Subscriber Policy Broker Administration Guide, Release 6.40.01

05-00219-C02
2014-2-18

The most current version of this document is available on the Sandvine Customer Support web site at *https://support.sandvine.com*.

Sandvine is committed to ensuring the accuracy of our documentation and to continuous improvement. If you encounter errors or omissions in this user guide, or have comments, questions, or ideas, we welcome your feedback. Please send your comments to Sandvine via email at *https://support.sandvine.com*.

Contacting Sandvine

To view the latest Sandvine documentation or to contact Sandvine Customer Support, register for an account at *https://support.sandvine.com*.

For a list of Sandvine Sales and Support offices, see *http://www.sandvine.com/about_us/contact.asp*.

You can access the most current Sandvine documentation at https://support.sandvine.com/. The related guides and references are:

Document	Has information about	Part number
SPB CLI Reference Guide	CLI command syntax and command output.	05-00249
SPB Alarm Reference Guide	Alarms and their resolution.	05-00250
SRP 3000-D Series Installation Guide	How to physically install an SRP 3000-D element.	05-00028
PTS SandScript Configuration Guide	The SandScript language.	05-00217
SPB API Guide	The SPB application programming interface (API) components.	05-00036
spb-webservices	The API components. The document is included as part of the spb-webservices zip file available from Sandvine's Customer Support web site (https://support.sandvine.com/). The web services client samples are included as part of the spb-webservices zip file.	--
Network Demographics Server User Guide	Creating reports on the Network Demographics server.	05-00222

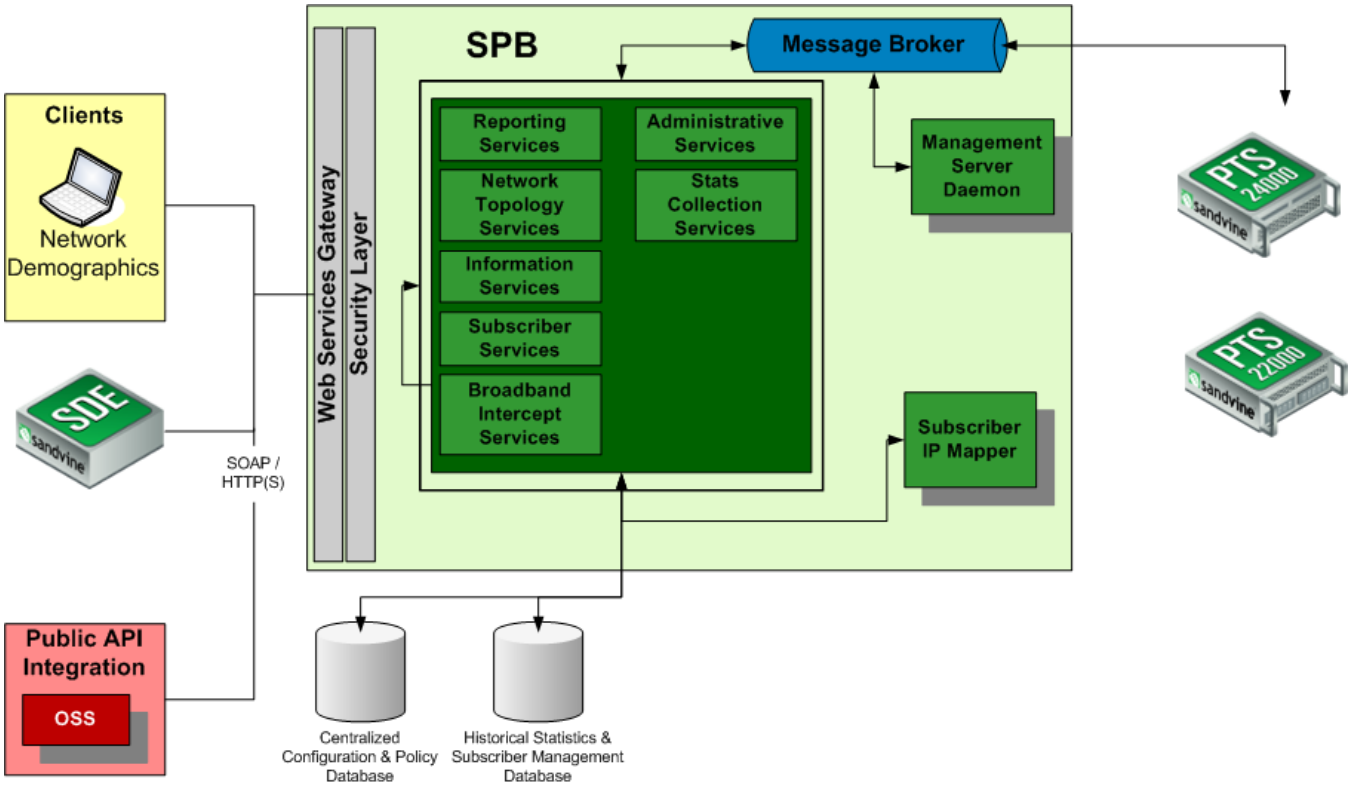
Contents

1

Overview

1.1 SPB System Overview

The Subscriber Policy Broker (SPB) is a central point of configuration for subscriber provisioning and SandScript policy configuration. The SPB provides services that enable communication and data access for Sandvine elements and third-party APIs.



The operational environment, which is the current live environment, manages the SPB. This environment contains data, active in the installation since the SPB was last deployed. The PTS or SPB performs all current activities such as statistics publishing, IP assignments, and subscriber management against this environment. The Network Demographic Server is used to view reports on the statistics gathered from the data in the operational environment.

The historical statistics and subscriber management database supports the operational environment. The environment holds live data concerning statistics and operational information about subscribers and network topology.

1.1.1 SPB Services

The SPB provides services that are a set of independent but interoperable operations performing business processes. The services available are:

- Statistics collection services manage the collection of statistical information that network elements observe.
- Reporting services provide access to historical statistical and subscriber operational information for the purpose of presentation and analysis.
- Subscriber services provide access to subscriber-related information enabling subscriber provisioning and SandScript policy configuration.

- Network topology services provide access to information concerning the physical aspects of the installation such as network elements and network structure.
- Information services provide access to manage general information about the installation such as VoIP providers and application protocols.

1.1.2 Session Qualifiers

A session qualifier represents a site number, port range, or any other identifier. It is used in combination with an IPv4 address to identify a unique subscriber session.

All Sandvine elements use the subscriber's IP address as the default session identifier. However, as IPv4 addresses become exhausted, Communications Service Providers (CSP) are implementing services, such as network address translation (NAT), that result in private overlapping IPv4 addresses on the network.

For networks that use such services, session qualifiers can uniquely identify subscribers that have overlapping IPv4 addresses, and thereby enable features such as subscriber mapping and subscriber lookup.

A site number is a positive 32-bit integer that you assign to an area of the network that sees only unique IP addresses. A site number is commonly derived from either a PTS cluster or a VLAN tag. The SDE's Subscriber Mapping application provides the site number to the SPB, through either SPB CLI commands or through Simple Object Access Protocol (SOAP) requests from other equipment.

The PTS uses the IP address and session qualifier together to uniquely identify sessions when applying SandScript policy.

1.1.2.1 Session Qualifiers Process

The process for session qualifiers in a Sandvine deployment differs depending on where the PTS is deployed: either the public side or the private side of a NAT device.

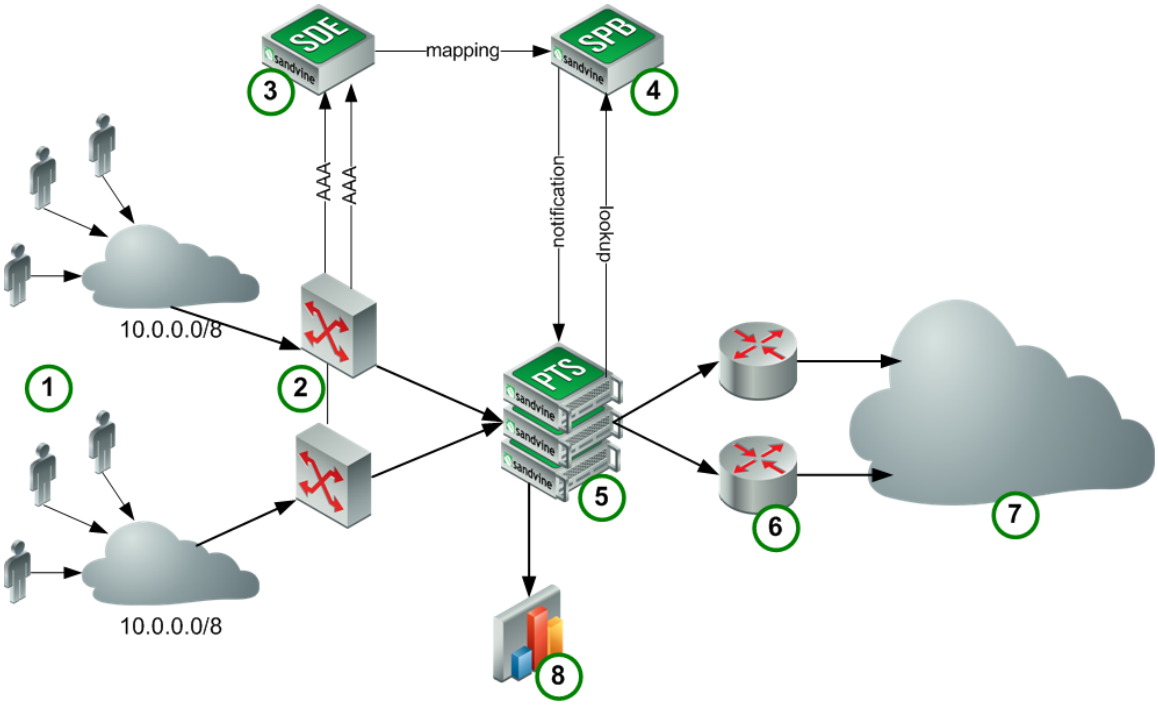


Figure: A PTS deployed on the private side of a NAT

A PTS deployed on the private side of a NAT can uniquely identify overlapping IP spaces by PTS cluster, VLAN-tagged packets, or bridge-group (PTS hardware ports that send traffic to each other are defined as a site). When the PTS is deployed on the private side of the NAT the process is:

1. Networks of subscribers are using the overlapping IPv4 space.
2. The subscriber traffic comes in via multiple access networks. The subscriber is mapped to an address using RADIUS, DHCP, or GTP-C at the time the subscriber joins the network. The different networks are on distinct VLANs when the traffic passes through the PTS.
3. The SDE receives the RADIUS, DHCP, or GTP-C message and processes it to determine the IP address, user name, and site.
4. The SDE passes on the IP address, user name, and site to the SPB, which stores the information in its database and forwards the information to the PTS.
5. The VLAN-tagged packets come into the PTS cluster. The PTS translates the VLAN tags into site numbers according to the configuration of the PTS. The PTS uses IP address and site number to uniquely identify subscribers, and then performs subscriber-aware SandScript. If the PTS does not know which subscriber the IP address and site number belong to, it looks up the information on the SPB.
6. One or more NAT routers translate the traffic to public IPv4 addresses.
7. The packets travel to their destinations in the internet.
8. Sandvine products identify subscribers in overlapping IP spaces.

When the PTS is deployed on the public side of a NAT device, it sees subscriber traffic after the NAT does its translation. Therefore the PTS sees a single IP used by multiple subscribers, with the only differentiator being the TCP or UDP port number of the flow. In this scenario, the PTS must rely on the subscriber mapping performed by the SDE and published by the SPB, so it can apply SandScript.

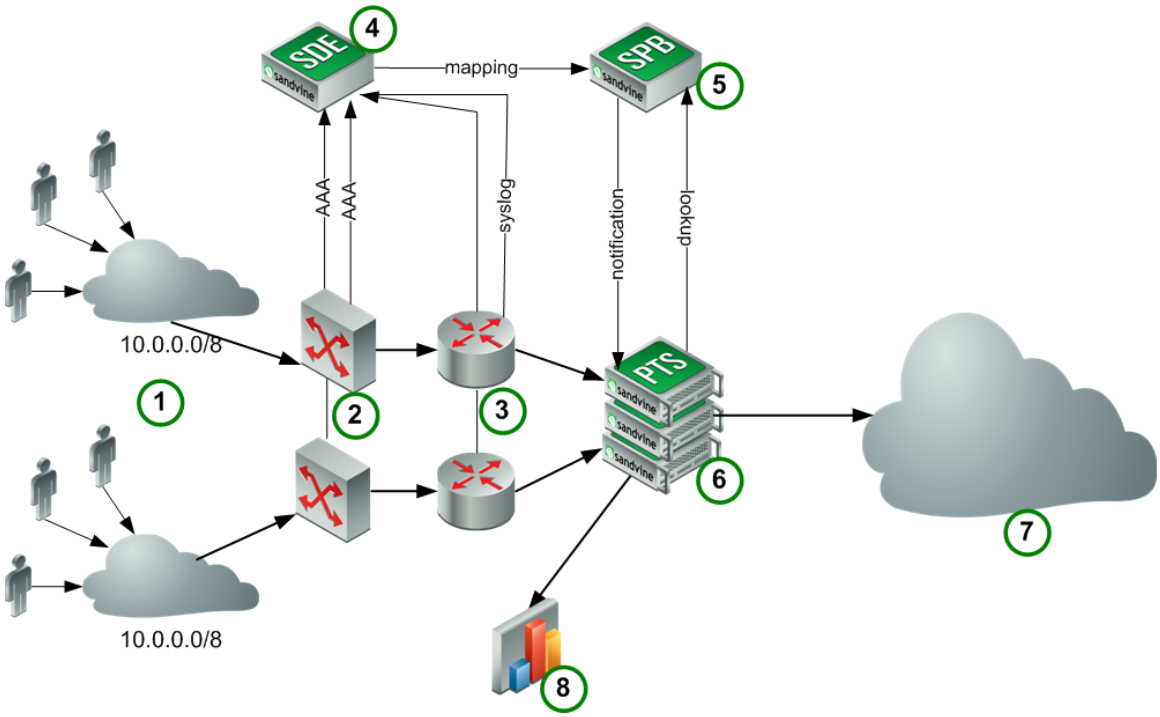


Figure: If the PTS is deployed on the public side of a NAT, it relies on the SDE to send NAT mappings to the SPB

When the PTS is deployed on the public side of the NAT the process is:

1. Networks of subscribers are using the overlapping IPv4 space.
2. The subscriber traffic comes in via multiple access networks. The subscriber is mapped to an address using RADIUS, DHCP, or GTP-C at the time the subscriber joins the network. The different networks are on distinct VLANs.
3. For each network, one or more NAT routers translate the traffic to public IPv4 addresses. The NAT server pushes a syslog message to the SDE for every port-block allocation or release action.
4. The SDE parses the syslog messages for NAT mapping information and passes on the private IP address, public IP address, and port block to the SPB.
5. The SPB stores the information in its database and forwards the information to the PTS.
6. The PTS uses the NAT mappings to discover the internal subscriber session and to classify traffic against the correct subscriber.
7. The packets travel to their destinations in the internet.
8. Sandvine products identify subscribers in overlapping IP spaces.

1.1.3 Subscriber IP Mapping

Subscriber awareness is achieved through a subscriber to IP address mapping.

The term subscriber refers to a unique subscriber identification (SID) value such as a network login ID or a cable modem's MAC address. The subscriber IP mapping ability is a pre-requisite for subscriber statistics collection, Top Talkers, and any per-subscriber aware SandScript policies.

The PTS maintains IP-subscriber mapping as long as a subscriber is active. The mapping times out when subscriber inactivity surpasses a configurable period of time.

Class-based subscriber SandScript policies require the mapping of subscribers to attribute classes. The session qualifier values, subscriber to IP address and subscriber to attribute mappings are maintained in the SPB. With the introduction of session qualifiers to tackle the overlapping IP address domains, you cannot use an IP address as a primary key. A session identifier sends a unique number to the PTS, which uses it to identify the IP assignment session, thereby correcting this problem. The scope of the SPB is to provide this unique number to the PTS. The session identifier is exposed anywhere an IpAssignment object is displayed or communicated.

There are multiple methods to achieve a subscriber-IP map. Refer to *Subscriber IP Mapping Configurations* on page 49 for more information.

1.1.4 Subscriber Attributes

Attributes are type-value pairs such as `servicelevel="gold"`. Each subscriber has a number of attributes used in SandScript conditions. The attributes typically represent the type of SandScript policies to apply and type of service the subscriber will receive (for example, collect statistics, shape traffic, allow/deny and so on).

1.1.5 Capability Exchange

The SPB and PTS (6.30 or higher) share version information and other capabilities, without the need to configure PTS manually. When connecting to a PTS running an older version, you still require manual configuration of the PTS.

To enable capability exchange, use the `set config service capability-exchange <enabled | heartbeat-interval>`.

To view the status of the capability-exchange, use the command `show config service capability-exchange <enabled | heartbeat-interval>`..

For more information, see the *SPB CLI Reference Guide*.

1.1.6 Network Demographics Server

The Network Demographics Server is a reporting tool that lets you view the data logged by all network elements in graphical or tabular reports. You can configure and customize the query in real time.

The reports provide data in meaningful terms such as the number of emails in the system, Voice over Internet Protocol (VoIP) minutes, Peer-to-Peer (P2P) file-sharing by protocol or user. Use these reports to identify subscriber usage patterns to gain a better understanding of subscriber reality.

You can view the reports in a browser and save, print, customize, or bookmark them for future reference, and distribute via email. The Network Demographics application provides a number of standardized reports for specific features such as Peer-to-Peer connections, Attack Traffic and Top Talkers. Advanced features are available to custom-build reports based on standardized reports and automatically schedule the generation and distribution of these reports via email.

1.2 SPB Clustering Overview

The SPB message broker and domain manager provide services to manage the operational and statistical data on the SPB.

A number of SPB message brokers and domain managers can be run in a clustered deployment in order to provide application level redundancy in the event of a failure. A clustered environment ensures longer periods of uninterrupted processing for clients of the SPB.

1.2.1 Message Broker

The message broker provides the communication mechanism between the PTS element and the SPB server.

The types of message brokers in Sandvine's messaging infrastructure are:

- The domain manager broker stores configuration and manages a cluster of message brokers
- An application messaging broker performs the bulk of the work of receiving and routing messages

In a single SPB cluster there is exactly one domain manager, but any number of application messaging brokers are allowed. Typically, whichever SPB in a cluster is configured as the domain manager also has the application messaging broker running as well.

The messaging infrastructure is scalable using additional SPB servers; each running an application messaging broker. The additional application messaging brokers register themselves with the domain manager and share the message load.

1.2.2 Application Server

An application server runs on each SPB server and provides services to process messages to and from PTS elements and manage operational and statistic data.

The application server also runs centralized processes for the SPB that support functionality such as Top Talkers and data summarization. In a cluster of SPB servers there is one application server on each SPB server with a single application server in the cluster elected to run the centralized processes. The election of a application server manager is done automatically.

1.3 SPB Hierarchy

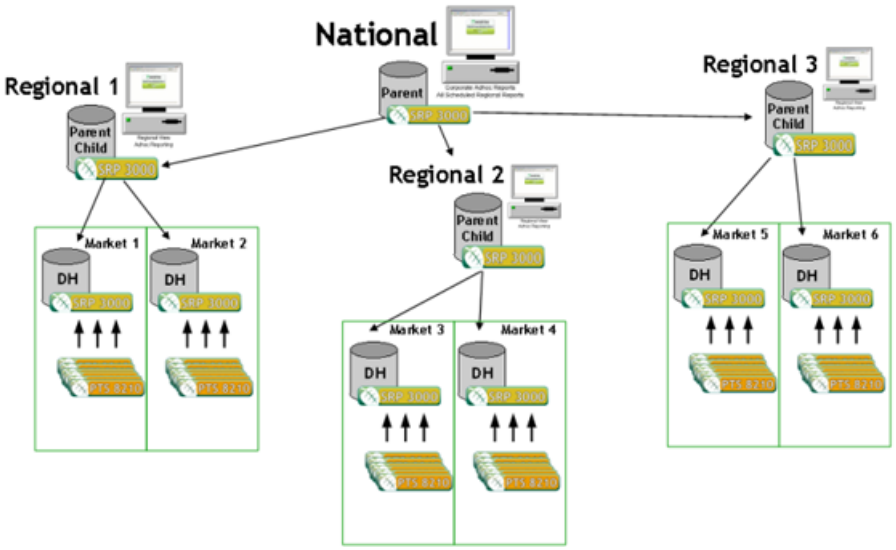
A datahome is a single SPB server or cluster of SPB servers where each contains an application server and a message broker, and each is identified by the same routing node name, plus a single database. The name of the datahome corresponds to the routing node name of its message broker.

A Sandvine installation site contains one or more logical datahomes. You can configure the datahomes in a hierarchy of parent/child relationships that represents their organization of operational sites.

When the datahomes are configured in a hierarchy, the data aggregation process transparently retrieves data from the parent datahome and its child datahomes. Data aggregation applies to reporting, search requests for subscribers, networks, network elements, application protocols, and more.

For example, a request for historical statistics is sent to a specific datahome. The response will contain statistics gathered from all network elements that are attached directly to the datahome where the request was received, and all children below that element.

Consider this datahome hierarchy: A top level request directed from the National datahome will gather any information from the National datahome as well as all child datahomes: Regional 1, Regional 2, and Regional 3. A lower level request directed at the Regional 1 datahome will gather any information from the Regional 1 datahome as well as all child datahomes configured under the Regional 1 datahome: Market 1 and Market 2.



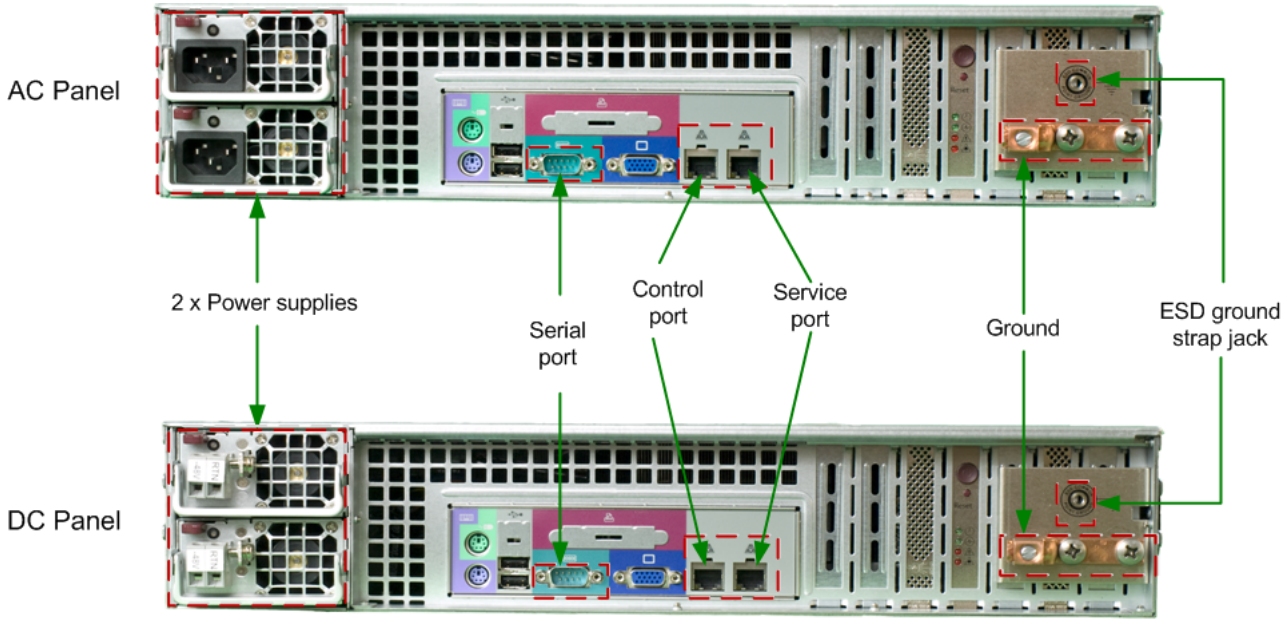
1.4 Storage, Reporting and Policy (SRP) Server

The Storage, Reporting and Policy (SRP) server provides the hardware infrastructure for the Subscriber Policy Broker (SPB).

