from customer to customer, and set each customer up in the manner that makes sense for them.

Finally, you can set up regions in whatever manner you choose: you can specify them according to geographical region, IP address of NAS equipment, even DNIS.

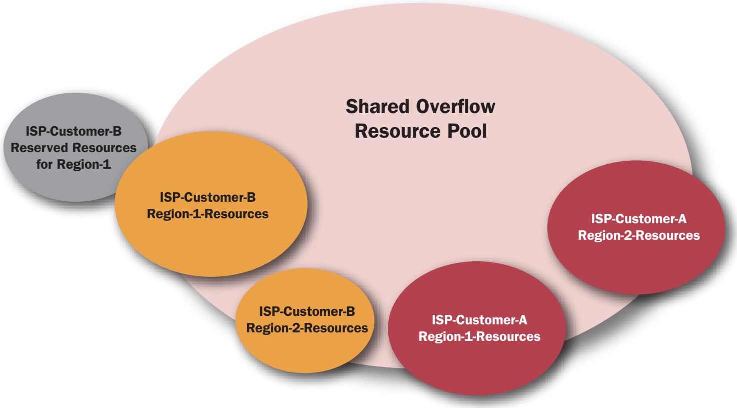
Enforcement, Overflow & Reservations

Enforcement of port limits is a key component of the port usage you sell.

The customer's soft limit is generally not enforced, but any overflow usage is recorded. This lets you maintain the quality of service that your customers require – particularly while their businesses grow – while you ensure that you understand, and can charge for, their actual level of port usage.

A customer's hard limit is always enforced: that is, any usage above the hard limit is rejected service. Hard limit enforcement lets you adhere to the Service Level Agreements you hold with all your customers; with hard limit enforcement, usage of one customer's extremely popular service will never block access by another customer's subscriber.

Overflow pools for port resources may be shared across ISP-customers and port reservations may be set up to guarantee that the required number of ports is always available for premium customers.


Shared Overflow Resource Pool
ISP-Customer-B Reserved Resources for Region-1
ISP-Customer-B Region-1-Resources
ISP-Customer-A Region-2-Resources
ISP-Customer-B Region-2-Resources
ISP-Customer-A Region-1-Resources

Time-of-Day Policies

As the overall network traffic load changes based on the time of day, port usage flows between peaks (which may mean overflow usage) and lower usage periods. SBR SLM allows you to offer rate plans based on the time of day. This provides more flexible options for your customer while making the best use of your network resources.

ISP-customer-A may have one set of soft/hard limits between 9am – 5pm and another between 5pm – 9am, while ISP-customer-B may have static limits since its regions span multiple time-zones.

Usage Reporting

SBR SLM reports on port usage on a customer-by-customer basis. Through its built-in LDAP Configuration Interface, you can view real-time usage information for any customer. You could, for example, see how many ports are currently being utilized by a particular customer.

In addition, SBR SLM logs port usage information which can then easily be imported into a report template. SBR SLM comes with pre-built report templates or you can easily customize your own templates.

With complete historical usage data – encompassing not only users who connect, but also all those who were rejected when all ports were full – you can 1) document, rather than estimate, the actual usage for each customer during any given time period, and 2) intelligently expand your network to meet additional customer demand.

Additional Management

As services and their management systems become more complex, the various reasons for denial of service do as well. Wholesalers (and ISPs) need a method to provide messaging information from the policy-enforcing server back through the chain.

SBR SLM supports the ability to populate Access-Reject messages with reason codes which indicate one of the various reasons that service was denied. There are five reason codes:

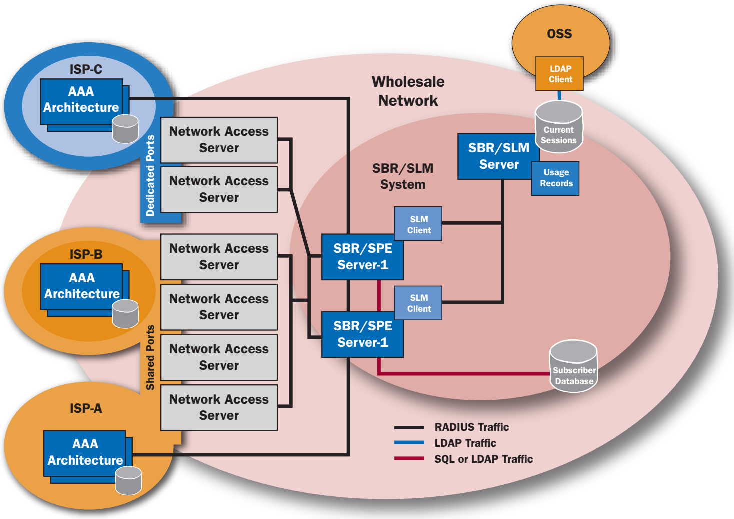
- SubscriberLimitViolation
- Error
- MappingFailure
- ResourceViolation
- SoftLimitBreach

Additionally, SoftLimitBreach can be present in Access-Accept response messages to clearly identify, for billing purposes, when the customer transitions into an overflow state.

SBR SLM reports SNMP v1 and v2c statistics to standard SNMP-based management consoles, and supports alarming (traps) for all reason codes as well as hard-limit violations and general connectivity to the SBR SLM server.

Performance

Whether deployed at an ISP, wholesale carrier, or at a service provider network that acts as both, SBR SLM's robust performance makes it capable of handling the busiest networks. By leveraging system resources for local and proxy request processing, SBR SLM will scale to meet the growth of your services.



Juniper NETWORKS®

CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737)
or 408-745-2000
Fax: 408-745-2100

www.juniper.net

EAST COAST OFFICE

Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL
SALES HEADQUARTERS

Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS

Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)-1372-385500
Fax: 44(0)-1372-385501