The SRP server can also host the Network Demographics reporting application. You must install and configure the SRP before proceeding to install and configure the SPB.

The front view of the hardware:

The rear view of the hardware:



See the *SRP 3000-D Series Installation Guide* for details about the SRP hardware platform.

2

Initial Configuration

2.1 Configuration Checklist

Use this checklist for the initial configuration of the SPB server.

Pre-requisite:

Verify that your SPB is correctly installed and wired prior to configuring it on your network. For more information on hardware installation, refer to the *SRP Installation Guide*. For more information on the installation procedure, refer to the *SPB Release Notes*.

1. Set up the control interface. *Setting Up the Control Interface* on page 20. If you performed this step as part of the hardware install, skip this step.
2. Connect to the element. *Connecting to an Element* on page 20.
3. Change the password. *Changing the Root Password* on page 22.
4. Create a default user. *Configuring the Default User* on page 23.
5. Verify the package upgrade or installation. *Updating svupdate* on page 38.
6. Configure the database setup. *Database Server Configuration* on page 79.
7. Configure SPB hierarchy settings. If the installation is a large scale deployment, you can use the SPB hierarchy feature to optimize performance. *Configuring an SPB Hierarchy* on page 42.
8. Restart the SPB. *SPB Services Restart* on page 45.
9. Verify the key SPB processes. *Verify SPB Services* on page 45.

Post-requisite: Next steps:

- Configure subscriber IP mapping. *Minimal IP Mapping Configuration* on page 53.
- Configure Network Demographics. *Configuring Network Demographics Connections to the SPB* on page 72.
- Configure a data hierarchy. *Example Configuration for an SPB Hierarchy* on page 43.

2.1.1 Variable Naming Conventions

Enter case sensitive variable names using the indicated case.

Ensure that where appropriate, IP addresses are used instead of hostnames. You must use unique names when deploying Sandvine solutions. This means that you cannot use the same name as the RSS and PTS cluster names. Unique names are required for:

- Regional service site names
- SPB and PTS names
- SPB cluster and PTS cluster names

2.2 Setting Up the Control Interface

To set up the control interface:

1. At the login prompt, log in as root with the password sandvine.
2. To begin configuration, at the prompt execute the quickstart command.
3. From the menu, select **Management Interface & Network Configuration**.
4. Enter relevant values for these parameters:

```
IPv4 address
Subnet mas
Default gateway
Hostname
Domain
DNS resolvers
Enable telnet access?
Enable ssh access?
```

5. Select **Check connectivity** to verify IP connectivity.

2.3 Connecting to an Element

The first time you connect to an element to configure it, you must use a terminal console session. Once an element is configured, you can remotely connect using Secure Shell (SSH) or Telnet, if it is enabled. Telnet is disabled by default.

The methods for establishing communications with an element are:

- A serial terminal console session – Always use this session to connect to the element for the first time.
- A Secure Shell (SSH) session, which provides security when connecting across the network (enabled by default).
- A Telnet session to the control interface, (disabled by default). Sandvine does not recommend using Telnet because passwords are sent in clear text.

Once you have configured a control IP address and verified communications, apply central authentication. For more information, see the *SPB CLI Reference Guide* for this release.

2.3.1 Launching a Serial Terminal Session

Perform the initial configuration of the PTS element using a terminal session.

The Quickstart Management Interface menu appears the first time you connect to the Management Console and login.

Note:
Until the control interface has been configured, the Quickstart, Management Interface menu will continue to appear each time you log in using the sv_admin user.

1. Connect a computer to the Management Console interface using the null-modem serial cable with a DB-9F to DB-9F connector that is provided with each element.
2. Launch a terminal session by entering these communication parameters:

- Baud rate: 115,200
- Parity: None
- Data bits: 8
- Stop bits: 1
- Flow Control: None

3. Establish the connection by pressing Enter.

   You can tell that the connection is established when the login prompt appears or the boot-up procedure completes.

4. At the login prompt, log in as sv_admin with the password "sandvine".

   If this is the first time you are connecting to the PTS, and the management interface has not yet been configured, Quickstart will automatically launch.

   To re-start Quickstart run:

   ```
   sv_enable svadmin
   quickstart
   ```

5. At the login prompt, log in as root with the password sandvine.

2.3.2 Connecting with SSH

Once the IP address, default gateway and DNS servers have been configured, Sandvine recommends you use an SSH session to communicate with the element.

There are several free SSH clients available for download. You can use your preferred SSH client.

1. On a remote workstation with an SSH client installed, initiate a connection with the PTS element. At a command prompt enter:

   ```
   $ ssh root@x.x.x.x
   ```

   ```
   $ ssh sv_admin@x.x.x.x
   ```

   Where x.x.x.x is the IPv4 address of the control interface on the element.

2. At the password prompt, enter the password.

3. You are initially logged in to the system as sv_operator. To increase your privileges to administrator, run the `sv_enable` command twice.

   For more information, see *Increasing Privileges using sv_enable*.

2.3.3 Connecting with Telnet

The Telnet daemon is disabled by default. To enable Telnet, use the Quickstart menu.

Pre-requisite:

The terminal should emulate vt100 or xterm.

Caution:
Sandvine does not recommend using Telnet because passwords are sent in clear text.

1. In a command prompt window, or in the Run dialog, enter:

   ```
   telnet root <x.x.x.x>
   telnet sv_admin <x.x.x.x>
   ```

   Where x.x.x.x is the IPv4 address of the control interface on the element.

2. At the password prompt, enter the password.

2.4 Users and User Groups

Users and groups allow or restrict access to the system.

A default user is configured for each user group that has the same name as the user group. The users and groups available are:

- sv_admin - Administrative users have full access. They can start or stop any application and edit files
- sv_service - Service users can start or stop some applications and edit run-time configuration files
- sv_operator - Operators have read-only privileges for accessing log files.

Three corresponding principle groups exist on the element:

- sv_admin (most privileges)
- sv_service (moderate privileges)
- sv_operator (minimum privileges)

The default principle group for all three accounts is sv_operator (having the least security privileges).

To log in as the administrative user the login name is sv_admin and the default password is sandvine.

The sv_admin account is:

- A built-in-account.
- The management account for the element.
- The default administrative account for the element, with absolute privileges on the system.

Once the element is configured, change the default password to enhance security.

2.4.1 Changing the Root Password

The root user is the default system account and as the superuser, has absolute privileges on the system. It is usually only used by the system administrator for adding users, managing the network and installing and maintaining hardware and software

All user IDs are password protected. The root user's default password is sandvine. To ensure a secure environment, the root password should be changed and set in accordance with your internal policies. Passwords should be a minimum of six characters in length and should conform to your corporate policies.

1. Connect to the element as the root user.

2. Execute the passwd command and respond to the on-screen prompts.

```
(SPB)# passwd
Changing local password for root
New Password:
Retype New Password:
```

2.4.2 Configuring the Default User

The SPB is shipped in secure mode. The default-user must be created on each SPB server before it can be used.

1. Put the CLI into configuration mode, then enable the default-user with these commands:

```
SRP# configure
SRP# set config default-user enabled true
```

2. Commit your changes:

```
SRP# commit
```

2.4.3 Managing User Accounts

This section explains how to authenticate users remotely, add or remove users, and track system changes made by users (Accounting).

The PTS has three privilege levels and ships with three default user accounts, one for each privilege level.

User	Privilege Level	Description
sv_admin	sv_admin	Full administrative privileges.
sv_service	sv_service	Operator plus the ability to modify and reload some configuration.
sv_operator	sv_operator	Read-only access.

The sv_admin account is enabled by default with the default password “sandvine”. The other two accounts are disabled and can be enabled by setting their passwords. When you are successfully authenticated, you are logged in as a member of the sv_operator group. You can increase your privilege level by executing the sv_enable command to obtain membership in another group. For example, to obtain membership in the sv_service group, run: sv_enable sv_service. To decrease the security level, use the `exit` command.

New user accounts can be added to the system using CLI, or the system can be configured to remotely authenticate users using TACACS+ or RADIUS.

2.4.3.1 Managing Local User Accounts

Use these CLI commands to manage User Accounts:

Command	Description
show user	Lists all users. **Name:** The user’s name. **Group:** The user’s privilege level.

Command	Description
	Type: The type of user account (local or remote to indicate if they were created locally or through remote authentication).
show user <name>	Displays additional detail for a specific user. **Name:** The user's name **Group:** The user's privilege level **Type:** The type of user account ("local" or "remote" to indicate if they were created locally or due to remote authentication) **DefaultShell:** The user's default shell, either "bash" or "cli" **LastLogin:** The last time the user logged in to the system.
add user <name> group <admin|service|operator>	Creates a new local user account with the specified privilege level.
delete user <name>	Deletes a user account.
set user password	Can be used by any user to change their password.
set user <name> password	Can be used by an administrative user to change any user's password.
set default-shell <bash|cli>	Can be used by an administrative user to change their default shell.
set default-shell <name> <bash|cli>	Can be used by an administrative user to change any user's default shell.

2.4.3.2 Remote Authentication

Administrative users of Sandvine elements can be authenticated using either RADIUS or TACACS+. Once you are successfully authenticated by a central server, you are logged in to the Sandvine element as a member of the sv_operator group, which has the least amount of privileges.

For more information on the commands for remote authentication using RADIUS and TACACS+, see the *SPB CLI Reference Guide*.

2.4.3.2.1 RADIUS User Authentication

To enable authentication of Sandvine users, the RADIUS server's dictionary file must be augmented to use Sandvine-specific attributes.

To the dictionary file add:

- A vendor named "Sandvine" with ID 11610.
- An attribute named "Sandvine-Group" of type string and vendor "Sandvine" and ID 2.

The RADIUS server must add these attributes onto the list of outgoing attribute-value pairs. "Sandvine-Group" specifies the comma-separated list of groups that the user belongs to. If the groups are not specified, or are all invalid, the default group "sv_operator" is assigned to the user. For example, if a user belongs to groups "sv_operator" and "sv_admin", then the attribute-value pairs would be listed as:

```
Sandvine-Group= "sv_operator,sv_admin"
```

For a freeRADIUS server, the user entry would look like:

```
userA Auth-Type := Local, User-Password=="passA"
      Sandvine-Group="sv_operator,sv_admin"
```

2.4.3.2.1.1 Configuring RADIUS Authentication

To configure an element to authenticate administrative users against a RADIUS server:

1. Enter CLI configuration mode. Run:

   ```
   configure
   ```

2. Run these commands:

   ```
   set config system authentication radius servers
   set config system authentication radius secret
   ```

   Where:

   - servers - specifies the list of RADIUS server IP addresses separated by a single space.
   - secret - specifies the common shared secret key between all the RADIUS servers and the element.

   For example:

   ```
   set config system authentication radius servers "192.168.0.1 192.168.0.2"
   set config system authentication radius secret "topsecret"
   ```

3. To commit the changes, run:

   ```
   commit
   ```

   Committing these changes restarts the authentication service.

2.4.3.2.2 TACACS+ User Authentication

The system can be configured to authenticate users against one or more TACACS+ servers.

2.4.3.2.2.1 Configuring TACACS+ Authentication

By default, the system tries to authorize users for the "sandvine" service, which requires some configuration on the TACACS+ server. Users that will be using the PTS must have this service granted for their account.

You can configure the system to use a different service name using the configuration command `set config system authentication tacacs+ service <service-name>`. On a TACACS+ server, each user entry must allow the service "sandvine". Within this service, the attribute-value pair is an attribute named "Sandvine-Group" of type string.

Note:
TACACS+ authentication is enabled by default.

Perfom these steps to configure an element to authenticate administrative users against a TACACS+ server:

1. Run this command to put the CLI in configuration mode:

   ```
   configure
   ```

2. Enable TACACS+ authentication if it is disabled:

   ```
   set config system authentication tacacs+ enabled true
   ```

3. Run these commands to set your servers and secrets:

   ```
   set config system authentication tacacs+ servers
   set config system authentication tacacs+ secret
   ```

   Where:

   - servers—Specifies the list of TACACS+ server IP addresses separated by a single space
   - secret—Specifies the common shared secret key between all the TACACS+ servers and the element

For example:

```
set config system authentication tacacs+ servers "10.10.10.1 10.10.10.2"
set config system authentication tacacs+ secret "topsecret"
```

4. Run this command to commit the changes:

```
commit
```

Committing these changes restarts the authentication service.

2.4.3.2.2.2 Sample TACACS+ Configuration

Here is a sample TACACS+ server configuration (for the tac_plus server) showing a user that is provisioned to use the "sandvine" service with administrative privileges:

```
user = jsmith {
     service=sandvine {
          Sandvine-Group="sv_admin"
     }
     login = cleartext "passA"
}
```

2.4.3.3 Accounting

All CLI and shell activity is logged to a local accounting file, `/var/log/cli_audit.log`. You can view the contents of the log file using the `show log cli` or `monitor log cli` CLI command.

Note:
To run this command, you must log in as a root user.

2.4.3.3.1 TACACS+ Accounting

In addition to the local accounting, you can configure the system to log accounting records to a remote TACACS+ accounting server.

The host port field is "unknown" for SSH logins because the TTY is allocated after the system authenticates/authorizes the user.

The remote host field is only logged for SSH logins/logouts and CLI and shell commands that are executed in an SSH session.

Note:
TACACS+ accounting is not enabled by default.

To configure an element to enable accounting of administrative users against a TACACS+ server:

1. Run this command to put the CLI in configuration mode:

```
configure
```

2. Run the `set config system accounting tacacs+ enabled true` CLI command to enable accounting.

3. Run these commands to set the servers and secrets:

```
set config system accounting tacacs+ servers <servers>

set config system accounting tacacs+ secret <secret>
```

Where:

- servers—Specifies the list of TACACS+ server IP addresses separated by a single space
- secret—Specifies the common shared secret key between all the TACACS+ servers and the element

For example:

```
set config system accounting tacacs+ servers “10.10.10.1 10.10.10.2”
set config system accounting tacacs+ secret “topsecret”
```

4. Run this command to commit the changes:

   ```
   commit
   ```

   Committing these changes enables accounting.

2.5 Using Quickstart

Use the Quickstart menu to perform basic initial configuration tasks of the network and element.

To select a menu option, enter the menu option number. When you select an option from the System Quickstart menu, you are guided through a number of configuration questions.

- If a default for the option exists, the default is displayed in square brackets. For example:

  ```
  Enable telnet access? (y/n)[YES]:
  ```

- Press **Enter** to accept the default or type another response.
  Appropriate responses are indicated in round brackets.
- If a submenu appears, select the desired option to continue configuration.
- The last option in each menu is `Apply changes?`. To apply changes, enter **y**. To cancel the selections, enter **n**.
- Choose option **0** to exit Quickstart.

2.5.1 Quickstart Menu Options

The menu options that are available from the Quickstart menu are:

Select this Quickstart menu option...	**To...**
Management Interface & Network Configuration	Configure the element on the network, including: IP address, subnet mask, default gateway, enable SSH, enable Telnet.
Cluster Interface	Assign an IP address to the cluster interface.
NTP Configuration	Select an NTP server.
Time Zone	Set the local time zone on the element.
SPB Configuration	Identify the SPB to use for logging statistics.
SNMP Configuration	Identify the SNMP version, community, and trap server for each SNMP management machine.
Show Settings	Display the current settings on the element.
Check Connectivity	Ping an IP address to verify that the element is connected on the network.
Firewall Configuration	Configure firewall settings and ports. **Note:** There is a specific default firewall configuration. Sandvine recommends that you avoid changing the firewall configuration unless required.

Select this Quickstart menu option...	To...
Exit	Exit from the Quickstart menu.

2.5.2 Logging into Quickstart for the First Time

The first time that you connect to an element and log in as sv_admin, a message appears to indicate that the element is not configured. The Management Interface menu prompt is then displayed:

```
System appears not to have been previously configured.
Proceeding with management interface quickstart.
Management Interface
====================
IPv4 address:
```

You are prompted to configure parameters including the IP address, subnet mask, and gateway. When you have responded to the management interface menu prompts and applied the changes, the entire Quickstart menu is displayed. Other menu options are available to set the time zone, specify Network Time Protocol servers and other parameters.

When you exit from the Quickstart menu, you are logged in as the sv_admin user with the lowest group privilege level (sv_operator). To return to the highest privilege level for sv_admin, you must run sv_enable with the requested group as the argument (for example, run sv_enable sv_admin).

Note:
If the IP address on the control interface is not configured, the Quickstart menu is displayed every time you log in as sv_admin.

2.5.3 Manually Invoking Quickstart

Quickstart automatically starts during the initial setup only. You can run the quickstart command later to manually initiate the process.

1. Connect to the element and login as an administrative user. When you connect as an administrative user, you are logged in to the group with the lowest privilege level. To increase your privilege level, run the `sv_enable` command with the requested group as the argument.

2. At a command prompt, enter: `quickstart`.

   For example:

```
login as: sv_admin
sv_admin@<hostname>'s password:
Last login: Wed Oct 10 09:49:05 2012 from 10.10.10.1
SVOS Stock Image

(<hostname>:sv_operator)$ sv_enable sv_admin
(<hostname>:sv_admin)# quickstart
SYSTEM QUICKSTART
=================
1.  Management Interface & Network Configuration
2.  Cluster Interface
3.  NTP Configuration
4.  Time Zone
5.  SPB Configuration
6.  SNMP Configuration
7.  Show Settings
8.  Check Connectivity
9. Firewall Configuration
10.  Exit
>
```

2.5.4 Exiting the Quickstart Menu

Exit the Quickstart menu with **Ctrl** + **c**.

This returns you to the Quickstart utility. Entering 0 for Exit will exit the utility and return you to the command prompt.

2.6 Control Center

Control Center is Sandvine's unified policy and operations management graphical user interface, providing a single mechanism for monitoring operational information, editing network policies, configuring elements, and deploying network policy control solutions.

Control Center lets communications service providers (CSPs) centrally create and deploy service policies for the entire network in response to new opportunities or trends. This simplifies all aspects of Sandvine operations management, delivering real-time information and granular control.

Control Center lets you safely configure SandScript in isolation from the physical devices in order to control when the elements enforce new SandScript behavior. Control Center is also a repository of configuration information for the elements (PTS, SDE, and SPB). The elements are responsible for managing real-time data and enforcing SandScript. Control Center manages all SandScript and configuration changes in its database. The migration of SandScript and configuration to the elements is called a deployment. Deployment is not automatic; you must start it manually.

2.6.1 System Requirements

These system requirements are necessary for optimal performance.

2.6.1.1 PC Requirements

Your PC must meet these requirements:

- Windows PC running Windows 7 (recommended), Windows XP, or Windows Vista.
- Windows PC minimum hardware requirements are:

- 1 GB free RAM.
- 500 MB free disk space.
- 1 gigahertz (GHz) processor.

2.6.1.2 Network Connection

The Control Center client runs on a client PC and communicates with the Control Center server on an SRP element. The speed and quality of the network connection between the client and the SRP affect the performance of Control Center. The recommended network properties are:

- Bandwidth – 1 Mbps or faster.
- Latency – 100ms or less.

2.6.1.3 Network Size

Control Center supports deployments of up to 200 elements (any combination of PTS, SDE, or SPB elements). Each datahome can have up to 50 elements. To create a deployment containing more than 50 elements, operators must use multiple datahomes.

2.6.1.4 Sandvine Platforms

To allow Control Center to manage elements, change the element's cluster name from the default name.

Note:
These are the default names:

- SPB – DefaultCluster
- PTS – SANDVINE-1
- SDE – SANDVINE-SDE-1

Control Center is compatible with these Sandvine platform versions, or higher:

- SPB 6.00.02

  Note:
  Upgrade the SPB to 6.00.02 before installing Control Center.

- PTS 6.10
- SDE 6.20.03

2.6.1.5 Feature Compatibility Matrix

This table lists the Control Center features that require a higher minimum version of platform software for the feature to run. When Control Center is managing platforms with less than these minimum platform software versions installed, the feature is not available.

Control Center Feature	Minimum Required Platform Versions
Alarms sub-tab and Alarms Count Panel	• PTS - 6.20 • SPB - 6.30 • SDE - 6.30 • Control Center server - 6.20
ServiceDesigner	• SDE - 7.00 • Control Center server - 6.40

2.6.2 Launching Control Center

This section describes the steps to launch Control Center on your system.

To launch Control Center on your machine you need to download the installer. Follow these steps to launch and install Control Center:

1. Open a web browser.

2. Enter the IP address or host name of the Control Center server using HTTPS. For example:
   `https://x.x.x.x:y/sandvine/`

   Where:

   - *x.x.x.x* is the IP address or host name.
   - *y* is the default port number that the server is listening on.

   The defaults are:

   `https://x.x.x.x:8443/sandvine`

   Note:
   If you are using HTTPS to connect to Control Center, install a signed certificate on the Control Center application server. If you do not want to install the certificate you can skip this step and launch Control Center directly. See the *SPB API Guide* for instructions on Creating a Server Certificate.

   The Control Center launch page opens.

3. Click **Control Center for Windows** on the Control Center launch page.

   The client installer file downloads.

4. Double-click on the `client installer.exe` file.

   The *Control Center 6.40 Installer* dialog appears.

5. Click **Next** to continue.

   The *License Agreement* dialog appears. Read and accept the terms and conditions before clicking **OK** to continue.

6. Choose the installation location.

   Note:
   Sandvine recommends that you use the default folder.

7. Click **Next** to continue.

8. Select the **Launch Control Center** option.

9. Click **Finish** to complete the installation process.

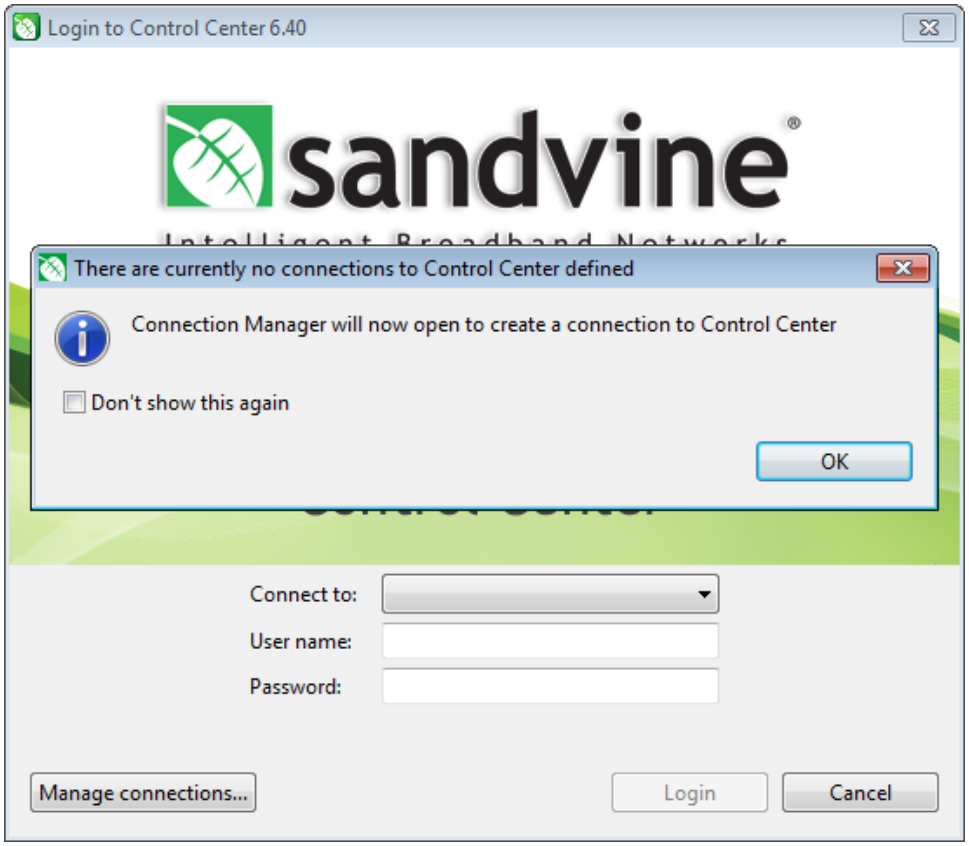
   Note:
   A Control Center shortcut is created in the start menu, you can launch Control Center using the shortcut.

   The *Login to Control Center 6.40* dialog appears. See *Login to Control Center* on page 32 for instructions on how to log in to Control Center.

2.6.2.1 Login to Control Center

This section describes the steps to login to Control Center.

If you are logging in to Control Center for the first time, you need to create and add a new connection. After launching Control Center, the *Login to Control Center 6.40* dialog appears. Follow these steps to create and add a new connection:

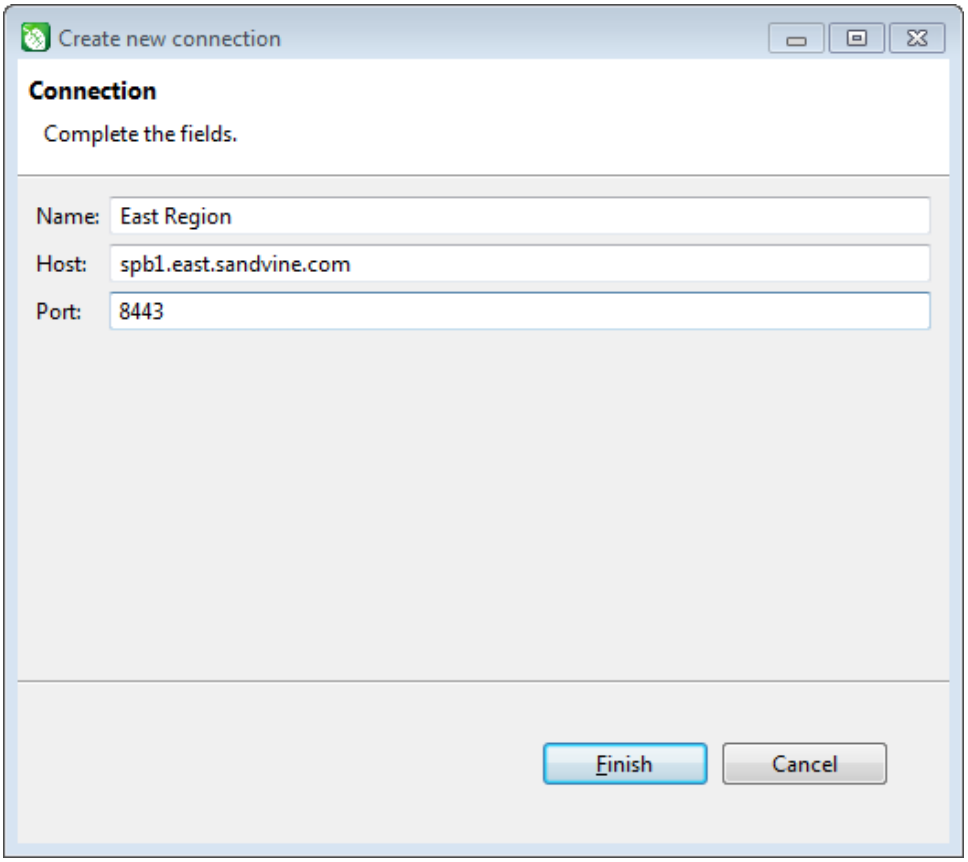


1. Click **OK** on the *There are currently no connections to Control Center defined* dialog.

   The *Create new element* dialog appears.

2. Type in the details for:

   - Name – Display name for the connection.
   - Host – Host name of the Control Center server.
   - Port – Port to connect to.



3. Click Finish.

   The **Manage Connections** dialog appears. The connection created in step 2 appears.

4. Click **Close** to close the *Manage Connections* dialog.

   The *Login to Control Center 6.40* dialog appears.

5. Select the server from the **Connect to** drop-down menu.

   See *Manage Connections* on page 34 for more information on how to edit and delete a connection.

6. Log in with your user name and password.

Post-requisite:

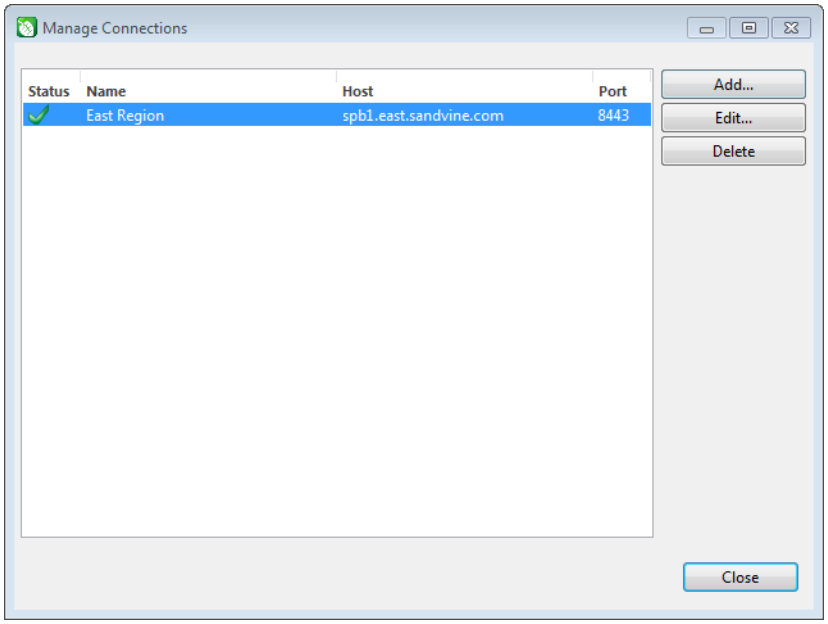
If this is the first time you have launched Control Center for a new installation, add the datahome configurations in the **Setup** wizard.

2.6.2.2 Manage Connections

Manage connections helps you to add, edit, or delete a server. You can add multiple servers to Control Center using manage connections.

Select **Manage connections** on the *Login to Control Center 6.40* dialog.

Fields	Description
Status	Status of the connection: • ✔ means the server is connected successfully. • ⊗ means the server is offline or not running control center. • ? means that status is currently unknown (check in progress). **Note**: If the user hovers their mouse over a row with an ⊗, the error appears in a tooltip.
Name	This is the user friendly name for the connection. You can use any name but duplicate names are not allowed. This is the value shown in the “Connect to” drop-down menu on the Login Dialog.
Host	This is the IP address or host name of the Control Center server. The hostname must match RFC 1123.
Port	Port to connect to, defaults to 8443 (HTTPS default port). May be set to any value between 1 and 65535.



The *Manage connections* dialog appears. Follow these steps to add, edit, or delete a server:

- Click **Add...** to add a new server.

The **Create new connection** dialog appears, repeat step *2* on page 33 and step *3* on page 34 in the section *Login to Control Center* on page 32.

- Click **Edit...** and update the required fields.

Repeat step *2* on page 33 and step *3* on page 34 in the section *Login to Control Center* on page 32

To delete an existing server, do one of these:

- Select a connection and click **Delete**.
- Select a connection and press the **Delete** key on the keyboard.
- Right-click on a connection, and select **Delete**.

2.6.3 Online Help

For further information about Control Center, see the online help. Control Center's policy creation wizards contain help content and tool tips are available when you hover your mouse over a GUI button.

2.7 Using the CLI Shell

The Sandvine Command-Line Interface (CLI) provides commands to view the active configuration and operational metrics of Sandvine elements, and commands to configure the system.

The CLI includes tab completion (automatically completes a command from partial input, or shows the available options) and provides integrated help. For more information about the CLI and CLI commands, refer to the *CLI/Operations Reference Guide* for this release.

Note:
Some variables are still configured using rc.conf. For information on the specific variables, see the release notes for this release. Note that the "#" character in rc.conf is reserved for comments. Therefore, if you need to use this character for any other operation, use its hexadecimal equivalent "\x23".

1. Log into the Sandvine element, either through a console connection or using SSH.

2. At the command prompt enter:

   ```
   svcli
   ```

   You are now in operational mode. In this mode you can view operational metrics, the configuration of the system and set some system variables.

   You can also access the CLI using the command `cli`.

3. To use configuration mode, you must be an administrative user. To enter configuration mode, enter:

   ```
   SRP> configure
   ```

   ```
   PTS> configure
   ```

   You are now in configuration mode. In this mode you can change the configuration of the system. Only one person at a time is allowed in configuration mode. Any changes made to the configuration are saved, but not applied.

4. To apply your configuration changes enter:

   ```
   SRP# commit
   ```

   ```
   PTS# commit
   ```

   The system will automatically reload, restart, or reboot any required processes or elements.

   Note:
   Committing configuration changes can potentially impact service. Sandvine recommends that you perform these changes during regularly scheduled maintenance windows.

5. To exit configuration mode and return to operational mode enter:

```
SRP# exit
PTS# exit
```

6. To exit the CLI, from operational mode enter:

```
SRP> exit
PTS> exit
```

2.8 Updating Packages with svupdate

2.8.1 About svupdate

Use `svupdate` to install or upgrade packages on an element (PTS and SPB only).

You can run `svupdate` in either interactive or non-interactive mode:

- Interactive mode enables you to select the required product and release from the menu.
- Non-interactive mode enables you to select the required product and release from the command line.

2.8.2 Using the svupdate Menu

To run svupdate, connect to an element, and at the command prompt, run `svupdate`.

svupdate will:

- Indicate whether you need to upgrade svupdate to a newer release.
- List the packages that are currently installed on the element.
- Display the Family menu for the element.

To install or upgrade, select the family: for example, PTS or SPB. Once you identify the family, subsequent menus prompt you to select the specific product, software release, and the operation to perform.

Operation	Description
Install Images	Fetches and installs packages.
Install Images, Fetch Documentation	Fetches and installs packages and documentation.
Fetch Change Images	Fetches the packages but does not install them.
Fetch Documentation	Fetches the documentation, including Release Notes.
List Images	Lists the packages available for the selected release.
List Documentation	Lists the documentation available for the selected product (excluding Release Notes).
Compare Images	Compares the available packages with those that are installed on the system and provides a list of what is already installed and what you need to install.

Operation	Description
Fetch All Images	Use to build a remote update server. All images for the selected release, regardless of whether they are already installed on the current machine, are fetched.
Exit	Terminates svupdate.
b	Displays the previous menu.
q	Exits svupdate.

2.8.3 Updating svupdate

Before beginning the upgrade, you must update svupdate.

Each time you run the `svupdate` command, it checks to see if there is a new version available. If an update is available, a message similar to this appears:

```
There is a newer version of svupdate available <version_number>.
Please upgrade to that first before continuing with the upgrade.
Failure to do so may impair the upgrade process.
*********************************************************************
Continue (y/n/q)?
```

Type `y` to continue.

When the svupdate upgrade is completed, the svupdate menu is displayed. This ensures that the most current menu options are available.

Note:
Failure to upgrade svupdate can result in serious problems.

If the element you are upgrading does not have access to the Internet, use an element with access to the Internet to download the software. Follow the steps outlined in *For Elements without Internet Access* on page 39.

2.8.4 Performing an svupdate

When you perform an svupdate, it provides information about your system such as which packages are installed. svupdate has an interactive menu that you can use to download/install products and complete other tasks.

1. Ensure that the element you are connected to has Internet access.
2. Log in as an administrative user.
3. At the command prompt, enter **svupdate**.
4. Enter your Sandvine Support user ID and password as prompted.
5. If a newer version of svupdate is available (a message appears), update svupdate before you download or install any software packages. See *Updating svupdate* on page 38. Otherwise, select a menu option.

2.8.5 Running svupdate Command on Internet-Connected Element

To run `svupdate` command on an internet-connected element:

1. Log on to the element as an administrative user.
2. Run `svupdate` command to initiate `svupdate`.
3. Respond to the prompts to enter your Sandvine Customer Support user ID and password.
4. If a message appears indicating that there is a newer version of svupdate available, update svupdate before proceeding to update packages (see *Updating svupdate* on page 38).
5. Choose one of these options at the **Continue** prompt.
   - To choose the Family menu, enter **y**.
   - To terminate svupdate, enter **n** or **q**.
6. Select from additional menus as required.

2.8.6 For Elements without Internet Access

If the element to be upgraded does not have access to the internet, download the install files for the upgrade.

Pre-requisites:

- Any machine with access to the internet.
- A method of transferring a single file from the machine with internet access to the Sandvine element that does not have access.

1. Log in to the Sandvine Customer Support site at *https://support.sandvine.com*
2. Download the release tarball.
3. Copy the tarball to the Sandvine element.
4. Run this command to install the package:

   ```
   pkg_add <downloaded_tar_ball>
   ```

2.8.7 svupdate Command Line Options

Sandvine has developed the `svupdate` script to install or upgrade Sandvine product packages. This script encapsulates only standard Linux commands. Enter `svupdate -h` to display the list of options.

Option	Description
-C	This option compares the available packages with those that are installed on the system. It also provides a list of what is currently installed and what you need to install. It shows what will happen if you upgrade the element to the selected release without taking any action. It is the equivalent to selecting **Compare Image** from the interactive mode menu.

Option	Description
-d *value*	This give you the choice of fetching documents only or documents and install images. You can choose one of these options: • 1 = documents in addition to installing images. • 2 = documents only.
-f *value*	Fetches packages but does not install them. The available options include: • 1 = places all modified packages in the same root directory. Does not maintain the FTP directory hierarchy. • 2 = places all modified packages in the same root directory while maintaining their directory hierarchy. • 3 = places all packages for the selected version in the same root directory while maintaining their directory hierarchy. The environment variable $TMPDIR determines the root directory and, if this variable is not set, the default is `/d2/tmp`.
-F *value*	Family of products. This option is used in conjunction with the `-V` and `-P` options to provide a method to specify an exact release from the command line. The value that is specified must match a specific value located in the Family sub-menu.
-I|-image value	Upgrade using packages from an upgrade image.
-l	Selects the latest release automatically. Use this option in conjunction with the `-P` and `-F` options.
-L *value*	Lists the packages that are available for the selected release. You can choose one of these options. • 1=list packages with their directory hierarchy. • 2=list packages without their directory hierarchy. The `-L 2` option is equivalent to selecting `List Images` from the interactive mode menu.
-o	Operating system override if different from uname. This option lets you specify which packages to download for the specified Operating System version, instead of the current devices. You can use this when downloading packages for a different system.
-p *value*	Identifies the clear text password for a non-interactive logon to the FTP server.
-P *value*	Identifies the specific product to use. Use this option in conjunction with the `-V` and `-F` options to specify an exact release from the command line. The release specified must match an entry on the Product sub-menu.
-R	Automatically reboot after an upgrade (if required) rather than prompting the user to reboot.
-s	Runs `svupdate` in silent mode, which outputs as little information as possible.
-u *value*	Identifies the clear-text user name for a non-interactive logon to the FTP server.
-U *value*	Identifies the URI to fetch files. This allows you to specify a non-standard URI from which to fetch files. This option is incompatible with the `-u` and `-p` options.
-V *value*	Identifies the specific version to get. Use this option in conjunction with the `-P` and `-F` options to specify an exact release from the command line. The version specified must match an entry on the Release sub-menu.
-Z	Upgrade licenses. This option checks for product license upgrades and then exits.

2.9 Populating /etc/hosts

To ensure that PTS elements and other clients can access the SPB, the SPB server requires that the `/etc/host` file have an entry for the local host matching its hostname to an IP address.

Pre-requisite:

You must run Quickstart before starting this procedure. See *Using Quickstart* on page 27

When configuring firewall rules refer to *Network Security* on page 108 for details regarding port access requirements required for external clients.

1. As an administrative user logon to each SPB server.

2. Display the settings in Quickstart. At the command prompt, run the `quickstart` command, then choose the **Show Settings** menu option.

3. With the hostname, IP address and domain name as specified in Quickstart, verify that the /etc/hosts file has an entry for the hostname.

   ```
   ip-address hostname hostname.domainname
   10.10.10.1 spb-1.anydomain.com
   ```

   Where:

   - 10.10.10.1 is the IP address of the SPB server that is accessible by internal clients such as PTS elements
   - sbp-1.anydomain.com is the host name as specified in Quickstart

   When adding alias names to the etc/hosts file, ensure that the hostname is the first entry. For example:

   ```
   10.10.10.1 spb-1.anydomain.com spb1.alias1 spb1 alias2
   ```

   When configuring firewall rules refer to *Network Security* on page 108 for details regarding port access requirements required for external clients

4. Ping the SPB server via the hostname to verify the resolution is working correctly.

   A two to three minute delay, before hostname resolution starts to work correctly, is not uncommon.

2.10 Configuring Cluster Name

A default cluster name must be set to use the SPB. Ensure that you configure all SPBs in the cluster to use the same cluster name.

1. Put the CLI into configuration mode using the `configure` command.

2. Run this command:

   ```
   SRP# set config cluster name <name>
   ```

   Where <name> is a short, descriptive name for the SPB. The name chosen must be unique across all sites in a large deployment. The cluster name cannot contain more than 64 characters and can contain only alphanumeric characters or underscores (_). Other special characters are not allowed.

3. Commit your changes:

   ```
   SRP# commit
   ```

Committing this change requires restarting the message broker and application server. You are prompted for confirmation.

2.11 Configuring an SPB Hierarchy

To initially configure an SPB hierarchy, add datahome settings for each datahome in the hierarchy. See *SPB Hierarchy* on page 153.

In the SPB hierarchy, a datahome is only configured for its immediate parent and any children in order for the hierarchy to operate properly.

- Use the same datahome name as the cluster name specified by `set config cluster name <name>`. See *Variable Naming Conventions* on page 19.
- Each cluster/datahome, in every SPB hierarchy, must use unique names. In a given SPB hierarchy, the value for each datahome ID must be unique.

2.12 Changing the Configuration for an SPB Hierarchy

After initial setup, any changes made to the SPB hierarchy configuration will require a restart of the application server and the message broker.

When upgrading an SPB hierarchy, start at the bottom of the hierarchy and upgrade the levels in sequence to the top. This ensures that requests being formed at higher levels are backward compatible with the newer versions in the hierarchy below.

2.12.1 Datahome Name Changes

To change the datahome name, in CLI configuration mode, run:

```
SRP# set config data-home <id> name <name>

SRP# commit
```

Make sure that when you set the cluster name (`set config cluster name <name>`) you use the same name as the local datahome name. Using either of these commands will reload the message broker and application server when they are committed.

2.12.2 Removing a Datahome

In order to remove a datahome, in CLI configuration mode, run:

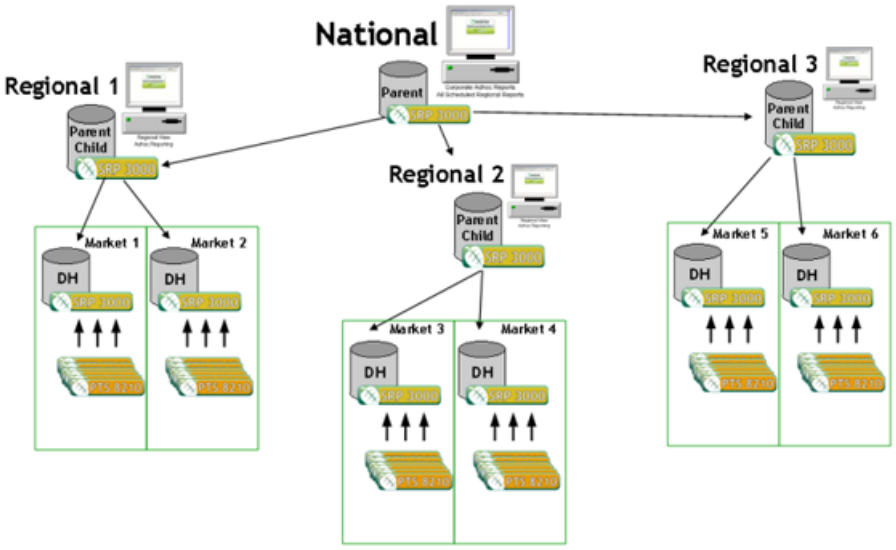
```
SRP# delete config datahome <id>

SRP# commit
```

This will also restart message broker and the application server.

2.13 Example Configuration for an SPB Hierarchy

This is an example of a typical SPB hierarchy. Committing these configuration changes requires a restart.



The IP addresses in the examples are:

```
National - 0.0.0.0
Regional 1 - 1.1.1.1
Regional 2 - 2.2.2.2
Regional 3 - 3.3.3.3
Market 1 - 1.0.0.1
Market 2 - 1.0.0.2
Market 3 - 2.0.0.3
Market 4 - 2.0.0.4
Market 5 - 3.0.0.5
Market 6 - 3.0.0.6
```

Configuration for National datahome:

```
SRP# set config cluster name National
```

Configuration for Regional 1 datahome:

```
SRP# set config cluster name Regional1
```

Configuration for Regional 2 datahome:

```
SRP# set config cluster name Regional2
```

Configuration for Regional 3 datahome:

```
SRP# set config cluster name Regional3
```

Configuration for Market 1 datahome:

```
SRP# set config cluster name Market1
```

Configuration for Market 2 datahome:

```
SRP# set config cluster name Market2
```

Configuration for Market 3 datahome:

```
SRP# set config cluster name Market3
```

Configuration for Market 4 datahome:

```
SRP# set config cluster name Market4
```

Configuration for Market 5 datahome:

```
SRP# set config cluster name Market5
```

Configuration for Market 6 datahome:

```
SRP# set config cluster name Market6
```

These settings are required for the National datahome:

```
SRP# add config data-home 1 name National display-name National url ssl://0.0.0.0:2507
SRP# add config data-home 2 name Regional1 display-name Regional1 url ssl://1.1.1.1:2507 parent
 National
SRP# add config data-home 3 name Regional2 display-name Regional2 url ssl://2.2.2.2:2507 parent
 National
SRP# add config data-home 4 name Regional3 display-name Regional3 url ssl://3.3.3.3:2507 parent
 National
```

These settings are required for the Regional1 datahome:

```
SRP# add config data-home 1 name National display-name National url ssl://0.0.0.0:2507
SRP# add config data-home 2 name Regional1 display-name Regional1 url ssl://1.1.1.1:2507 parent
 National
SRP# add config data-home 5 name Market1 display-name Market1 url ssl://1.0.0.1:2507 parent
Regional1
SRP# add config data-home 6 name Market2 display-name Market 2 url ssl://1.0.0.2:2507 parent
Regional1
```

These settings are required for the Regional2 datahome:

```
SRP# add config data-home 1 name National display-name National url ssl://0.0.0.0:2507
SRP# add config data-home 3 name Regional2 display-name Regional2 url ssl://2.2.2.2:2507 parent
 National
SRP# add config data-home 7 name Market3 display-name Market3 url ssl://2.0.0.3:2507 parent
Regional2
SRP# add config data-home 8 name Market4 display-name Market4 url ssl://2.0.0.4:2507 parent
Regional2
```

These settings are required for the Regional3 datahome:

```
SRP# add config data-home 1 name National display-name National url ssl://0.0.0.0:2507
SRP# add config data-home 4 name Regional3 display-name Regional3 url ssl://3.3.3.3:2507 parent
 National
SRP# add config data-home 9 name Market5 display-name Market5 url ssl://3.0.0.5:2507 parent
Regional3
SRP# add config data-home 10 name Market6 display-name Market6 url ssl://3.0.0.6:2507 parent
Regional3
```

These settings are required for the Market1 datahome:

```
SRP# add config data-home 2 name Regional1 display-name Regional1 url ssl://1.1.1.1:2507 parent
 National
SRP# add config data-home 5 name Market1 display-name Market1 url ssl://1.0.0.1:2507 parent
Regional1
```

These settings are required for the Market2 datahome:

```
SRP# add config data-home 2 name Regional1 display-name Regional1 url ssl://1.1.1.1:2507 parent
 National
SRP# add config data-home 6 name Market2 display-name Market2 url ssl://1.0.0.2:2507 parent
Regional1
```

These settings are required for the Market3 datahome:

```
SRP# add config data-home 3 name Regional2 display-name Regional2 url ssl://2.2.2.2:2507 parent
 National
SRP# add config data-home 7 name Market3 display-name Market3 url ssl://2.0.0.3:2507 parent
Regional2
```

These settings are required for the Market4 datahome:

```
SRP# add config data-home 3 name Regional2 display-name Regional2 url ssl://2.2.2.2:2507 parent
 National
SRP# add config data-home 8 name Market4 display-name Market4 url ssl://2.0.0.4:2507 parent
Regional2
```

These settings are required for the Market5 datahome:

```
SRP# add config data-home 4 name Regional3 display-name Regional3 url ssl://3.3.3.3:2507 parent
 National
SRP# add config data-home 9 name Market5 display-name Market5 url ssl://3.0.0.5:2507 parent
Regional3
```

These settings are required for the Market6 datahome:

```
SRP# add config data-home 4 name Regional3 display-name Regional3 url ssl://3.3.3.3:2507 parent
 National
SRP# add config data-home 10 name Market6 display-name Market6 url ssl://3.0.0.6:2507 parent
Regional3
```

2.14 SPB Services Restart

On each SPB server:

1. Set up the spbuser and spbadmin users. Run the CLI command:

   ```
   set config default-user enabled true
   ```

2. Restart the message broker. Run the CLI command:

   ```
   SRP> restart service message-broker
   ```

3. Restart the application server. Run the CLI command:

   ```
   SRP> restart service application-server
   ```

2.15 Verify SPB Services

To verify the system:

1. Check the `/var/log/svlog` for error messages.
2. Run the `show alarms` CLI command.
3. Check the status of the message broker, by running the `show service message-broker status` CLI command.

   The application broker's status should be online.

4. Check the status of the application server, by running this CLI command:

   ```
   SRP> show system services
   ```

A similar output should appear:

```
Name                        AdminStatus OperStatus
--------------------------- ----------- ----------
JBoss Application Server    [up]        [online]
```

3

Customized configurations

3.1 Centralized Configuration

Centralized configuration reduces complexity when managing multiple Sandvine elements. Centralized files are easier to maintain and ensure that all elements are configured with the same variables.

A centralized rc.conf file may reside on an FTP or HTTP/HTTPs server and is pushed out to all the elements when any of the main services are restarted. When you update the centralized rc.conf file, you must also reload or restart the appropriate processes on all Sandvine elements in order for changes to take effect. Any configurations in the local rc.conf file that are below the command to fetch the centralized rc.conf file will override the configurations in the centralized file.

3.1.1 Setting up Centralized Configuration

To set up centralized configuration

Pre-requisite:

Centralized configuration requires a File Transfer Protocol (FTP) or Hypertext Transfer Protocol (HTTP/HTTPS) server.

1. Create an SPB configuration file on an FTP or HTTP/HTTPS server. The name of the file should reflect the function of the file - SPB_central_rc.conf where SPB is the name of the SPB.

2. In the CLI configuration mode enter:

   ```
   SRP# set config files remote-config <url>
   ```

   Where <url> is the path to the remote configuration file.

3. Commit the changes:

   ```
   SRP# commit
   ```

Post-requisite: The created files are populated later in the configuration process.

3.2 Subscriber IP Mapping Configurations

SPB supports mapping subscribers to both IPv4 and IPv6 addresses.

IPv4 addresses can be dynamically mapped based on DHCP or RADIUS within the SPB. IPv6 addresses are dynamically mapped by the SDE platform which receives the IPv6/IPv4 DHCP or RADIUS data and sends the subscriber mappings to the SPB for provisioning. For further information on dynamic mappings for IPv6 consult the SDE documentation on configuring DHCP/RAIDIUS for the SPB.

Sandvine also provides a PopulateSubIpMap script, used to load a static subscriber-IP map, which is suitable for lab or test environments.

3.2.1 Expressing IP Addresses

IP addresses are expressed as fixed IP addresses or with a prefix using CIDR notation for either IPv4 or IPv6 addresses.

Some of the different formats of IP addresses that the SPB supports for its subscriber mappings are:

IP type	Format	Example
IPv4, fixed	A.B.C.D	1.0.0.0
IPv4, prefix	A.B.C.D/E	1.0.0.0/20
IPv6, fixed	A:B:C:D:E:F:G:H	2001:0db8:85a3:0000:0000:8a2e:0370:7334
IPv6, prefix	A:B:C:D:E:F:G:H/I	2001:0db8:85a3:0000:0000:8a2e:0370:7334/64
IPv6, leading zeros	A:B:C:D:E:F:G:H - leading zeros are not required on one or all octets	2011:db8:aaaa:bbbb:cccc:dddd:e:1 is functionally equivalent to 2011:db8:aaaa:bbbb:cccc:dddd:000e:0001
IPv6, zero compression	A:B:C::D - using "::" indicates one or more groups of 16 bits of zeros	2011:db8::1 is functionally equivalent to 2011:0DB8:0000:0000:0000:0000:0000:0001

3.2.1.1 Longest prefix matching

IP address look ups take into account that the IP address may contain a prefix and not be an exact match to the IP address being looked up. The SPB looks up IP addresses using longest prefix matching where a specific IP address may be represented by a more general IP address that is mapped with a prefix. Longest prefix matching is applicable to either IPv4 or IPv6 addresses that make use of the CIDR notation prefix. For example, a mapped address of 1.0.0.0/16 will be retuned for lookups by any of the specific IP addresses in the range of 1.0.0.0 to 1.0.255.255.

3.2.1.2 Overlapping IP address

Because of prefixes on IPv4 and IPv6 addresses, it is possible that various assignments or unassignments will result in more than one address overlapping each other. SPB does not support overlapping IP addresses and the IP mappings will be adjusted to handle this event.

This table illustrates some of the various scenarios involving an overlapping IP address. In each example below the initial state is Sub1 is currently mapped to 1.0.0.0/16.

Scenario	Input	Actions performed	Final state
IP within the range assigned	Assign Sub1 -> 1.0.0.1	Unassign Sub1 -> 1.0.0.0/16 Assign Sub1 -> 1.0.0.1	Sub1 -> 1.0.0.1
Smaller prefix range assigned	Assign Sub1 -> 1.0.0.0/20	Unassign Sub1-> 1.0.0.0/16 Assign Sub1 -> 1.0.0.0/20	Sub1 -> 1.0.0.0/20
Reassignment with same subscriber & IP address	Assign Sub1 -> 1.0.0.0/16	N/A	Sub1 -> 1.0.0.0/16
Larger prefix range assigned	Assign Sub1 -> 1.0.0.0/10	Unassign Sub1 -> 1.0.0.0/16 Assign Sub1 -> 1.0.0.0/10 □	Sub1-> 1.0.0.0/10
IP within the range assigned to another subscriber	Assign Sub2 -> 1.0.0.1	Unassign Sub1-> 1.0.0.0/16 Assign Sub2 -> 1.0.0.1	Sub2 -> 1.0.0.1
Smaller prefix range assigned to another subscriber	Assign Sub2 -> 1.0.0.0/20	Unassign Sub1-> 1.0.0.0/16 Assign Sub2 -> 1.0.0.0/20	Sub 2 -> 1.0.0.0/20
Prefix assigned to another subscriber	Assign Sub2 -> 1.0.0.0/16	Unassign Sub1 -> 1.0.0.0/16 Assign Sub2 -> 1.0.0.0/16	Sub 2 -> 1.0.0.0/16
Larger prefix range assigned to another subscriber	Assign Sub2 -> 1.0.0.0/10	Unassign Sub1 -> 1.0.0.0/16 Assign Sub2 -> 1.0.0.0/10	Sub2 -> 1.0.0.0/10

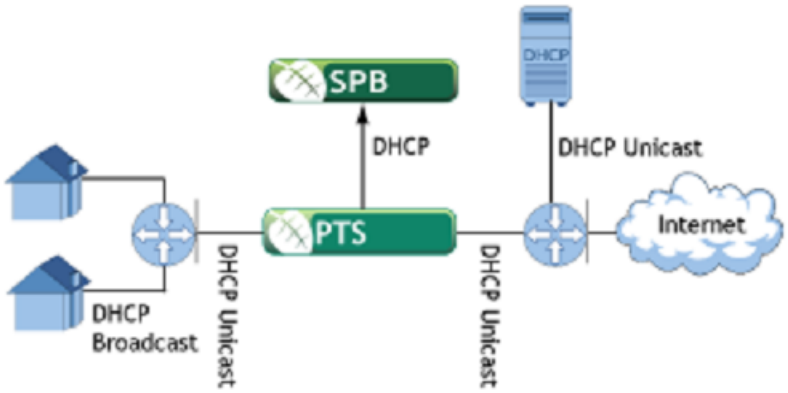
Scenario	Input	Actions performed	Final state
Smaller range unassigned	Unassign Sub1 -> 1.0.0.1 □	Unassign Sub1 -> 1.0.0.0/16	---

3.2.2 SPB - DHCP IP Mapping Overview (IPv4 Only)

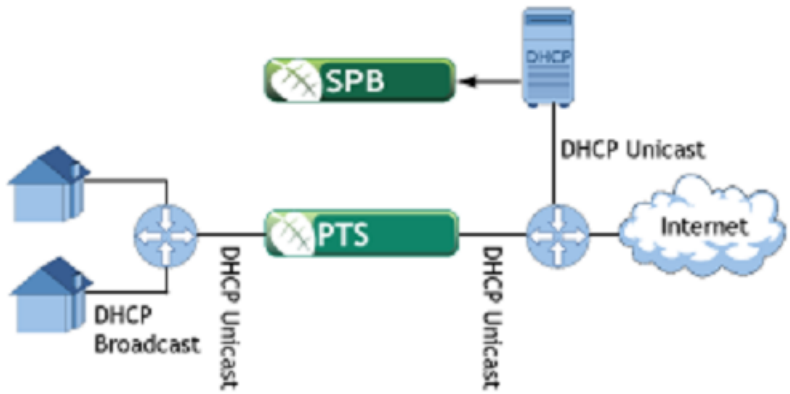
In the DHCP subscriber-IP mapping option, a module on the SPB server processes packets of Dynamic Host Configuration Protocol (DHCP), acknowledges packets, extracts the subscriber information, and maps the subscriber to their IP.

The PTS may run a DHCP packet-forwarder which performs a tee copy on the DHCP packets. For more information on configuring the tee operation on the PTS, refer to the *PTS SandScript Configuration Guide*.

Since the PTS and the SPB are not Layer 2 adjacent, the messages must be encapsulated and forwarded to the destination IP. An example of DHCP sniffing on a PTS deployment is:



In this next example, a network tap or Switched Port Analyzer (SPAN) copies DHCP packets directly to the SPB. The SPB parses the DHCP packets in the same manner as the previous example. This is an example of a DHCP network tap, or a SPAN deployment:



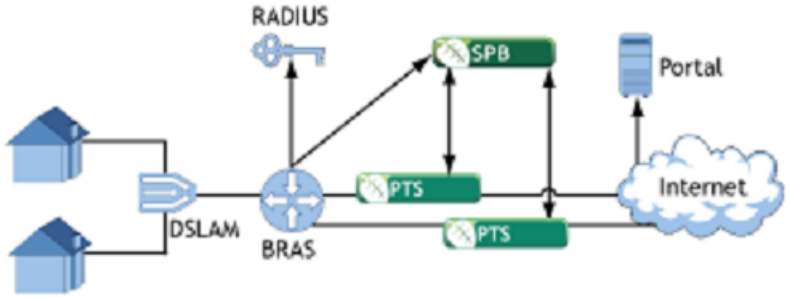
3.2.3 SPB - RADIUS IP Mapping Overview (IPv4 Only)

RADIUS accounting records are used to map subscribers to IPs.

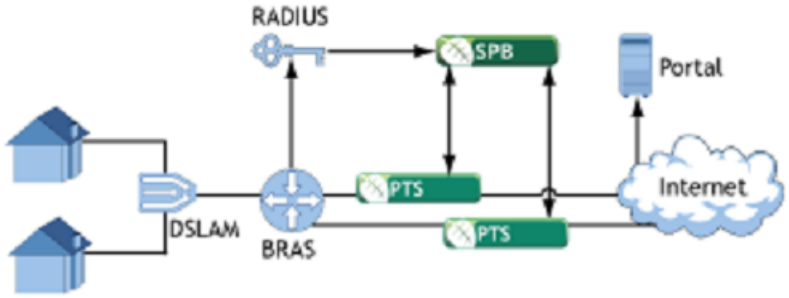
The RADIUS subscriber-IP mapping method utilizes a Sandvine script to listen for Remote Authentication Dial-In Service (RADIUS) accounting records in order to extract the Framed-IP-Address and User-Name attribute fields (per RFC 2865).

RADIUS accounting records and authentication requests contain fields that provide information about the subscriber such as their IP address, username, NAS port, NAS port type and so forth. Sandvine can map these RADIUS attributes to the subscriber-enabling SandScript in our solution.

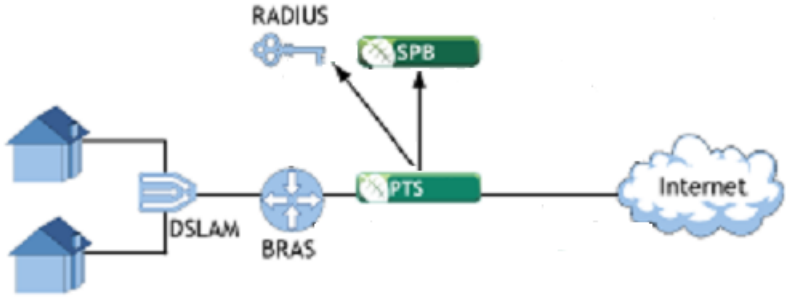
A Network Access Server/Broadband Remote Access Server (BRAS/NAS) replication deployment echoes accounting information to the Sandvine application on the SPB, in addition to the existing primary and secondary RADIUS servers. A “with reply” replication mode is also possible where the SPB will reply with RADIUS response messages to RADIUS request messages. With the reply mode, the SPB acts as the end of a RADIUS proxy chain. An example of a BRAS RADIUS replication deployment is:



This next example illustrates a RADIUS server replication deployment. This deployment is essentially the same as the previous example except that RADIUS performs the replication to the SPB. An example of a RADIUS server replication deployment is:



In a PTS sniffing deployment, the PTS sniffs the RADIUS packets and then forwards them to the SPB. An example of a PTS sniffing deployment is:

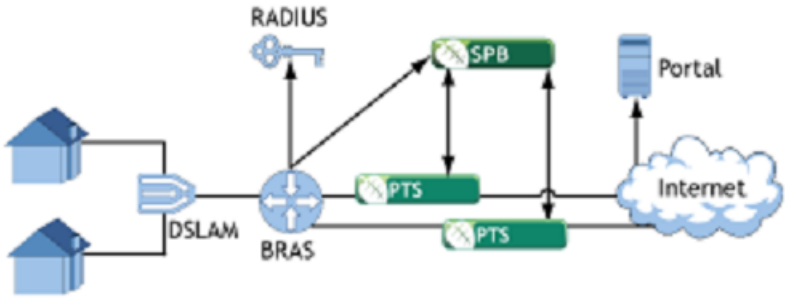


3.2.4 SDE IP Mapping Overview (IPv6 and IPv4)

IPv6 data can be dynamically mapped using the SDE platform to parse the DHCP/RADIUS traffic for either IPv4 or IPv6.

The parsed mappings are then forwarded to the SPB for storage to accommodate queries and reports on subscriber-based data. The SPB notifies all connected elements of changes to the subscriber state to ensure that subscriber state is consistent across the elements.

This example illustrates a RADIUS server replication deployment, where the RADIUS performs the replication to the SDE. The SDE performs the IPv4/IPv6 mappings from RADIUS and forwards the subscriber provisioning to the SPB, the SPB processes the provisioning and notifies the PTS of the changes to the mappings.



3.2.5 General Configuration for SPB RADIUS/DHCP

Configuration is a multi-step procedure.

1. On the SPB, configure required variables.
2. Configure the Network Access Server (NAS) to broadcast to the existing DHCP or RADIUS servers and the SPB. Or configure the PTS to forward packets to the SPB.

3.2.5.1 Minimal IP Mapping Configuration

This is the minimum configuration to enable DHCP or RADIUS subscriber to IP mapping.

1. Run this command to put the CLI into configuration mode:

   ```
   configure
   ```

2. Run these commands to set the ports that the SPB will use to listen for DHCP or RADIUS packets:
   - `SRP# add config service ip-user-map dhcp interface "PORT_1 67"`
   - `SRP# add config service ip-user-map dhcp interface "PORT_1 68"`
   - `SRP# add config service ip-user-map radius interface "PORT_1 1813"`

3. Run this command to enable mapping:

   ```
   set config service ip-user-map enabled true
   ```

4. Run one of these commands to specify RADIUS or DHCP:

- `SRP# set config service ip-user-map dhcp enabled true`
- `SRP# set config service ip-user-map radius enabled true`

5. After you have completed your configuration, run this command to commit the changes:

   `commit`

   Committing the commands for RADIUS requires a restart.

6. To verify the configuration run the `show service ip-user-map config` CLI command.

3.2.5.2 Configuring IP Mapping Failover

Whenever there is a failure in IP mapping service, the failover process is triggered automatically.

Pre-requisite:

These configurations must be in place:

- IP address redundancy must be configured. See *Configuring Multiple Virtual IPs* on page 74
- Subscriber-IP mapping service must be enabled. See *Minimal IP Mapping Configuration* on page 53

1. Run this command to put the CLI into configuration mode:

   `configure`

2. Configure a unique virtual host using this command:

```
SRP#  add config virtual-host <int:0..255> ipv4-subnet <ipv4-subnet> interface <interface>
 priority <int:0..255> heartbeat-interval <int:1..30> master-script <file-path> backup-script
 <file-path>
```

   Where:

Attribute	Description
virtual-host	The virtual-host ID.
ipv4-subnet	An IPv4 subnet, in the form x.x.x.x/xx. For example, 10.10.10.10/01.
interface	The name of the interface corresponding to the external IP address configured for the server. For example, mgmt2.
priority	A priority in the range 0 - 255. A value of 255 indicates the default master and a value < 255 indicates a backup.
heartbeat-interval	The interval, in seconds, that the host sends heartbeat messages to other cluster members. Members consider the master to have failed at three times the configured number of seconds.
master-script	A script to execute when the node takes over mastership.
backup-script	A script to execute when the node loses mastership.

   And the file path to the scripts are:

```
/usr/local/sandvine/bin/ipmapper_masterscript.sh
/usr/local/sandvine/bin/ipmapper_backupscript.sh
```

3. To configure failover, run these commands:

```
SRP# set config service ip-user-map failover enabled true
SRP# set config service ip-user-map failover virtual-host-id 1
SRP# set config service ip-user-map failover script /usr/local/sandvine/bin/vrrp_ctrl.sh
```

Note:
If you used the previous add commands in the minimal IP mapping configuration task, you need to delete them before adding these interfaces. The commands to run are:

```
SRP# delete config service ip-user-map dhcp interface <row>

SRP# delete config service ip-user-map radius interface <row>
```

4. Modify the RADIUS or DHCP physical interface to use the virtual IP address.

   If, for example, the virtual IP were 2.0.0.9, the configuration could be:

```
SRP# add config service ip-user-map dhcp interface "2.0.0.9 68"
SRP# add config service ip-user-map radius interface "2.0.0.9 1813"
```

5. After you have completed your configuration, run this command to commit the changes:

```
commit
```

   Committing these changes requires a restart.

6. Beginning with the master SPB, run this command on each SPB:

```
set service ip-redundancy join-cluster
```

3.2.5.3 Configuring a PTS to Tee DHCP or RADIUS to the SPB

A PTS can tee DHCP or RADIUS traffic to the SPB.

These are examples of SandScript that you can add to the PTS by editing `/usr/local/sandvine/etc/policy.conf`. The policy.conf file contains SandScript rules and actions. If SandScript's policy.conf does not exist, make a copy of the sample SandScript file available on each PTS element (/usr/local/sandvine/etc/policy.conf.sample) and edit the copy. Note that in the examples:

- the SPB running IP Mapper has IP address 3.0.0.2
- the DHCP traffic is on port 67 and 68
- the RADIUS traffic is on port 1813

To tee DHCP:

```
destination "ipusermap" ipmap mode ip_rewrite ip 3.0.0.2
if (client udp_port 67-68 or server udp_port 67-68) then \
  tee from client destination "ipusermap" and \
  tee from server destination "ipusermap"
```

To tee RADIUS:

```
destination "ipusermap" ipmap mode ip_rewrite ip 3.0.0.2
if (client udp_port 1813 or server udp_port 1813) then \
  tee from server destination "ipusermap" and \
  tee to server destination "ipusermap"
```

For additional information on teeing to a destination, refer to the *PTS SandScript Configuration Guide* for this release.

3.2.5.4 Configuring DHCP Options or RADIUS Attributes to Subscriber Attribute Mapping

The values of DHCP options or header fields or RADIUS attributes can be mapped to subscriber attributes in order to use them as conditions in SandScript.

Subscriber attributes are defined in configuration files on the PTS and they are automatically propagated to the SPB when you run the svreload command. See the *PTS SandScript Configuration Guide* for more information on subscriber attributes and configuring the `policy.conf` file.

Use this procedure for mapping either DHCP (see *SPB - DHCP IP Mapping Overview (IPv4 Only)* on page 51) or RADIUS (see *SPB - RADIUS IP Mapping Overview (IPv4 Only)* on page 51).

1. On the PTS:
   a. Edit `/usr/local/sandvine/etc/policy.conf` and declare the subscriber attribute.

      For DHCP:

      ```
      attribute "dhcp_attr" type string
      ```

      For RADIUS:

      ```
      attribute "calling_station_id" type string
      ```

   b. To create this attribute definition, run the `svreload` command.

2. On the SPB, run this command to put the CLI into configuration mode:

   ```
   configure
   ```

3. Run these commands.
   - For DHCP:

     ```
     SRP# add config service ip-user-map dhcp attribute-mapping "224 dhcp_attr"
     ```

   - For RADIUS:

     ```
     SRP# add config service ip-user-map radius attribute-mapping "31 calling_station_id"
     ```

4. After you have completed your configuration, run this command to commit the changes:

   ```
   commit
   ```

3.2.6 DHCP Configuration Examples

These are common DHCP configuration examples.

3.2.6.1 Configuring the Subscriber MAC Address to Come From the Client Hardware Address

The default location of the subscriber ID (MAC address) in the DHCPACK packet is Option 82, Agent Remote ID sub option. To extract the subscriber ID from the client hardware address (chaddr), in CLI configuration mode run these commands:

```
SRP# set config service ip-user-map dhcp subscriber-identifier mode cpe-mac
SRP# commit
```

3.2.6.2 DHCP Header Fields

DHCP header fields are configured in CLI in the same way as DHCP options. The supported DHCP header fields are:

```
ci_addr
yi_addr
si_addr
gi_addr
ch_addr
server_host_name
boot_file
```

For example:

```
SRP# add config service ip-user-map dhcp attribute-mapping "<dhcp_header_field>
<subscriber_attribute>"
```

3.2.6.3 DHCP Bootfile Mapping

You may specify the source of the subscriber attribute as the static BOOTP 'bootfile name' field or the DHCP Option 67, or one of the two with priority if both exists. To set the attribute, run this command:

```
set config service ip-user-map dhcp boot-file source
```

The options are:

Option	Description
NONE	Turns off this feature.
FILENAME_ONLY	Uses only the static BOOTP 'bootfile name' field.
OPTION_67_ONLY	Uses only the DHCP option 67 field.
FILENAME_FIRST	Uses the static BOOTP 'bootfile name' field first. If it is empty (after regex/formatting, if used), uses the DHCP option 67 field.
OPTION_67_FIRST	Uses the DHCP option 67 field. If it is empty (after regex/formatting, if used) or does not exist, uses the static BOOTP 'bootfile name' field. Note that the 'bootfile name' field is not read if it is used for option overloading (that is, if option 52 exists in the packet and is 1 or 3). You can compare the value against a regex and format it. If the value does not match the regex, or if it does but the formatted value is blank, then the attribute is not written.

You can set an optional expiry time using the CLI configuration mode and the command:

```
SRP# set config service ip-user-map dhcp boot-file attribute expiry <time>
```

The expiry is expressed as an offset from mapping time and may be defined as:

```
 infinity|(n days|hours|minutes|seconds [n d|hr|min|sec ...])
```

where the default expiry time is `infinity`.

3.2.7 RADIUS Configuration Examples

These are common RADIUS configuration examples. Committing changes to RADIUS configuration requires a restart.

3.2.7.1 RADIUS Dictionary Files

The SPB uses a set of RADIUS dictionary files to determine the data type of vendor-specific attributes (VSA) for in-coming RADIUS packets. Each dictionary file contains a list of RADIUS attributes and values, which the server uses to map between descriptive names and on-the-wire data. The dictionary files are installed with the SPB-services package and can be found in:

```
/usr/local/sandvine/etc/radius
```

Note:
Modifying Sandvine dictionary files is not supported. Any changes are undone on the next software upgrade.

3.2.7.2 Custom RADIUS Attributes

If a RADIUS attribute is either missing from the Sandvine dictionary files, or has a different data type than the one present in the RADIUS packets, the data type can be manually provided or overridden to ensure that the Sandvine system has proper formatting. You can either configure the RADIUS attribute data type using CLI or add customer-specific RADIUS dictionaries to the path:

```
/usr/local/sandvine/etc/radius/customer/
```

Configuring a Custom RADIUS Attribute

If there are only a small number of RADIUS attributes that need to be customized, use the CLI. You can add new custom RADIUS attributes or you can override the data type of existing RADIUS attributes in dictionary files. In either case, you must run this command:

```
add config service ip-user-map radius attribute-definition <attribute> type
```

For example:

```
SRP# add config service ip-user-map radius attribute-definition "VSA 9 14" type integer
```

Adding a Dictionary File

If you need to add a large number of custom attributes, perhaps because an entire vendor is needed, then you can add one or more RADIUS dictionary files under the `/usr/local/sandvine/etc/radius/customer/` directory. A dictionary file has this format (based on the FreeRadius dictionary format):

```
VENDOR        <VendorName>    <VendorId>
BEGIN-VENDOR  <VendorName>
ATTRIBUTE     <VendorName>-<AttributeName>    <AttributeValue>    <Attribute-DataType>
VALUE         <VendorName>-<AttributeName>    <ValueName>         <ValueNumber>
END-VENDOR    <VendorName>
```

This is an example of a dictionary file for the Airespace vendor. For more examples refer to dictionary.* files installed under the `/usr/local/sandvine/etc/radius/` directory.

```
VENDOR       Airespace                 14179
BEGIN-VENDOR Airespace
ATTRIBUTE    Airespace-Wlan-Id          1       integer
ATTRIBUTE    Airespace-QOS-Level        2       integer
ATTRIBUTE    Airespace-DSCP             3       integer
ATTRIBUTE    Airespace-8021p-Tag        4       integer
ATTRIBUTE    Airespace-Interface-Name   5       string
ATTRIBUTE    Airespace-ACL-Name         6       string

VALUE   Airespace-QOS-Level           Bronze              0
VALUE   Airespace-QOS-Level           Silver              1
VALUE   Airespace-QOS-Level           Gold                2
VALUE   Airespace-QOS-Level           Platinum            3
VALUE   Airespace-QOS-Level           Uranium             4

END-VENDOR Airespace
```

3.2.7.3 Configuring IP Mapper in RADIUS Proxy Mode

If a RADIUS server forwards accounting packets to the SPB, you can configure the SPB to send Accounting-Response packets in acknowledgment. You must also configure the RADIUS secret to enable this feature.

In this example, IP Mapper accepts accounting packets on two different UDP ports (1646 and 1813), each of which is configured with a different RADIUS shared secret key to use when constructing reply packets.

```
SRP# set config service ip-user-map radius accounting reply true
SRP# add config service ip-user-map radius interface "PORT_1 1646" shared-secret "secret1"
SRP# add config service ip-user-map radius interface "PORT_2 1813" shared-secret "secret2"
```

3.2.7.4 RADIUS Representation in the Sandvine System

The Sandvine system stores RADIUS attribute values as a string. The RADIUS data types (per RFC 2865) are represented as:

Data type	Format	Example
Text	UTF-8 string representation	“abcd”
String	ASCII hexadecimal representation	“FFFFFFFF”
Integer	ASCII decimal representation	“4660”
IP address	Dotted decimal notation	“1.2.3.4”
Vendor specific attribute (VSA)	If the VSA is in the RADIUS dictionary, the format is specified in the dictionary. Otherwise, this data type uses the ASCII hexadecimal format (see `/usr/local/sandvine/etc/radius`).	If the attribute is an IP address, the data type follows the standard IP format (1.2.3.4). If there is a dictionary entry, the data type in the dictionary specifies the format. Otherwise, the data type uses the ASCII hexadecimal format `01020304`.

3.2.8 SDE Mapping Configuration

SandScript on the SDE manages the configuration for mapping DHCP/RADIUS traffic.

Once the SDE is configured to map DHCP/RADIUS and communicate to the SPB, by default the SPB is setup to listen for mapping messages that are sent from the SDE. See the *Subscriber Mapping User Guide* for further details.

3.2.8.1 Cache Miss Notification

Cache miss notifications allow the SPB to send requests back to the SDE in the event of an unmapped subscriber on the SPB. If the SPB receives a lookup request for a subscriber that is unknown to the SPB, with this option enabled the SPB sends a cache miss notification to the SDE, which triggers the SDE to re-send any mapping information for the subscriber.

To enable/disable this feature on the SPB, in CLI configuration mode run:

```
SRP# set config service subscriber-provisioning cache-miss notifications enabled <true|false>
```

then run this command to commit your changes:

```
commit
```

3.2.9 The PopulateSubIpMap Script

If an existing database containing session qualifier and subscriber-IP information is not available, you can create a text file containing this information and use the file to populate the subscriber-IP and subscriber-attribute maps in the database.

Populating the database with a text file is appropriate in a lab or testing environment. The general steps to follow are:

1. On the SPB, create a text file containing the session qualifier values, subscriber-IP IDs and Subscriber-Attribute data (file can be either UNIX or Windows format).
2. On the SPB, execute the PopulateSubIpMap script with the appropriate arguments to populate the system with the subscriber information.

The PopulateSubIpMap script can also provision NAT mappings.

3.2.9.1 PopulateSubIpMap Script Information

A text file is used to identify session qualifier values, subscriber-IP and Subscriber-Attribute mappings. On the SPB, you can create a text file or you can edit the sample file that is provided (`/usr/local/sandvine/tcl/tools/PopulateSubIpMap/sample_sub_ip_map.txt`). This sample file also provides additional information on correct syntax.

You can map each IP qualified by a site number to a given subscriber name. If a subscriber name is not specified, the PopulateSubIpMap script uses the IP address string as the subscriber name. IP-subscriber mappings can exist in multiple files.

Note:
- The file should contain one IP-address subscriber name per line.
- The same subscriber can have multiple IPs assigned.
- The same IP cannot be assigned to multiple subscribers. Any existing subscriber-IP mappings found in the database for any IP specified in the file are removed and replaced. Therefore, if there are multiple entries in the file with the same IP specified, the last entry for that IP in the file is applied.

Each subscriber-IP entry qualified by a site number is entered as:

```
== site <site-number>
<IP_ADDRESS> [SUB_NAME] :=<OPTIONS_LIST>
```

Each NAT mapping entry qualified by a site number is entered as:

```
== site <site-number>
NAT <PRIVATE_IP_ADDRESS> <PUBLIC_IP_ADDRESS> <LOW_PORT> <HIGH_PORT>
```

Where:

- == – these characters without the site number indicate that the default value of "0" is used for the session qualifier.
- site-number – is the site number used to qualify the IP assignments that follow.
- IP_ADDRESS – is an IPV4 or IPV6 address (or range of addresses).
- SUB_NAME – subscriber name is taken as all characters found on a line after IP_ADDRESS.
- OPTIONS_LIST – is an optional comma-separated list of options to be applied to the subscriber.
- PRIVATE_IP_ADDRESS – is an IPV4 or IPV6 address.
- PUBLIC_IP_ADDRESS – is an IPV4 address.
- LOW_PORT – is the low port of a NAT mapping port range.
- HIGH_PORT – is the high port of a NAT mapping port range.

Note:
Specifying `== site <site-number>` is optional. If this line is not present, the default value of "0" is used for the session qualifier.

For example:

```
1.2.3.0
1.2.3.1 unique1@sandvine.com
1.2.3.2 unique2@sandvine.com
1.2.3.3 unique3@sandvine.com
1.2.3.20/30 Special Addresses
2001:0DB8:85A3:0000:0000:8A2E:0370:7334 unique4@sandvine.com
      21DA:D3:0:2F3B::/64 unique5@sandvine.com

== site 123
1.2.3.4 unique6@sandvine.com
1.2.3.5 unique7@sandvine.com
1.2.3.6 unique8@sandvine.com

==
1.2.3.7 unique9@sandvine.com

1.2.3.8 unique10@sandvine.com := set_attribute captive=true

== site 123
NAT 1.2.3.9 10.0.0.1 1000 2000
```

This creates:

- One IP address (1.2.3.0) with the IP string as the subscriber's name "1.2.3.0". The default value of session qualifier "0" is used.
- Three IP addresses (1.2.3.1 through 1.2.3.3) mapped to subscribers with names "unique1@...." to "unique3@...." respectively. The default value of session qualifier "0" is used.
- Four IP addresses (1.2.3.20 through 1.2.3.23) all mapped to one subscriber with name "Special Addresses". The default value of session qualifier "0" is used.
- One IP address (2001:0DB8:85A3:0000:0000:8A2E:0370:7334) mapped to one subscriber with name "unique4@sandvine.com". The default value of session qualifier "0" is used.
- One IP address (21DA:00D3:0000:2F3B:0000:0000:0000:0000/64) mapped to one subscriber with name "unique5@sandvine.com". The default value of session qualifier "0" is used.
- Three IP addresses (1.2.3.4 through 1.2.3.6) mapped to subscribers with names "unique6@...." to "unique8@...." respectively. Site number 123 is used as the session qualifier value.
- One IP address (1.2.3.7) mapped to subscriber with name "unique9@sandvine.com". The default value of session qualifier "0" is used.
- One IP address (1.2.3.8) mapped to subscriber with name "unique10@sandvine.com" with the "captive" attribute set to "true". The default value of session qualifier "0" is used.
- One private IP address (1.2.3.9) mapped to a public IP address (10.0.0.1) with a low port of "1000" and a high port of "2000". Site number 123 is used as the session qualifier value.

Note:
With the `-useV4CidrNotation` option, instead of creating four IP addresses 1.2.3.20 through 1.2.3.23, only one address is created which is 1.2.3.20/30. Example

```
10.16.0.0/16
```

Without the `-useV4CidrNotation` option, this creates 10.16.0.0 through 10.16.255.255, each mapped to subscribers with name equal to the IP address. (10.16.0.0 -> '10.16.0.0', 10.16.0.1 -> '10.16.0.1' ... 10.16.255.255 -> '10.16.255.255'). With the `-useV4CidrNotation` option, this creates one IP address, 10.16.0.0/16, mapped to the subscriber '10.16.0.0/16'.

3.2.9.2 Setting Subscriber-Attributes

To set subscriber attributes, add the `set_attribute` variable to the end of the IP map line. You can use a comma-separated list to set multiple attributes at one time.

```
1.2.3.1 unique1@sandvine.com :=set_attribute
"attr_name"="attr_value",set_attribute
"attr_name2"="attr_value2"
```

For example, a single IP entry is mapped to one subscriber with a “captive” attribute set to “true”.

```
 1.2.3.4 subscriber@sandvine.com :=set_attribute "captive"="true"
```

A single IP entry is mapped to a default subscriber name with a “captive” attribute set to “true”.

```
1.2.3.8 :=set_attribute "captive"="true"
```

A range of IPs (subsets) are mapped to one subscriber name with both “captive” and “abuser” attributes set to “true”.

```
1.2.3.20/30 subscriber@sandvine.com :=set_attribute “captive”=”true”, set_attribute
“abuser”=”true”
```

3.2.9.3 Executing the PopulateSubIpMap script

The `PopulateSubIpMap` script populates subscriber state information (subscribers, subscriber-IP assignments and subscriber-attribute assignments) via the SubscriberServices SPB module. The `PopulateSubIpMap` script options are:

Option	Description
-n,--host	The host name. Default is localhost.
-u,--user	The SPB username.
-p,--password	The password for the username specified.
-disableNotification	Disables change notifications while work is being performed. Change notifications are re-enabled later. Disabling change notification significantly reduces the time to process a large set of mappings and is usually appropriate for a one-time population.
-f filename	The subscriber-IP map file to parse. You can specify multiple files if subscriber-IP map is broken up. To do this, simply list all files. For example: -f file1 file2 ...fileN.
-h, --help	Displays basic help information.
-noprompt	Disables prompting.
-silent	Does not print progress messages to console.
-useV4CidrNotation	Appends CIDR Notation to IPV4 IP addresses.

To run the script on the SPB servers, use this command:

```
 PopulateSubIpMap -f filename -n hostname -u user -p password
```

Note that you must run this command as an administrative user. The default username is spbadmin and the default password is sandvine.

3.2.10 Verifying Subscriber IP Mapping Configuration

After configuring the system, verify that it is functioning correctly.

- To verify the mappings where the SPB directly parses the DHCP or RADIUS, confirm the correct configuration and processing using this CLI command:

  ```
  show service ip-user-map config
  ```

  The command displays general information common to both DHCP and RADIUS, followed by your specific settings for DHCP and RADIUS.
- To verify that mappings successfully occur from DHCP or RADIUS, use this CLI command:

  ```
  show service ip-user-map stats
  ```

  When packets are successfully mapped, the LoginRate and LogoutRate output shows the current rates of assignment and unassignment that the SPB currently processes.
- To verify the mappings where the SDE parses DHCP or RADIUS, confirm the correct configuration and processing using this CLI command:

  ```
  show service subscriber-provisioning config
  ```
- To verify that mappings successfully occur from the SDE, use this CLI command:

  ```
  show service subscriber-provisioning stats
  ```

  When packets are successfully mapped, the TotalLoginCount and TotalLogoutCount output increases based on the assignments and unassignments of the mappings received from the SDE.

3.2.11 Verifying Session Qualifiers on the SPB

For a few known currently-active subscribers, run one of these commands and verify that the subscriber information is accurate compared to the PTS.

```
show subscriber name <subscriber-name>
show subscriber ip <ip-address> site-number <site-value>
```

3.3 Top Talkers

Top Talkers are those subscribers who use their bandwidth the most.

One instance of the Top Talkers processing agent runs per database to identify and quantify subscribers by bandwidth usage. You can configure the number of top talkers to identify and the interval of identification using these CLI commands in configuration mode:

```
SRP# set config service top-talker enabled true
SRP# set config service top-talker policy-file <path>
SRP# set config service top-talker schedule <schedule>
```

Run this CLI command for the changes to take effect:

```
commit
```

Note:
To use Top Talkers, enable subscriber IP mapping. Refer to the *SPB CLI Reference Guide* for additional information.

3.3.1 Top Talkers Policies

The Top Talkers search uses a specific SandScript that consists of two parts: a single condition and an AND-separated action list.

Top Talker SandScript policies do not support multiple conditions in one rule. The Top Talkers search can only use the "find top …" or "find over …" condition and the “set subscriber attribute” action. For detailed information on SandScript syntax, refer to the *PTS SandScript Configuration Guide*.

The Top Talkers search is based on the total bytes transferred. It is not intended to be used for instantaneous measurement, but rather for finding long-term use. Carefully consider the duration over which the “find top …” condition is implemented. For example, “find top … for 7 days” identifies subscribers using resources extensively full-time, rather than subscribers who may be using resources extensively for a single day.

You can perform any number of top *n* searches based on different criteria (such as upload/download) and time ranges. Each of these criteria set a different attribute, or sets of attributes, equal to a value and the length of time for which the attribute is active. The times for subscriber tracking depend on the times for the subscriber attribute: you can set an attribute to automatically expire after a certain amount of time or to never expire.

Note:
Missing subscriber attribute definitions in the Top Talker policy are logged in the jboss log.

On the application server where Top Talkers is configured, create a SandScript file that specifies how to identify Top Talkers.

3.3.2 Top Talkers SandScript Syntax Without Classifiers

Classifiers are used to apply labels to SandScript contexts such as flows or subscribers and to categorize flows or subscribers into meaningful groups. The maximum number of subscriber classifiers that can be used is 38. Of that number, 32 can be a sum and 6 can be used to report the maximum value over the past 12 hours. Beyond these values, the number of active subscribers is reduced by half.

With extended classifiers, the maximum number of subscriber classifiers that can be used is 76, of which 64 can be a sum and 12 can be used to report the maximum value over the past 12 hours.

Top Talkers SandScript that does not use classifiers provides concise information. For detailed information, see *Top Talkers Syntax using Classifiers* on page 66.

3.3.2.1 Condition Syntax

The condition syntaxes to define the SandScript are:

```
find top <count>{%} {uploaders|downloaders} for <interval> {cluster "<clustername>"}
find over <size>{KB|MB|GB} {upload|download} for <interval> {cluster "<clustername>"}
```

Parameter	Description
count	A positive integer (such as 1000) or a positive percentage (such as 3%).
size	A positive integer (such as 1000) with a unit of KB, MB, or GB.
uploaders or downloaders	Optionally specify either uploaders for the amount of uploaded bytes or downloaders for the number of downloaded bytes. If neither is specified, the default is the total (uploaded + downloaded) bytes.
upload or download	Optionally specifies the amount of uploaded or downloaded bytes. If neither is specified, the default is the total (upload + download) bytes.
interval	Whole number of days (such as 7 days) or whole number of hours (such as 48 hours).

Parameter	Description
cluster	Optionally specify a cluster name. If one is not specified, all clusters are assumed. The cluster specification limits the search to statistics for a specific cluster of Sandvine elements.

3.3.2.2 Action Syntax

Top Talkers perform a single `set_attribute` action, which is used to tag a subscriber with an attribute.

```
set_attribute {client|server} "<name>" = "<value>" {for interval}
```

Parameter	Description
client or server	Optionally specify either client (the attribute is set on the client side of the flow) or server (the attribute is set on the server side of the flow). If not specified, the attribute is set on both the client and server.
name	The name of the attribute.
value	The value to assign to the attribute.
interval	Whole number of days (such as 7 days) or whole number of hours (such as 48 hours), minutes or seconds. The default is infinite. The attribute expires after the specified interval.

For example:

- This rule identifies the top ten subscribers based on uploaded bytes for seven days and then sets the “abuser uploader” attribute to “true” for 14 days.

  ```
  if find top 10 uploaders for 7 days then \
  set_attribute "abuser_uploaders"="true" for 14 days
  ```

- This rule identifies the top ten subscribers in Region_A based on uploaded bytes for seven days, then sets the “abuser uploader” attribute to “true” for 14 days.

  ```
  if find top 10 uploaders for 7 days cluster "Region_A" then \
  set_attribute "abuser_uploaders"="true" for 14 days
  ```

- This rule identifies the top 10% of subscribers based on downloaded bytes for the past twelve hours. Two attributes are set, both of which expire in five hours.

  ```
  if find top 10% downloaders for 12 hours then \
    set_attribute "abuser_downloaders"="true" for 5 hours
  if find top 10% downloaders for 12 hours then \
    set_attribute "search_type"="percent" for 5 hours
  ```

- This rule identifies subscribers who uploaded more than 10 GB over a period of seven days and then sets the “abuser uploader” attribute to “true” for 14 days.

  ```
  if find over 10GB upload for 7 days then \
  set_attribute "abuser_uploaders"="true" for 14 days
  ```

- This rule identifies subscribers in Region_A who uploaded more than 10 GB over a period of seven days, then sets the “abuser uploader” attribute to “true” for 14 days.

```
if find over 10GB upload for 7 days cluster "Region_A" then \
set_attribute "abuser_uploaders"="true" for 14 days
```

- This rule identifies subscribers who downloaded 100 GB over the past twelve hours. Two attributes are set, both of which expire in five hours.

```
if find over 100GB download for 12 hours then \
set_attribute "abuser_downloaders"="true" for 5 hours
if find over 100GB download for 12 hours then \
set_attribute "search_type"="top_downloader" for 5 hours
```

3.3.3 Top Talkers Syntax using Classifiers

SandScript which uses classifiers provides more detailed information based on the defined classifiers. SubscriberClassifiers and customer fields are used in SandScript.

```
if find top <count>[%] field = “<fieldname>” {for “<subscriber classifier>”
{= “<subscriber classifier instance>”}} for interval [cluster “<clustername>”]
```

```
if find over <size>[KB|MB|GB] field = “<fieldname>” {for “<subscriber classifier>”
{= “<subscriber classifier instance>”}} for <interval> [cluster “<clustername>”]
```

Parameter	Description
count	A positive integer (such as 1000) or a positive percentage (such as 3%).
size	A positive integer (such as 1000) with a unit of KB, MB, or GB.
fieldname	The name of the custom field as defined in the PTS classifiers SandScript.
subscriber classifier	The name of subscriber classifier as defined in the PTS classifiers SandScript. If not specified, all subscriber classifiers are used.
subscriber classifier instance	The name of subscriber classifier as defined in the PTS classifiers SandScript (optional). If not specified, all subscriber classifier instances are used.
cluster	Optionally specify a cluster name. If one is not specified, all clusters are assumed. The cluster specification limits the search to statistics for a specific cluster of Sandvine elements.

For example:

- This rule does not use classifier information.

```
if find top 10 field=”TOTAL_BYTES” for 1 day \
then set_attribute “top_talker_sports”=”true” for 7 days
```

- This rule uses classifier information, in this case, all ZONEs.

```
if find top 10 field=”TOTAL_BYTES” for “ZONE” for 1 day \
then set_attribute “top_talker_sports”=”true” for 7 days
if find over 10GB field=”TOTAL_BYTES” for “ZONE” for 1 day \
then set_attribute “top_talker_sports”=”true” for 7 days
```

- This rule uses a classifier as an instance: use only SPORTS ZONE.

```
if find top 10 field=”TOTAL_BYTES” for “ZONE”=”SPORTS” for 1 day \
then set_attribute “top_talker_sports”=”true” for 7 days
if find over 10GB field=”TOTAL_BYTES” for “ZONE”=”SPORTS” for 1 day \
then set_attribute “top_talker_sports”=”true” for 7 days
```

3.4 Subscriber Attribute Advanced Sizing and Tuning

To optimize performance, you may want to perform advanced sizing and tuning on subscriber attributes.

3.4.1 Properties of Subscriber Attribute Definitions

You can assign an attribute definition one or more of these properties:

- Audited—Changes to an attribute generate logs in the SPB database.
- Reported—Attribute is included in the Subscriber Attribute Archiver process (if active) and is available for queries by Network Demographics reports.
- Visible—Attribute is visible to the entire system including Web Service calls. Attributes that do not have visible enabled are still available for use by internal systems such as the PTS.
- Notifiable—Changes to the attribute trigger a change notification to the PTS elements.
- IP-Notifiable—Dictates whether or not the attribute should be included in IP assignment change notifications.

Enable these properties only if required as they affect the performance of the system, especially for attributes that are large, or when there are a large number of attributes.

To set a property for an attribute definition, use this CLI command:

```
set subscriber attribute-definition attribute <your attribute definition>
[audit|reported|visible|notifiable|ip-notifiable|values] [true|false]
```

You can use the output for the command to verify that the property was set correctly. For example:

```
SRP> set subscriber attribute-definition attribute tier audit true values "gold,silver,bronze"
Name : Tier
IsVisible : false
IsNotifiable: false
IsAudited : true
```

```
IsReported : false
Values : gold, silver, bronze
```

Alternately, you can list the subscriber attribute definitions to see the current properties that are set for all subscriber attributes. For example:

```
SRP> show subscriber attribute-definitions
Name    Audited Reported Visible Notifiable IpNotifiable
------- ------- -------- ------- ---------- ------------
abuser  [true]  [false]  [true]  [true]     [true]
captive [true]  [false]  [true]  [true]     [true]
tier    [true]  [false]  [true]  [true]     [true]
```

3.4.2 Storing Attributes In-Memory

The SPB stores attributes differently depending on their size, determined as length in bytes.

Attributes can have any length up to whatever was defined by this CLI configuration command:

```
set config service subscriber-management cache attributes max-length <int:0..>
```

Experience has shown that attribute values normally fall into one of these categories:

- Minor attributes of perhaps 20-50 bytes
- Major attributes of hundreds of bytes or more

If the length (in bytes) of an attribute value is less than or equal to the value defined by this CLI command, it is stored in-memory in a single minor attribute block:

```
show config service subscriber-management cache attributes minor-length
```

If the length in bytes of the value is greater than this CLI command, the attribute value is stored in memory across one minor attribute block and one or more major attribute blocks:

```
show config service subscriber-management cache attributes minor-length
```

To set the attribute length, run:

```
SRP# set config service subscriber-management cache attributes major-length 5
SRP# commit
```

3.4.3 Default Sizing for Subscriber Attributes

SPB default tuning assumes that the vast majority of attribute values fit into a minor block, with far fewer attribute values requiring one or more major blocks.

The amount of memory used by attributes is proportional to:

```
(spb_maximum_attributes * spb_minor_attribute_length) + (spb_maximum_major_attributes *
spb_major_attribute_length)
```

Each category of attribute can be tuned differently to get the most out of the available memory. The primary sizing parameters for the SPB are:

- Maximum number of subscribers
- Maximum number of subscriber and session attributes
- Maximum number of IP assignments
- Average size of attribute values

A number of other parameters are involved as well. The SPB automatically selects reasonable defaults for tuning and sizing parameters based on the available RAM in the hardware.

To set the default sizing, run:

```
SRP# set config service subscriber-management cache attributes major-memory-blocks <int:0..>

SRP# set config service subscriber-management cache attributes major-length <int:0..>
SRP# commit
```

Note:
Consider the settings for these CLI commands very carefully when tuning. The product of these two numbers is the number of bytes of memory that is dedicated just to major attributes. With millions of subscribers, it is easy to exhaust system memory by setting the cache attributes major-length too aggressively.

The SPB's sizing defaults are:

Parameter	32 GB (SRP 3000-C)	96 GB (SRP 3000-D)
Max Subscribers	40,000,000	80,000,000
Max IP Assignments	40,000,000	80,000,000
Max Attributes (including subscriber and session attributes)	100,000,000	200,000,000
Max Major Attribute Blocks	40,000,000	200,000,000
Minor Attribute Size	20	20
Major Attribute Size	128	128

3.4.4 Adjusting Default Sizing for Subscriber Attributes

In most scenarios, the default SPB settings are sufficient. Some common situations that might need special tuning are described in the following sections.

3.4.4.1 Prior to Upgrading from Release 5.4

A one-time upgrade from the legacy on-disk database to the in-memory database is performed the first time SPB is started in in-memory mode. If sufficient room is not available in memory to import the data from the legacy data, the SPB fails to come online and errors appear in the logs. To prevent this situation, it is recommended that you analyze the legacy database for sizing limits before upgrading from 5.4.

To estimate the current size, run these queries against the pre-upgraded database:

Entity	Query	CLI commands
Subscribers	select count(1) from subscriber;	show config service subscriber-management cache subscribers max <int:0..>
IP Sessions	select count(1) from sub_ip_assignment;	show config service subscriber-management cache subscribers ip-assignments max <int:0..>
Attributes	select count(1) from subscriber_attr_value where expiry_time > current_timestamp;	show config service subscriber-management cache attributes max <int:0..>

Entity	Query	CLI commands
Major Attributes	select sum(ceil((length(value) - 20) /128.0)) from subscriber_attr_value where (expiry_time > current_timestamp or expiry_time is null) and length(value) > 20;	show config service subscriber-management cache attributes major-memory-blocks

If any of these numbers exceed the limits defined by the sizing default of the SPB (see *Default Sizing for Subscriber Attributes* on page 68), adjust the appropriate maximum values. You can view these values using the CLI command:

```
show config service subscriber-management cache attributes max
```

If session attributes are used after the upgrade, ensure the configured maximum attributes are large enough to accommodate the existing subscriber attributes as well as the number of session attributes that are used after the upgrade.

3.4.4.2 In-Memory Database Becomes Full after Running for a Time

Once the in-memory database of the SPB becomes full, it rejects new operations. When this happens, you must increase the SPB maximum values. See *Tuning CLI Commands* on page 151.

3.4.4.3 More Than One Large Attribute Per Subscriber or Session

It is a general expectation that the SPB default tuning is not more than one large attribute (in the range of 20-128 bytes) per subscriber. If a deployment calls for multiple large attributes per subscriber:

1. Enter the configuration mode:

   ```
   configure
   ```

2. Run this command:

   ```
   set config service subscriber-management cache attributes major-memory-blocks <int:0..>
   ```

If large attribute values frequently exceed 128 bytes, then run this command to set a size larger than 128 bytes:

```
set config service subscriber-management cache attributes major-length <int:0..>
```

When configuration is complete, commit the changes:

```
commit
```

3.5 Subscriber Attribute Archiver

The subscriber attribute archiver takes a snapshot of the in-memory attributes and persists them to disk so that they can be used in Network Demographics reports and API requests of subscriber statistics by attribute.

The archiver archives each subscriber attribute where the attribute is marked as reportable. By default, all attributes are reportable. The archived attributes are then available for queries that join against the subscriber statistics.

3.5.1 Scheduling the Subscriber Attribute Archiver

The subscriber attribute archiver runs each day at midnight by default.

To change the default runtime, run the CLI configuration command:

```
set config service attribute-archiver schedule <schedule>
```

Scheduling is set in an expression similar to Unix. The cron expression comprises these required and optional fields, separated by whitespace:

Field meaning	Allowed values	Allowed special characters
seconds	0-59	, - * /
minutes	0-59	, - * /
hours	0-23	, - * /
day-of-month	1-31	, - * / ? L W
month	1-12 or JAN-DEC	, - * /
day-of-week	1-7 or SUN-SAT	, - * / ? L
year (optional)	empty, 1970-2099	, - * /

Note:
- Specifying both the day-of-month and day-of-week is not supported, therefore there must be a “?” in at least one of the two fields.

The special characters used in the scheduling cron expression are:

Character	Meaning	Example	Note
*	All possible values.	* in minutes field means “every minute”.	
?	No specific value.	? in the day-of-week field means “there is no preference on which day this occurs”.	Only allowed in the day-of-month and day-of-week fields.
-	Specifies range of numbers.	10-12 in the hours field means “on the 10th, 11th, and 12th hour”. 22-2 in the hours field means “on the hour of every hour from 10 at night until 2 in the morning”.	Overflowing ranges are allowed (that is, number on left is larger than number on right) but may result in unexpected behavior.
,	Deliminates values.	TUE,THU in day-of-week field means “on Tuesdays and Thursdays”.	No spaces between the “,” and the values since spaces indicate separation of the fields.
/	Specifies increments of the form 'm/n', which indicates increase by n starting from m.	0/15 in the seconds field means “at the 0th, 15th, 30th, and 45th second”. 5/15 in the seconds field means “at the 5th, 20th, 35th, and 50th second”.	*/n is equivalent to 0/n Incrementing outside of the allowed range of the field is ignored (that is, 7/6 in month field is same as indicating 7).
L	Last day of month/week; used as nL means “last n-day of month”.	L in day-of-month field means “the last day of the month” (accounts for leap years for example Feb 28th on non-leap, Feb 29th on leap) 6L in day-of-week means “the last Friday of the month”.	Only allowed in the day-of-month and day-of-week fields L in day-of-week field indicates a Saturday.
W	The closest weekday (Mon-Fri) of the given date. Used as nW where n is the day of the month.	15W means “the weekday closest to the 15th of the month”; if it falls on a Saturday, this will mean Friday the	Only allowed for day-of-month field. Does not cross a boundary of the month (for example 1W and the first is a Saturday, it will indicate Monday

Character	Meaning	Example	Note
		14th; if it falls on a Sunday, this will mean Monday the 16th.	the 3rd instead). Only works for single days, not ranges.

Examples of cron expressions for scheduling are:

Expression	Meaning
0 0 0 * * ?	Daily at midnight (Every month, every day of the month, at 0 hours, 0 minutes and 0 seconds)
0 0 0 1 1 ?	Yearly on the first of January at midnight (First month, first day of that month, at 0 hours, 0 minutes and 0 seconds)
0 0 * * * ?	Hourly (Every month, every day of the month, every hour at 0 minutes and 0 seconds)
0 0 12 ? * TUE,THU	Every Tuesday and Thursday at noon (Tuesday and Thursday of every month at 12 hours, 0 minutes and 0 seconds)

Note:
The archiver may have to write data measuring multiple GigaBytes to disk. Therefore, the default scheduling is once per day. Keep this in mind if you decide to run the archiver more frequently.

3.6 Configuring Network Demographics Connections to the SPB

By default, Network Demographics is configured to run over HTTP with no restrictions. You can alter the Network Demographics configuration so that it runs over HTTPS or you can configure restricted HTTP access.

3.6.1 Configuring SSL Connections

The Network Demographics is not configured to run over HTTPS by default. Use these steps to configure Secure Sockets Layer (SSL):

1. To verify that the Apache + `mod_SSL` package is installed, at the shell prompt run this command:

   ```
   show system version detail
   ```

2. Put the CLI into configuration mode and run the command:

   ```
   SRP# configure
   SRP# set config nds http-server protocol https
   ```

3. Copy your SSL certificates to the Network Demographics server.

4. Create an *httpd.conf* snippet that resembles the default Sandvine file (must contain the entire content of the Sandvine file) */usr/local/sandvine/reports/etc/nds-httpd-ssl.conf*, but set these variables to reference your own certificates:

   ```
   SSLCertificateFile /path/to/your/certificate
   SSLCertificateKeyFile /path/to/your/certificate
   ```

5. To configure Network Demographics to use the configuration file created in step 4, run the command:

   ```
   set config nds http-server ssl-config <file-path>
   ```

6. Commit the changes by running this command:

   ```
   commit
   ```

   Committing the changes through CLI will automatically restart Apache.

3.6.2 Restricting HTTP Access

By default, anyone can access the Network Demographics server. Use these steps to configure HTTP to restrict access to the server.

1. As an administrative user, copy the default Apache security configuration file */usr/local/sandvine/reports/etc/nds-httpd-security.conf* to a different location or copy to a new file name.

2. Edit the new security file created in Step 1 with new directives.

   a. Comment out these lines (# at beginning of line indicates that the line is a comment).

   ```
   # Order allow, deny
   # Allow from all
   ```

   b. Add these new directives.

   ```
   Allow 127.0.0.1
   Allow ip-mask
   ```

   Make sure not to deny access to the local machine or you will disable the scheduler.

3. Edit */usr/local/sandvine/etc/rc.conf* and update the `svreports_http_server_security_conf` variable with the full path to the new security file (the file created in Step 1).

3.6.3 Verifying Data Source Configuration for Network Demographics

To verify the data connection between Network Demographics and the SPB:

Open */usr/local/etc/odbc.ini* and verify that `Servername` and `Port` match the SPB's configuration.

```
[svreports]
Driver = WSDL
Servername = https://spb hostname or IP address
Database = sv_stat
UserName = spbadmin
Password = sandvine
Port = 8443
UseWithReports = Yes
```

Warning: If the VRRP feature is used, do not change the default value of the `Servername` parameter.

3.7 Optional Configurations

These configurations are optional.

3.7.1 Configuring Multiple Virtual IPs

You can configure multiple virtual IPs on each SRP, for example one for the IP Mapper and one for the database. However, the number of virtual IPs is limited to the number of physical interfaces, and the SRP has two. To add a virtual IP, run the CLI command:

```
SRP# add config virtual-host <virtual-host-id> ipv4-subnet <ipv4-subnet> interface <interface>
priority <int:0..255> heartbeat-interval <int:1..30> master-script <file-path>
backup-script <file-path>
```

Warning: If the VRRP feature is used, do not change the default value of the `Servername` parameter in */usr/local/etc/odbc.ini* and do not use the CLI command:

```
set config service application-server bind-address
```

If these parameters are changed from the default, then automatic failover may not work correctly.

3.7.2 NAT Mappings

You can optionally enable NAT mappings. Use this CLI command:

```
set config service nat enabled true
```

Enabling NAT mappings reduces the number of IP assignments supported. This enables you to use the available memory for NAT mappings.

In a cluster of SPBs, if you enable NAT mapping on one SPB, ensure that you configure each SPB in the cluster to have NAT enabled and the same maximum number of NAT mappings.

3.7.3 Statistics Cluster Name

The SPB generates some of the statistics used to generate the Quota Manager reports in Network Demographics. Identify the SPB by name to publish statistics and ensure that the name is the same for all members of an SPB cluster. To configure the name, run:

```
SRP# set config service attribute-summarizer cluster-stat-name <cluster-stat-name>
SRP# commit
```

Use the `cluster_stat_name` parameter to name the cluster and element in statistics produced by the SPB; for example, by the attribute summarizer. The statistics are not actually produced until this parameter is changed from its default value of SANDVINE-1.

4

Database Installation and Configuration

4.1 Setting up a Standalone Database Server

For performance reasons, Sandvine recommends that you install the database and application servers on separate systems. The supported database is PostgreSQL 8.2 and the supported operating system is FreeBSD 6 or FreeBSD 8.

4.1.1 Configuring the database server

Perform these steps on the stand-alone database server:

1. Put the CLI into configuration mode:

   ```
   configure
   ```

2. Disable the application sever:

   ```
   set config service application-server enabled false
   ```

3. Accept the prompt when notified that the application server will restart.

4. Disable the message broker:

   ```
   set config service message-broker enabled false
   ```

5. Accept the prompt when notified that the message broker will restart.

6. Disable the Network Demographics process:

   ```
   set config nds http-server enabled false
   ```

7. Configure the standalone database element to point to the SPB application server:

   ```
   set config service spb servers <server>
   ```

8. Commit the changes:

   ```
   commit
   ```

   Committing these changes will require a restart.

9. Stop the Network Demographics process:

   ```
   stop service nds
   ```

10. Set up permissions on the database server.

    a. Use this CLI command to edit *usr/local/pgsql/data/pg_hba.conf*.

       ```
       edit service database authentication
       ```

    b. Add a line to *pg_hba.conf* to allow the SPB application server to connect. The *pg_hba.conf* file contains comments and examples to help you set up the required permissions. For example:

       ```
       TYPE  DATABASE    USER     CIDR-ADDRESS        METHOD
       host  all         all      10.0.0.1/32         trust

       host  all   all      10.0.0.0 255.0.0.0  trust
       ```

In the first example, permission is allowed only to the server with address 10.0.0.1. The second example grants permission to any server with address 10.x.x.x.

11. Reload PostgreSQL using this CLI command:

```
reload service database
```

4.1.2 Configuring the Application Server

Perform these steps on the SPB application server:

1. Put the CLI into configuration mode:

```
configure
```

2. As an administrative user, run this CLI configuration command:

```
SRP# set config service database ip-address <ip-address>
```

Optionally, run these CLI commands:

```
SRP# set config service database port <int:0..>

SRP# set config service database name <name>

SRP# set config service database ssl enabled <false|true>

SRP# set config service database username <username>

SRP# set config service database password <password>
```

3. Commit the changes:

```
commit
```

Committing these changes will require a restart.

4. Stop the local Postgres process. As an administrative user, run this CLI command:

```
SRP> stop service database
```

The application server acts as a client to the database server, so running a local version of PostgreSQL is not required.

5. Disable the Postgres process:

a. Put the CLI into configuration mode:

```
configure
```

b. Run this CLI command:

```
SRP# set config service database enabled false
```

4.2 Database Server Configuration

If an SPB accesses the database of another SPB server, you must update *pg_hba.conf* on the database server to configure host-based access. This is a Postgres DBMS security mechanism to ensure that connection attempts are only permitted from a list of authorized IP addresses.

To configure host-based access to the server, log in to the database server as an administrative user and run the CLI command `edit service database authentication` to edit */usr/local/pgsql/data/pg_hba.conf*. The *pg_hba.conf* file is a PostgresSQL configuration file. See the PostgresSQL documentation for more information.

The *pg_hba.conf* file is used to control:

- Which hosts are allowed to connect
- How clients are authenticated
- Which PostgreSQL user names clients can use
- Which databases they can access

Each line in the *pg_hba.conf* file applies to one IP address or netblock. Lines are processed in order and the first match is used. Each line has this syntax:

```
host database user IP-address IP-mask method {option}
```

Where:

- host — Either a plain or Secure Sockets Layer (SSL) encrypted TCP/IP socket.
- database — Can be **all**, **sameuser**, **samegroup**, a database name (or a comma-separated list of database names), or a file name prefixed with **@**.
- user — Can be **all**, an actual user name, a group name prefixed with **+**, or a list containing both user names and group names.
- IP-address IP-mask — The set of hosts the record matches.
- method — Can be **trust**, **reject**, **md5**, **crypt**, **password**, **krb4**, **krb5**, **ident**, or **pam**. Note that **password** uses clear-text passwords; **md5** is preferred for encrypted passwords. CIDR-MASK is an integer between 0 and 32 that specifies the number of significant bits in the mask, so an IPv4 CIDR-MASK of 8 is equivalent to an IP-MASK of 255.0.0.0.
- option — The ident map or the name of the pluggable authentication model (PAM) service.

4.3 Configuring SSL on the Database Server

On the database server, you can enable SSL for security. You need to acquire your own private key and certificate to enable security.

1. On the database server, copy your private key and certificate to */usr/local/pgsql/data*.
2. Ensure that the private key and certificate are named **server.key** and **server.crt** respectively.
3. If necessary, change the directory to */usr/local/pgsql/data*, then run:

   ```
   ls -l
   ```

4. Examine the file permissions and verify that both **server.key** and **server.crt** are owned by the pgsql user. If this is not the case, to change the permission on these files, run:

   ```
   chown pgsql server.key server.crt
   ```

5. Enable SSL:
   a. Put the CLI in configuration mode:
      ```
      configure
      ```
   b. Run this CLI command:
      ```
      SRP# set config service database ssl enabled true
      ```
6. Restart PostgreSQL by running this CLI command:
   ```
   restart service database
   ```

4.4 Changing Data Retention

Statistics removal in the database is managed by an SPB process that is based on the data retention configuration file. Retention is configurable for all the various statistic, history, and audit tables.

4.4.1 Overriding Default Data Retention Configuration

To override the configured defaults, run the CLI command `set service database retention table <table name> days <int:1..1000>`.

To see the currently configured retention periods for partitioned tables, use the CLI command `show service database retention`.

4.4.1.1 Retention Values

The retention values found in the default configuration file (*dataRetention.conf.default*) span the total number of days for which table partitions are pre-allocated. Decreasing these retention values removes data more aggressively from the database, freeing up storage, but the partitions themselves remain. This can result in many empty partitions, but is not considered a problem. You can increase the retention periods anywhere back to their original size at any time. If you increase the retention periods beyond the default value, the partitions required to span the specified number of days are added automatically.

When the truncate and allocate script runs the next time, it truncates the partitions containing data older than the new retention period.

Note:
Setting the retention value to zero removes data from the database more aggressively. Do not decrease the retention of any statistic to a value less than the summarization interval of any associated digest or summary table.

4.4.2 Identifying High Disk Consumption

You can use CLI commands to show how much disk space the tables in the database are consuming and growth rates of the tables. If disk usage is high (defined as greater than 70% of the disk consumed), you should consider changing the default data retention rates for the statistics that are consuming the most space.

For example, this command shows that **elem_stats** (Network Element statistics) is consuming the majority of the disk space:

```
SRP> show service database table-groups
  tablegroup   |    MB    |       Rows
```

```
----------------+----------+-----------------
dts-stats       |          |
elem-stats      |    1,314 |         7,084,292
sub-stats       |      196 |           760,150
network-stats   |      196 |           812,905
dns-stats       |      158 |           766,916
sub-info        |       27 |               874
wdtm-stats      |       20 |               380
voip-stats      |        4 |               384
voip-qoe-stats  |        3 |                 0
sms             |        0 |                 1
```

To examine this further, request a breakout of that particular table-group:

```
SRP> show service database table-group elem-stats
         tablename           |    MB    |       Rows
-----------------------------+----------+------------------
elem_classifier_prot_dtl     |      462 |         4,453,798
elem_classifier_stats_dig1   |      227 |         1,502,182
elem_classifier_prot_dig1    |      224 |         1,004,728
elem_classifier_stats_dtl    |      157 |           856,093
elem_classifier_stats_dig2   |      152 |         1,040,524
elem_classifier_prot_dig2    |       34 |           279,865
elem_interface_prot_dtl      |       30 |           164,267
elem_interface_prot_dig1     |       15 |            81,237
elem_performance_dtl         |        4 |            17,919
elem_interface_dtl           |        3 |             6,482
elem_interface_prot_dig2     |        3 |            15,730
published_expr_stats_dtl     |        2 |             9,732
published_expr_stats_dig1    |        1 |             4,359
elem_interface_dig1          |        1 |             2,944
elem_classifier              |        0 |                 7
published_expr_stats_dig2    |        0 |               504
elem_interface_dig2          |        0 |               366
elem_classifier_templ        |        0 |                10
elem_classifier_templ_col    |        0 |                11
```

This output shows that the table consuming the most space is **elem_classifier_prot_dtl**. In the */usr/local/sandvine/etc/dataRetention.conf.default file*, the default retention for the **elem_classifier_prot_dtl** statistics table is 33 days. If you change the retention of this statistic to 16 days by running the CLI command `set service database retention table elem_classifier_prot_dtl days 16`, you should gain back about 200 MB of disk space the next time the hourly truncollator runs.

Detail statistics tables (those ending in “dtl”) contain the finest time granularity of a statistic, while their corresponding digests (“dig1”, “dig2”) contain the same data at a coarser time granularity. Instead of reducing the retention period for the detail statistics, you could reduce the retention of “dig1”. Generally, reducing digest level 1 statistics retention is the recommended approach. It retains the details for as long as possible while not effecting the longer term data trends that are stored in the “dig2” digests.

When reducing retention periods, it is important to make sure that you do not drop the retention period of any given statistic to be less than the size of its immediate digest level. As a rule of thumb, this means do not set “dtl” retention to be less than two days, “dig1” to less than one week and “dig2” to less than one week. You should not set the retention of other partitioned tables, such as audits and history tables, to less than one day.

4.5 Configuring Warm Standby System

Database log files are shipped from the primary database server to the standby server via secure, encrypted file transfer.

4.5.1 Enabling a Trust Relationship Between Servers

To allow for seamless and continuous file transfer from the primary server to the standby server, set up a trust relationship between the servers. Since the archive process on the primary server runs as the pgsql database user, generate a public key for the pgsql user and copy the key to the standby server to avoid a password prompt at each copy command.

1. On the primary database server, put the CLI into configuration mode, configure the warm-standby server, then commit the changes:

```
SRP> configure
SRP# set config service warm-standby server <ip-address>
SRP# commit
```

2. As an administrative user:

   a. Log in to both the primary and standby servers.

   b. To generate a key for the pgsql user, on both servers, run this CLI command:

```
SRP> set service warm-standby generate-key
```

   c. When prompted, accept the default key file */usr/local/pgsql/.ssh/id_dsa*.

   d. When prompted, accept the default empty pass phrase.

   e. Exit the CLI:

```
SRP> exit
```

4.5.2 Enabling Database Archival

Once a trust relationship is set up between database servers, archive database log files from the primary server to the standby server. It is important that this step functions properly before proceeding with subsequent steps.

1. As an administrative user, log in to the primary server.

2. Put the CLI into configuration mode, over ride the default settings, then commit your changes using these commands:

```
SRP> configure
SRP# set config service warm-standby archive log <log>
SRP# set config service warm-standby archive threshold warning <int:0..90>
SRP# set config service warm-standby archive threshold stop <int:0..90>
SRP# set config service warm-standby archive email <email-address>
SRP# set config service warm-standby archive frequency <int:0..10080>
SRP# commit
```

   For more information on these commands and the default settings see the *SPB CLI Reference Guide*.

3. Exit the configuration mode using this command:

```
SRP# exit
```

   This message appears:

```
The CLI is now in OPERATIONAL mode.
```

4. To start the archive process, run this CLI command:

```
SRP> start service warm-standby primary
```

5. To see the status of the archive process, run this CLI command:

   ```
   SRP> show service warm-standby status
   ```

   After the successful execution of these steps, database log files begin to appear in the archive directory on the standby server. To verify that the log files are successfully archived to the standby server, */var/log/archive.log* on the primary server must include these messages:

   ```
   archive: Archived transaction log file log_file last modified at date
   ```

   If any error messages appear in the log file, then, if possible, correct the problem and restart the database archival by running these CLI commands:

   ```
   SRP> stop service warm-standby
   SRP> start service warm-standby primary
   ```

   Ensure that database archival functions properly before proceeding.

6. Exit the CLI:

   ```
   SRP> exit
   ```

4.5.3 Starting the Standby Server in Recovery Mode

After the database archival is successfully configured and a base backup is underway on the primary server, start the standby server in recovery mode. While the standby server is in recovery mode, it is not available to process any queries. However, the standby server continuously replays the database log files received from the primary server and takes over operations in a short time if the primary server experiences an unrecoverable failure.

When the recovery starts, the standby server extracts the base backup received from the primary server, and replays all the database log files received while the backup was being taken to restore the data files to consistency. For large databases, this process may take several hours and so a consistent backup may not be available during this time.

1. As an administrative user, log in to the standby server.

2. Put the CLI into configuration mode:

   ```
   configure
   ```

3. If you set `set config service warm-standby archive log` to a non-default directory on the primary server, be sure to set this variable to the same location on the standby server.

4. If required, set any other recommended or optional configuration variables to override their respective defaults.

   ```
   SRP# set config service warm-standby restore email <email-address>
   SRP# set config service warm-standby restore frequency <int:0..10080>
   ```

5. Commit the changes using the command:

   ```
   commit
   ```

6. Exit the CLI configuration mode using this command:

   ```
   SRP# exit
   ```

   This message appears:

   ```
   The CLI is now in OPERATIONAL mode.
   ```

7. Run this CLI command:

```
SRP> start service warm-standby standby
```

8. At the warning prompt indicating that this action must be performed on the standby server, answer **Y** (yes) to continue.

   Output to the console should appear as:

```
Starting database recovery ...

*** PLEASE NOTE: ****************************************************************
When database recovery is started, it will stop the database, clean out the
database data files, and extract the contents of
  /usr/local/pgsql/archives/svdb_base_backup_20130826_123130.gz
into the database backend. Please ensure that this command is executed on
the standby server and not on an active database server.
*********************************************************************************

Start database recovery? <Y/N> :Y
This will clean out the existing database data files
Are you sure? <Y/N> :Y
Database recovery started in background
Source directory is /usr/local/pgsql/archives
```

9. To view the status of the recovery, run this CLI command:

```
SRP> show service warm-standby status
```

10. Exit the CLI:

```
SRP> exit
```

4.5.4 Configuring Automatic Database Failover

The automatic failover mechanism provides link and application awareness by configuring IP address redundancy using VRRP (freevrrpd implementation) and by database monitoring techniques. This setup minimizes service interruptions due to failures in the database server.

Note:
If both IP mapping failover and database failover are required, you must have a four-element deployment: two element for SPB clustering and two element for database failover. If you have a two-element deployment, you can configure automatic IP mapping failover or database failover, but not both.

Use these steps to configure automatic database failover on both the primary and standby database servers.

1. Put the CLI into configuration mode by running:

```
configure
```

2. Configure a unique virtual host using these commands, where *n* is the identified virtual host ID:

```
SRP# add config virtual-host <n> ipv4-subnet <ipv4-subnet> interface <interface> priority
<int:0..255> heartbeat-interval "6"
            master-script "/usr/local/sandvine/dbtools/warmstandbydb_vrrp_master.sh"
            backup-script "/usr/local/sandvine/dbtools/warmstandbydb_vrrp_backup.sh"
```

Attribute	Description
virtual-host	The virtual-host ID.
ipv4-subnet	An IPv4 subnet, in the form x.x.x.x/xx. For example, 10.10.10.10/01.

Attribute	Description
interface	The name of the interface corresponding to the external IP address configured for the server. For example, mgmt2.
priority	A priority in the range 0 - 255. A value of 255 indicates the default master and a value < 255 indicates a backup.
heartbeat-interval	The interval, in seconds, that the host sends heartbeat messages to other cluster members. Members consider the master to have failed at three times the configured number of seconds.
master-script	A script to execute when the node takes over mastership.
backup-script	A script to execute when the node loses mastership.

3. Set the parameters to configure database monitoring, where *n* is the identified virtual host ID:

```
SRP# set config service db-monitor enabled true
SRP# set config service db-monitor vrrp-vhid <n>
```

4. Commit the changes:

```
commit
```

5. Starting with the primary database server, add the servers to the cluster. As an administrative user, run this CLI command:

```
set service db-monitor join-cluster
```

6. Verify that the primary database server is the master node. The status can be verified using the CLI command:

```
show service db-monitor status
```

7. On the primary database server only, start database monitoring using the CLI command:

```
set service db-monitor start
```

8. Verify the status of database monitoring using the CLI command:

```
show service db-monitor status
```

4.5.4.1 Configuring the Data Source in SPBs

1. As an administrative user, log in to all SPBs that are connected to the primary database server.

2. Put the CLI into configuration mode by running:

```
configure
```

3. Set the data source host to the configured virtual IP address using the command:

```
set config service database ip-address <ip-address>
```

4. Commit the changes using the command:

```
commit
```

4.6 Reconfiguring or Disabling a Warm Standby System

Once a warm standby system is set up, it is not possible to use `set config service warm-standby server <ip-address>` or `set config service warm-standby archive log <log>` without stopping the archive and restore processes and reconfiguring the warm standby system from scratch. You can dynamically modify any of the other CLI configuration commands associated with the warm standby system (such as warning messages required to be sent to a different email address). The archive process on the primary server or the restore process on the standby server immediately pick up configuration changes.

1. As an administrative user, log in to the primary server.
2. Put the CLI into configuration mode by running:

   ```
   configure
   ```

3. Set or update any configuration variables as appropriate.

   ```
   SRP# set config service warm-standby archive threshold warning <int:0..90>
   SRP# set config service warm-standby archive threshold stop <int:0..90>
   SRP# set config service warm-standby archive email <email-address>
   SRP# set config service warm-standby archive frequency <int:0..10080>
   ```

4. As an administrative user, log in to the standby server.
5. Set or update any configuration variables as appropriate.

   ```
   SRP# set config service warm-standby restore email <email-address>
   SRP# set config service warm-standby restore frequency <int:0..10080>
   ```

6. Commit the changes using the command:

   ```
   commit
   ```

7. To ensure the configuration changes have not adversely affected the system, check the status of the warm standby system.

4.6.1 Disabling a warm standby system

1. As an administrative user, log in to the primary server and run the command:

   ```
   SRP> stop service warm-standby
   ```

2. At the warning prompt indicating that this action will invalidate the standby server, enter **Y** (yes) to continue.
3. As an administrative user, log in to the standby server and issue the command:

   ```
   SRP> set service warm-standby failover
   ```

4. At the prompt, enter **Y** (yes) to confirm.
5. At the warning prompt indicating that this action will invalidate the standby server, enter **Y** (yes) to continue.

The former standby server is now decoupled from the system and you can reuse it for other purposes. You need to re-install a number of software packages to reinstate the warm standby system. Contact Sandvine Customer Support or its authorized partner for details if you need to re-install the system at a later time or if the database is not in a usable state.

4.7 SPB Load Balancing

To achieve the highest possible scalability, SPB servers in a cluster are load balanced, by default.

The implementation of load balancing involves configuring the cluster and a single virtual IP address for the clients to access. Once configured, clients can access load balanced ports in order to take advantage of load balancing requests across the servers in the cluster.

Note:
Once configured, the load balancing service automatically starts whenever the server reboots/restarts.

1. Configure IP address redundancy as outlined in *Configuring Multiple Virtual IPs* on page 74.
2. Configure message broker/application server redundancy as outlined in *Message Broker and Application Server Redundancy* on page 88.
3. Enable the load balancer:
   a. Put the CLI in configuration mode:
      ```
      configure
      ```
   b. Run the CLI command:
      ```
      SRP# set config service load-balancer enable true
      ```
4. To start load balancing, run this CLI command on each SPB server in the cluster:
   ```
   SRP> start service load-balancer
   ```

4.7.1 Client Default Connections

The SPB accepts connections on default ports and then load balances across the cluster. You must configure clients to connect to the virtual IP address and the correct port. The client default settings are:

Client port	Group	Service
58080	svhttp	Web server (HTTP) for web applications running on the SPB (Network Demographics Server)
58081	svws	Web Services (SOAP over HTTP) for client applications using the SPB API
58443	svwss	Web Services (SOAP over HTTPS) for client applications using the SPB API

4.7.2 Configuring Client Connections to the SPB

If the default ports are not desirable for client applications, you can adjust the configuration. To adjust default load balancing for a cluster of SPB servers where centralized configuration is in use:

1. As an administrative user, edit the centralized SPB configuration file for the cluster or connect to the SPB server and edit */usr/local/sandvine/etc/rc.conf*.

2. Adjust these entries as required:

```
spb_lb_<group>_port
spb_lb_<group>_sticky
spb_lb_enable
```

3. To apply the load balancing changes, run this CLI command:

```
restart service load-balancer
```

If centralized configuration is not in use, adjust the load balancer port settings on each SPB in the cluster. See the *SPB CLI Reference Guide*.

4.7.3 Message Broker and Application Server Redundancy

You can configure the SPB application servers and message brokers running on each server within the cluster for redundancy. Complete these steps on all SPB elements in the cluster, beginning with the domain manager:

1. Log in as an administrative user.

2. Put the CLI into configuration mode by running:

```
configure
```

3. Run these commands to set the variables, and commit your changes:

```
SRP# set config cluster name <name>
SRP# set config cluster servers <servers>
SRP# set config cluster domain-manager <ip-address>
SRP# set config service database ip-address <ip-address>
SRP# set config service application-server bind-address <ip-address>
SRP# commit
```

   Commiting these changes requires a restart.

4. On the database server only, set permissions on the SPB server, as identified by the `show config service database ip-address` CLI command, to allow connections from other SPB servers in the cluster. The SPB server designated as the database server could be an SPB server from the cluster or a separate standalone SPB database server.

   a. As an administrative user, run this CLI command to edit the `/usr/local/pgsql/data/pg_hba.conf` file on the database server:

```
edit service database authentication
```

   b. To add unrestricted access to a host or subnet, add a line for each SPB server in the cluster similar to one of these:

   - `host  sv_stat     all    <ip address> <subnet mask>  trust`

     The *<ip address> <subnet mask>* identifies the IP of the SPB server. For example: `192.0.2.1 255.255.255.255`.

   - `host    sv_stat       all      <CIDR notation>  trust`

     The *<CIDR notation>* identifies the IP of the SPB server. For example: `192.0.2.1/32`.

   c. Reload the configuration by running this CLI command:

```
reload service database
```

5. Run this CLI command to verify that messaging infrastructure has started correctly on the SPB server in the cluster designated as the domain manager:

   ```
   show service message-broker status
   ```

   The display results for the SPB server designated as the domain manager should be similar to this example:

   ```
   SonicVersion: MQ8.5

   Name                                      Host        State  ConnectedSince
   ----------------------------------------- ----------- ------ ----------------------
   DefaultCluster.DomainManager_Container    <hostname>  Online 2013-08-28 09:11:53 IST
   DefaultCluster.AppBrkr7F000001_Container <hostname>  Online 2013-08-28 09:12:07 IST
   ```

   The example indicates that both the domain manager and an application messaging broker are running.

6. Run this CLI command to verify that the messaging infrastructure has started correctly on the remaining SPB servers in the cluster:

   ```
   show service message-broker status
   ```

   The display results for the SPB server should be similar to this example:

   ```
   SonicVersion: MQ8.5

   Name                                      Host        State  ConnectedSince
   ----------------------------------------- ----------- ------ ----------------------
   DefaultCluster.AppBrkr7F000001_Container <hostname>  Online 2013-08-28 09:12:07 IST
   ```

7. Verify that the application server has started correctly. At the command prompt, run:

   ```
   show system services
   ```

8. Verify that the application servers are operating in a clustered mode. For each SPB server in the cluster, run this command at the command prompt:

   ```
   show cluster config
   ```

   The display results should be the same for all servers in the cluster. For example:

   ```
   ActiveNodes         : 1.0.0.1:3100,1.0.0.2:3100
   ```

After the application server starts, it may take a few minutes for the cluster status command to indicate that the application server has started. If the application server status command indicates that the server has started but the cluster status command indicates that the server has not started, then wait for a few minutes up to an hour, depending on the deployment configuration.

5

High Availability and Load Balancing

5.1 High Availability

The SPB achieves high availability through IP redundancy, clustering technology for message broker and application server, and warm stand-by for the database.

When a failure occurs on the primary or master machine, the standby or slave machine takes over.

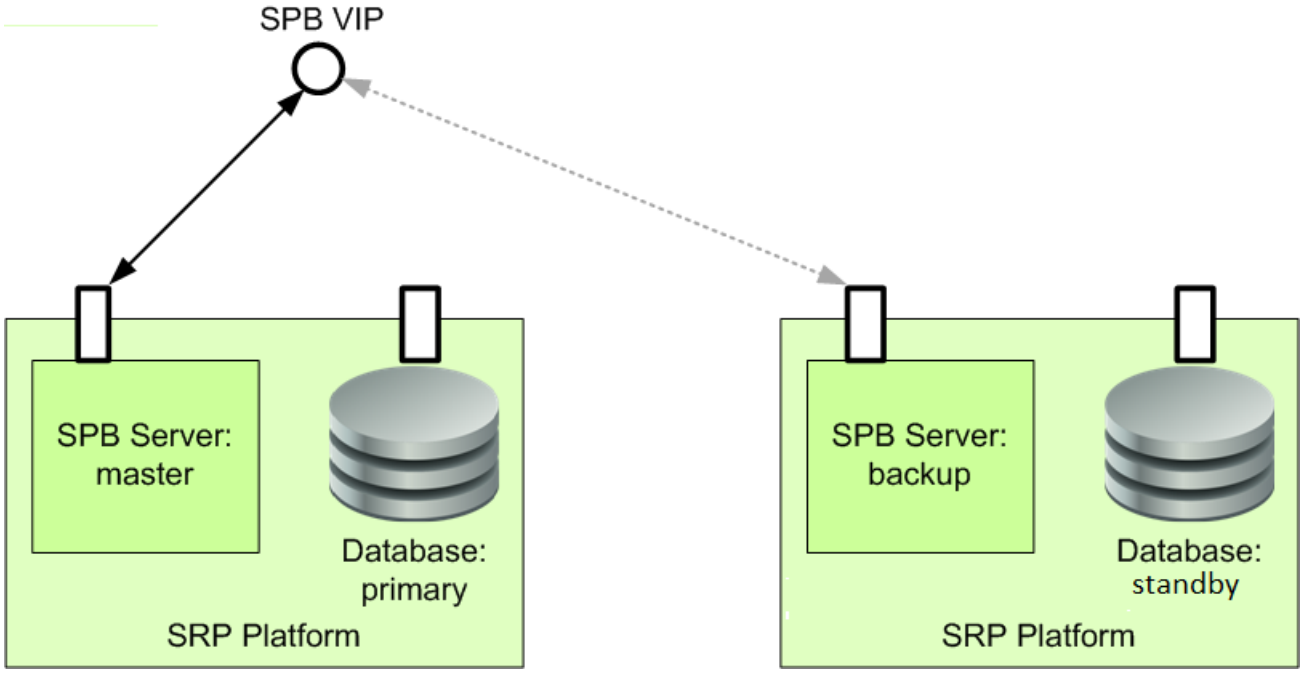
- VRRP provides IP redundancy at the interface level for IP mapping and for the database connections.
- The PTS exchanges JMS messages with the SPB. The message broker handles these messages to provide redundancy for the PTS sending statistics messages to the stats collection service.
- Subscriber management service achieves redundancy through the application server.
- Warm standby provides database redundancy.

5.2 IP Address Redundancy

External clients of an SPB cluster achieve connection redundancy by configuring a virtual IP address (VIP) using the Virtual Router Redundancy Protocol (VRRP).

The VIP is an abstract representation of two or more SPB servers acting as a group, but where only one SPB server actually responds to requests at a time. The physical SPB that currently forwards data on behalf of the cluster is called the master. Physical SPBs standing-by to take over from the master SPB in case something goes wrong are called backups. If the current physical SPB that provides data on behalf of the SPB cluster fails, the VRRP specifies an election protocol that dynamically and automatically assigns the responsibility of master to one of the backup SPBs in the cluster. The VRRP implementation in Sandvine conforms to RFC 2338.

Clients access the SPB cluster through the virtual IP:



The initial configuration uses priorities to determine the SPB server that functions as the VRRP master and the servers that function as backup servers. The variable `vhid_n_pri` (see *Virtual Host Variables*) sets the priority of a server. This variable takes a value in the range 0-255, where:

- 255 indicates the default master server.
- A value between 1 and 254 indicates a backup server.
- 0 indicates that the current master has stopped participating in VRRP.

5.2.1 SPB Load Balancing

To achieve the highest possible scalability, load balance the SPB servers in a cluster.

The implementation of load balancing involves configuring the cluster and a single virtual IP address for the clients to access. Once configured, clients can access load balanced ports to take advantage of load balancing requests across the servers in the cluster.

5.3 Subscriber IP Mapping Failover

Subscriber IP mapping failover automates IP mapping from one SPB within a cluster to another SPB within the same cluster in the event of certain failover conditions. This mapping provides high availability to all services that depend on IP mapping.

Conditions that may cause a failover include:

- The SPB is not available for any reason (powered down, hardware or software failure, and so on).
- The connection is lost.
- There is an issue with the IP mapping process (critical thread down).

Note:
If both IP mapping failover and database failover are required, you must have a four-element deployment: two elements for SPB clustering and two elements for database failover. If you have a two-element deployment you can configure IP mapping failover or database failover, but not both.

You can enable subscriber IP mapping failover by sharing a virtual IP address among the SPBs in the cluster. In case of a failure at the link level, the IP redundancy (VRRP) can trigger VRRP failover. The subscriber IP mapping failover achieves application-level awareness by detecting IP mapping service failure and proactively triggering the VRRP failover process. The failover process sends out an SNMP trap to notify the operator to resolve the problem by manually putting the failed server back in the cluster.

The failover process takes only a few seconds. If the PTS tees RADIUS traffic to the SPB, traffic for a few seconds is lost. If the subscriber IP mapping service runs in RADIUS proxy mode, then retries are routed to the new master after a few seconds.

At the end of the failover procedure, this SNMP trap is sent to indicate that the VRRP master has stopped participating in VRRP:

`svSpbAppIpRedundancyLostNotification`

Once the server rejoins VRRP, this clear trap is sent:

`svSpbAppIpRedundancyResumeNotification`

The notification triggering the alarm has these variable bindings:

`SANDVINE-SPB-APP-MIB::svSpbIpRedundencyLostReason`

See the *SPB Alarm Reference Guide* for detail on setting default SNMP notification target and for more information on these SNMP notifications.

5.3.1 IP Mapping Failover Process

If all the SPB servers have the same hardware/software configuration, you can set them to the same priority.

In this configuration, when the master SPB server goes down, one of the backup servers take over as master. Once the problem is resolved on the previously failed master server, it rejoins VRRP and becomes a backup server.

If you designate one server as the primary SPB to process IP mapping traffic, then assign it the highest priority. The primary SPB always takes over the VRRP mastership and starts processing IP mapping traffic as soon as it comes online. One implication of this is that the primary SPB server triggers the failover process again when it rejoins VRRP.

If you stop the VRRP service administratively with the `stop service ip-redundancy` CLI command, the behavior is the same as interface failure. If the VRRP process experiences a crash or is killed, there is currently no way for it to properly release the VIP or the virtual MAC address, therefore, you need to restart the server.

It is possible for both servers to fail at the same time, either by interface failure or application failure. If both servers leave VRRP, then VRRP could run into a faulty state where the servers cannot reach each other and the `ping` command returns this error:

```
Host is down
```

This is often caused when the VRRP process is not able to recover itself in case of a network interface problem. In this situation, restart the VRRP process using the command:

```
restart service ip-redundancy
```

5.3.1.1 Same Priority Failover

If both SPBs have the same priority and the subscriber-IP mapping service fails, the standby SPB takes over as the master. The process when both SPBs have the same priority is:

Step	Description	SPB-A VRRP status	SPB-B VRRP status
1	In the initial state, SPB-A is VRRP master and SPB-B is the backup.	master with priority of 254	backup with priority of 254
2	The subscriber-IP mapping service goes down on SPB-A.	failure	backup
3	The system detects the failure and begins VRRP failover.	no longer in cluster	master with priority of 254
4	The operator receives an SNMP notification to solve the problem on SPB-A.		
5	The operator runs the `set service ip-redundancy join-cluster` CLI command.	backup with priority of 254	master with priority of 254

5.3.1.2 Differing Priority Failover

If one SPB is assigned a higher priority, it becomes master when it comes back online. The process when one SPB has a higher priority and subscriber-IP mapping service fails is:

Step	Description	SPB-A VRRP status	SPB-B VRRP status
1	In the initial state, SPB-A is VRRP master and SPB-B is the backup.	master with priority of 200	backup with priority of 100
2	The subscriber-IP mapping service goes down on SPB-A.	failure	backup
3	The system detects the failure and begins VRRP failover.	no longer in cluster, has priority 0	master with priority of 100
4	The operator receives an SNMP notification to solve the problem on SPB-A.		
5	The operator runs the `set service ip-redundancy join-cluster` CLI command.	master with priority of 200	backup with priority of 100

5.3.1.3 Network Interface Failover

If the network interface fails on the master, the other node(s) in VRRP should detect the failure and elect a new master. The process when the network interface fails is:

Step	Description	SPB-A VRRP status	SPB-B VRRP status
1	In the initial state, SPB-A is VRRP master and SPB-B is the backup.	master with priority of 254	backup with priority of 254
2	The network interface fails on SPB-A.	failure	backup
3	The system detects the failure and begins VRRP failover.	backup	master
4	The operator receives an alarm `Interface down:SERVICE_1`. Depending on the failure condition, SPB-A might automatically transition to a fixed state or the operator must solve the problem on SPB-A.	backup	master
5	On SPB-A, The operator runs the `set service ip-redundancy join-cluster` CLI command.	backup with priority of 254	master with priority of 254

5.3.1.4 JBoss Stopped or Restarted

If you stop JBoss (with the `stop service application-server` CLI command) or restart it (with the `restart service application-server` CLI command) on the master IP mapper VRRP node, then the IP-mapping processes automatically fail over to the other node. When JBoss starts again, it automatically rejoins the VRRP. The process when you stop or start JBoss is:

Step	Description	SPB-A VRRP status	SPB-B VRRP status
1	In the initial state, SPB-A is VRRP master and SPB-B is the backup.	master with priority of 254	backup with priority of 254
2	JBoss application is either stopped or restarted. The “leave cluster” action is automatically invoked on SPB-A.	JBoss not active	backup
3	VRRP failover begins.	no longer in cluster	master
4	The operator must restart JBoss on SPB-A if it was stopped (with `start service application-server`).		
5	SPB-A automatically rejoins the IP mapper VRRP cluster.	backup with priority of 254	master with priority of 254

If you use the `stop/restart service application-server` CLI commands to stop or restart the application server acting as the master IP mapper in an SPB cluster, any IP mapper packets in the queue are lost. Before running the CLI commands on the master IP mapper, fail over to the IP mapper slave using this CLI command:

```
set service ip-redundancy leave-cluster
```

5.3.1.5 Performing svupdate

You can invoke the failover process administratively, as when performing an svupdate. The process to perform an svupdate with minimal impact is:

Step	Description	SPB-A VRRP status	SPB-B VRRP status
1	In the initial state, SPB-A is VRRP master and SPB-B is the backup.	master with priority of 254	backup with priority of 254

Step	Description	SPB-A VRRP status	SPB-B VRRP status
2	The operator performs an svupdate on the SPB-B. Updating SPB- should have no impact on system functionality as it is the backup.	master	backup
3	On SPB-A, the operator runs the `SRP> stop service ip-redundancy` CLI command. SPB-B assumes mastership and begins processing IP mapper traffic. A few packets are dropped in the process.	no longer in cluster	master
4	The operator must wait for the JBoss server to finish processing existing traffic in the SPB-A queue. You can view the status of the process using the CLI command: `SRP> show service ip-user-map stats`	not in cluster	
5	The operator performs an svupdate on SPB-A. Since SPB-A is not in the cluster, there should be no impact on the system during the upgrade.	not in cluster	
6	The operator makes SPB-A rejoin the cluster using this CLI command: `SRP> set service ip-redundancy join-cluster`	backup with priority of 254	master with priority of 254

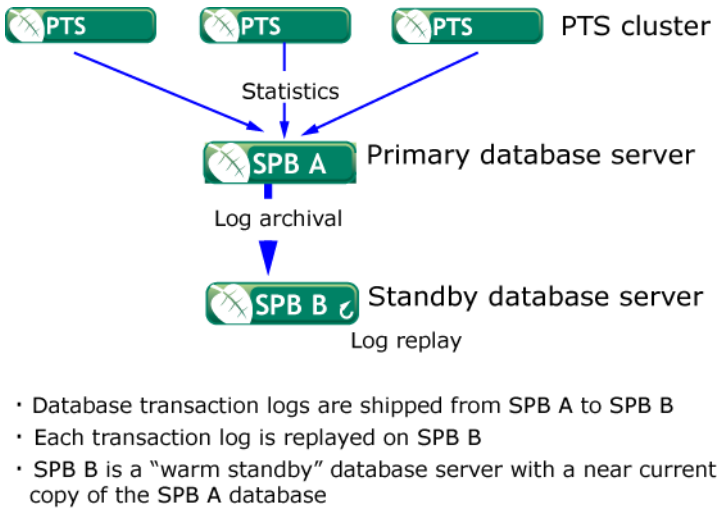
5.4 Overview of Database Redundancy and Failover

To guard against a database server failure, deploy a database redundancy solution.

If the primary database server fails, clients are redirected to the secondary server, which picks up where the primary server left off with minimal data loss. The SPB application server and even the PTS network elements retain a backlog of data not yet persisted for a certain window of time. If the database is able to recover and resume its online status in a timely manner, further failover is not required.

Database redundancy is achieved using log shipping. The transaction log files of the primary database are continually archived to another machine that replays the logs as they are received creating a warm standby system: at any point, you can bring up the second machine and it will have a near-current copy of the database.

Database log files from SPB-A are shipped to SPB-B where they are replayed. For example, here is a warm standby system utilizing two SPB servers participating in transaction log archival and replay:



5.4.1 System Configuration

When preparing to set up a warm standby system, it is important to verify that the SPB database servers (primary server and standby server) have identical hardware and platform configurations. The *SRP Installation Guide* details the relevant CLI commands to run. In particular, the output of these commands should be similar on both SPB servers:

- `show system hardware`
- `show system resources`
- `show system information`

Note:
You do not have to have administrative privileges to run these `show` CLI commands on the SPB, but you do need them in order to run any other CLI commands.

Having identical configurations on both servers not only facilitates efficient and predictable log shipping, it allows the entire cluster to transfer seamlessly from the primary server to the standby server in the event of a failover. While there is no strict requirement that the system dates are synchronized on both SPB servers, ensuring the system dates (time zone corrected) are within a few seconds of each other allow more meaningful status checking of the warm standby system.

While there is no hard requirement that the application server be decoupled from the primary database server, an administrator should take care to ensure the system setup makes sense for the purpose at hand. For example, application server redundancy (via SPB clustering) should be set up as a precursor to setting up database redundancy, particularly if the application server and primary database server reside on the same machine.

The transport connection between the primary and standby servers must support a minimum bandwidth of approximately 30 mega-bits per second. This is to ensure that the standby server can be initialized in a reasonable period of time and lag behind the primary server by a reasonable amount of time during normal operation.

5.4.1.1 Verifying System Configuration

Perform these steps on both the primary database server and standby database server and compare the results.

1. As an administrative user, at the default command prompt, enter:

   ```
   svcli
   ```

The CLI shell prompt appears:

```
# svcli

SRP>
```

2. Run these CLI commands:

```
show system hardware
show system resources
show system information
```

3. To exit the CLI shell, at the CLI prompt, enter:

```
exit
```

5.4.2 Disk Space Requirements

The initial phase of setting up a warm standby system involves taking a full file-system backup of the database data files as well as storing a significant backlog of database log files. Therefore, there must be at least 30% available disk space on the primary server before you attempt to set up a warm standby system.

If this requirement is not met, the initialization process is likely to run out of disk space and abort. To free up disk space, you can configure the retention period for certain statistic types to retain less data, which results in historical data being truncated.

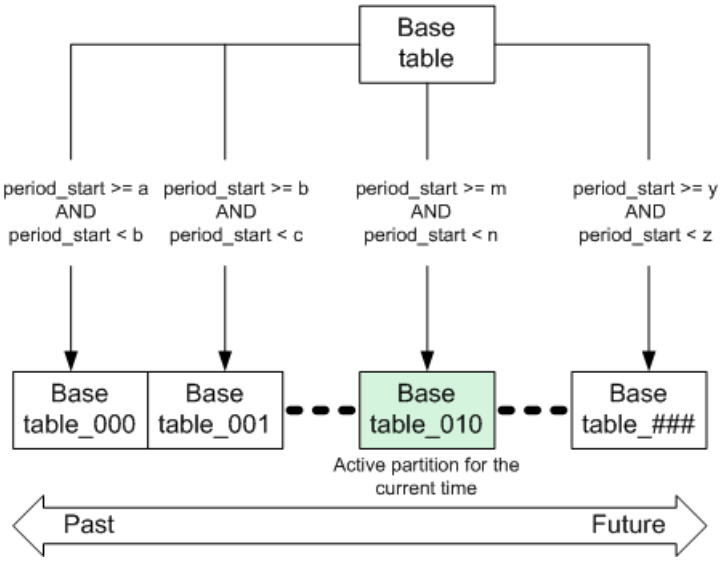
6

Data Retention

6.1 Data Retention Overview

To manage the size of the statistics database while providing optimum performance, the statistics database is partitioned at the table level and digest summary tables are created.

All statistic, digest, history, and audit tables (referred to as base tables) in the statistics database are partitioned on a timestamp. This means that any rows inserted into the base table are actually redirected into a partition based on the value of some timestamp field. Each partition is constrained to accept only a specific interval of values for the timestamp value and the set of partitions always constitute consecutive, non-overlapping intervals. These are rolling, consecutive partitions based on non-overlapping time intervals:

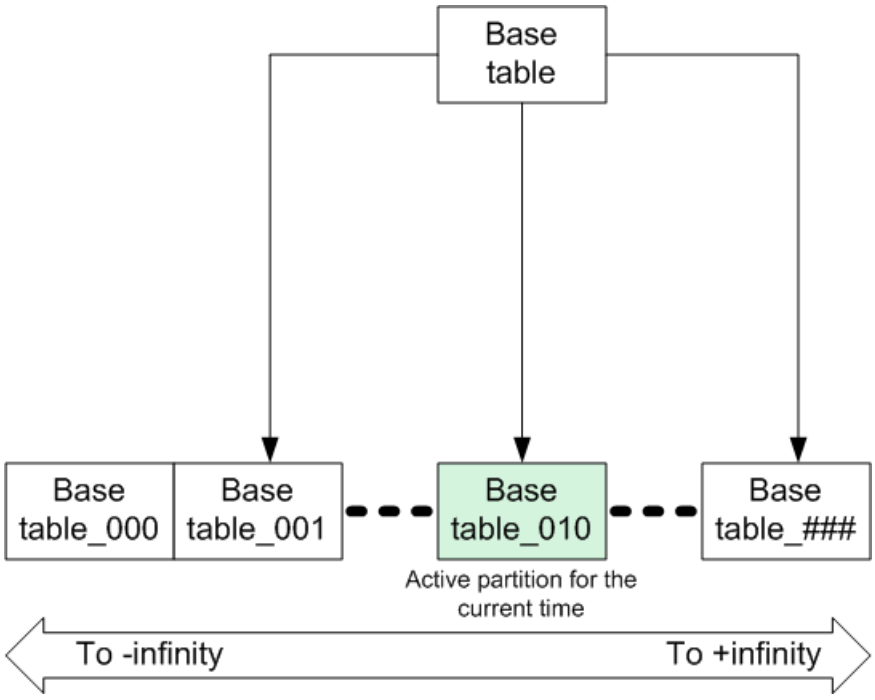


At any point in time there is always:

- one active partition to which rows are inserted
- some partitions allocated to past time intervals that may or may not contain data
- some partitions allocated to future time intervals that do not contain data

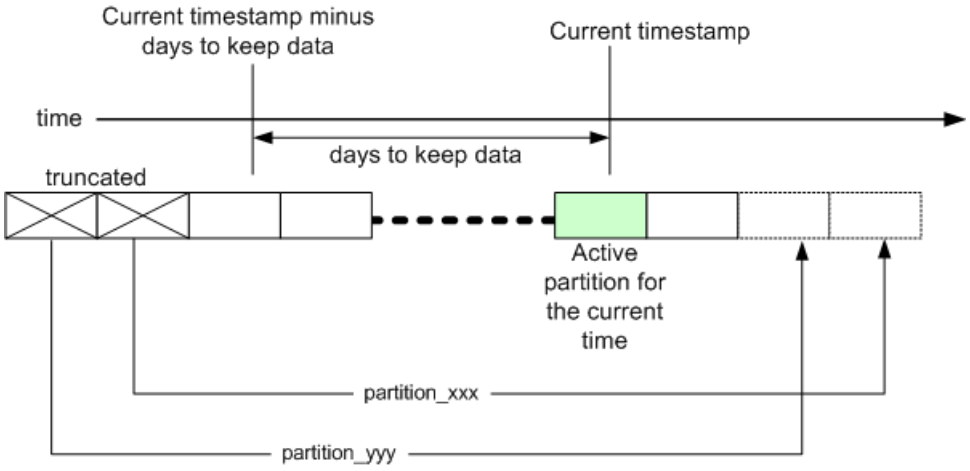
Rolling partitions allows the database to use a more-or-less fixed amount of space. On a regular basis, the data from old partitions is truncated and the empty partitions are then allocated to a future time interval. In this way, the set of partitions always spans a contiguous window of time that contains the current time.

When the statistics database is initially laid out, all partitions for a given base table are allocated (in order) to increasing, consecutive time intervals of some default size.



These same heuristics govern how you truncate and allocate (that is, recycle) partitions. All base tables that are partitioned have an entry in the */usr/local/sandvine/etc/dataRetention.conf* configuration file along with an integer value indicating the number of days to retain data.

If there are partitions allocated further into the past than what is specified by this value (data that is older than the specified retention period), then truncate the data in those partition(s) and re-allocate them to the future.



A scheduled job, running hourly at five minutes past the hour, handles partition truncation and allocation. This issues a script to truncate expired partitions and allocate new ones. Note that on any given execution of the job, there is no guarantee that any partition recycling will take place. However, each execution of the job ensures that the specified configuration parameters are honored.

6.2 Digest Tables

The SPB automatically creates digest summary tables of interval-based statistics.

The digest tables enable more efficient database queries when looking at statistics over long periods of time and allow the SPB to retain statistics over a longer period of time for a given amount of disk storage. These digest tables are identical in layout to the detailed statistics initially loaded into the database, but the measurements are aggregated up to a coarser time granularity. For example, these rows of details in the first table are aggregated into the two rows in the second digest table:

Network Element ID	Period Start	Period End	Rx bytes	Tx bytes
1	‘2012-12-02 00:00:00’	‘2012-12-02 00:15:00’	8686	1895
2	‘2012-12-02 00:00:00’	‘2012-12-02 00:15:00’	4076	868
1	‘2012-12-02 00:15:00’	‘2012-12-02 00:30:00’	6339	8535
2	‘2012-12-02 00:15:00’	‘2012-12-02 00:30:00’	156	7759
1	‘2012-12-02 00:30:00’	‘2012-12-02 00:45:00’	8719	4076
2	‘2012-12-02 00:30:00’	‘2012-12-02 00:45:00’	2306	6309
1	‘2012-12-02 00:45:00’	‘2012-12-02 01:00:00’	9463	3355
2	‘2012-12-02 00:45:00’	‘2012-12-02 01:00:00’	7774	127
1	‘2012-12-02 01:00:00’	‘2012-12-02 01:15:00’	7057	5348
2	‘2012-12-02 01:00:00’	‘2012-12-02 01:15:00’	22398	2458
1	‘2012-12-02 01:15:00’	‘2012-12-02 01:30:00’	291	5081
2	‘2012-12-02 01:15:00’	‘2012-12-02 01:30:00’	3072	9671
2	etc	etc	7175	
1	etc	etc	1194	
1	‘2012-12-02 02:45:00’	‘2012-12-02 03:00:00’		8886
2	‘2012-12-02 02:45:00’	‘2012-12-02 03:00:00’		1445

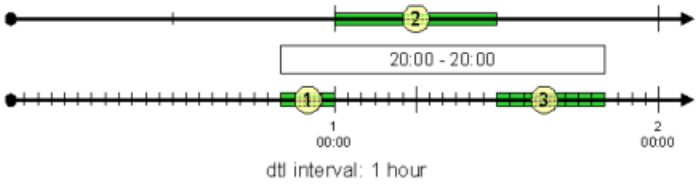
Network Element ID	Period Start	Period End	Rx bytes	Tx bytes
1	‘2012-12-02 00:00:00’	‘2012-12-02 03:00:00’	39260	37607
2	‘2012-12-02 00:00:00’	‘2012-12-02 03:00:00’	43393	41566

Once a digest level entry is created, if you delete the lower level digests or detail records, that time granularity becomes coarser. However, as finer granularity is generally more desirable, the SPB defaults to retain this content in the database:

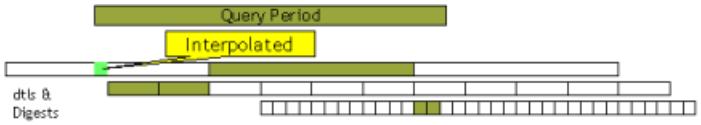
- Detailed statistics - These are kept for approximately one month.
- First level digest statistics - These are kept for six months.
- Second level digest statistics - These are kept for a period of three years.

The SPB creates the digest tables as soon as there is sufficient data in the digest or detail level below it to build the next digest interval. As such, the digest levels time period significantly overlaps the underlying detail rows. The SPB has information about the various digests and what periods of time they cover and uses this information when building queries to run against the database.

For example, if you query the SPB for the sum of rx_bytes over a day for subscribers sometime in the past month, the SPB reduces its I/O to the database by reading some data from the digest level and the rest from the details without sacrificing accuracy. The SPB then breaks the request into three separate statements and aggregates the results. This query is generally faster than just accessing the details alone due to the reduced I/O required. For example, this is a query request broken into three statements:

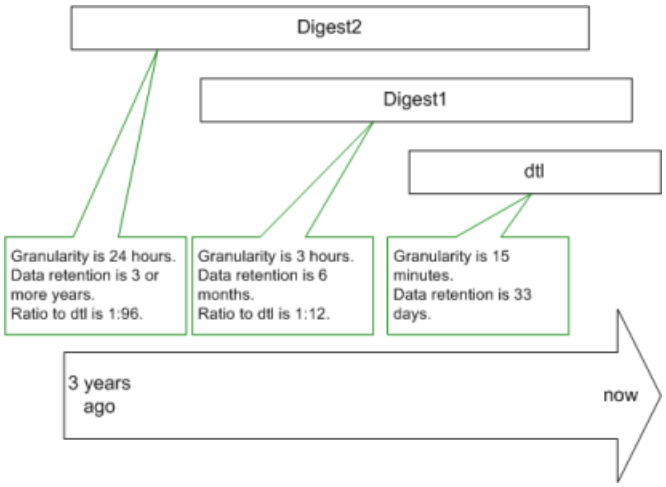


In cases where a request for data spans a period of time that does not align to the start and/or end of an interval, the SPB interpolates the result. As shown in the diagram below, statistical data for the start of the query period is only available at the second digest level. The time granularity of that interval means that the SPB takes the value it has for the entire interval, and interpolates an amount based on the proportion of the interval that it needs. For example, given that the interval size is 12 hours and the value for the interval is 12 000, if we need one hour of data from that interval, then the SPB will interpolate a value of 1000.



Because data retention is configurable at all digest levels, customers can balance their data retention needs with their desire for detail.

As shown here, significant savings are possible in the overall storage required to retain a given amount of statistic data at these different granularities.



Although you can use configuration files to change the interval size at the detail level, digest interval sizes are currently fixed. This results in two important effects:

- The detail interval size must be an integer multiple of the digest level.
- The detail interval size may not be configured larger than the interval size of the first digest level.

So, if the interval size of the first digest level of a statistic is 3 hours, the suggested detail level interval sizes is one of 5, 10, 15 (default), 30, 60, 90, or 180 minutes. Note that this is not the complete list of all possible interval sizes.

Warning: There can be serious implications to statistics collection performance if the interval size is set lower than the default (15).

If space in the database is at a premium, then it is usually desirable to decrease the retention of the first level statistics. This allows us to still keep statistical data for a long period of time, without sacrificing some fine level time granularity. If the SPB receives a request for data where an endpoint is somewhere in the middle of an interval, the SPB interpolates the measurement value as a percentage of the interval size.

7

Security

7.1 Web Services API

Sandvine provides a web services API that simplifies integration with operational support systems and other external systems.

The user ID "spbuser" has read-only permissions and authenticates only lookup requests. The user ID "spbadmin" authenticates all requests made to the web services API. Each request must carry the user ID and password in the Simple Object Access Protocol (SOAP) header, as shown here for the "spbadmin" user:

```
 <soap-env:Envelope

xmlns:soap-env=”http://schemas.xmlsoap.org/soap/envelope/”

xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance"

xmlns:xsd="http://www.w3.org/2001/XMLSchema"

xmlns:ns1="http://ws.reportingservices.sandvine.com">

    <soap-env:Header xmlns:svns1="http://services.sandvine.com">
        <svns1:username>spbadmin</svns1:username>
        <svns1:password>mypass123</svns1:password>
    </soap-env:Header>
    <soap-env:Body>

        ...
    </soap-env:Body>
</soap-env:Envelope
```

On the SPB server, PAM checks these credentials. By default, PAM is pointed to the local FreeBSD authentication.

7.2 Database Security

PostgreSQL database users have no password by default. If you choose to enable password protection, all database users must have a password. SRP elements within a cluster must use the same user/password combination.

If you have enabled passwords in the system and are downgrading to a release prior to 5.60.04, you must remove the passwords before downgrading.

To discover current database users and determine if a password is set for the user, run the `show service database users` CLI command. The output for this command is:

- Username – The database user name for a given account
- PasswordProtected – Whether the account is password protected
- Description – A brief description of the function of the user, if such a description is available

7.2.1 Setting Database Passwords

If you choose to enable password protection, then all database users must have a password. SRP elements within a cluster must use the same user/password combination.

1. Optionally, enable SSL encryption between the application server and the database server. Run this command in CLI configuration mode to configure the application server to connect to the database using SSL encryption:

   ```
   set config service database ssl enabled true
   ```

   See the PostgreSQL documentation (www.postgresql.org) for information on enabling SSL encryption on the database.

2. To enable password protection on the database, perform these steps on each database server in the cluster:

   a. Run this CLI command to edit */usr/local/pgsql/data/pg_hba.conf* so that all entries in the Method column are set to trust:

      ```
      edit service database authentication
      ```

   b. Reload PostgreSQL using this CLI command:

      ```
      reload service database
      ```

   c. In CLI configuration mode, run this command and input a password at the prompts:

      ```
      set service database password
      ```

      You can expect an output similar to this:

      ```
      SRP> set service database password
      Database user: svadmin
      Current password:
      New password:
      Confirm new password:
      The following local services were configured:
      Service
      ------------------
      Default Services
      Database
      Detected the following database authentication configuration:
      Type  Database User CIDR-Address       Method
      ----- -------- ---- ------------------ ------
      local all      all                     trust
      host  all      all  127.0.0.1/32       trust
      host  all      all  ::1/128            trust
      local sv_stat  all                     trust
      host  all      all  10.0.0.0 255.0.0.0 trust
      host  all      all  40.0.0.0 255.0.0.0 trust
      host  all      all  0.0.0.0 0.0.0.0    trust
      ```

3. On all application servers in the cluster, run this CLI command:

   ```
   set service database password
   ```

   This command configures the application server to use the new password when connecting to the database. You can expect an output similar to this:

   ```
   The following services were configured:

   Service
   --------
   Default Services
   Application Server
   ```

4. On all database servers in the cluster:

a. Run this CLI command to edit */usr/local/pgsql/data/pg_hba.conf* so that all entries in the Method column are set to password:

```
edit service database authentication
```

b. Run this CLI command to reload PostgreSQL:

```
reload service database
```

7.2.2 Removing Database Passwords

If you choose to disable password protection, you must also disable all database user passwords. To do this:

1. Optionally, disable SSL encryption between the application server and the database server. Run this command in CLI configuration mode to disable SSL on the SPB:

```
set config service database ssl enabled false
```

See the PostgreSQL documentation (www.postgresql.org) for information on disabling SSL encryption on the database.

2. To disable password protection on the database, perform these steps on each database server in the cluster:

a. Edit */usr/local/pgsql/data/pg_hba.conf* so that all entries in the Method column are set to trust.

b. Reload PostgreSQL using this CLI command:

```
reload service database
```

c. Run this command in CLI configuration mode and use the keyword "none" or an empty value to input an empty password:

```
set service database password
```

You can expect an output similar to this:

```
SRP> set service database password
Database user: svadmin
Current password:
New password:
Confirm new password:
The following local services were configured:
Service
------------------
Default Services
Database
Detected the following database authentication configuration:
Type  Database User CIDR-Address       Method
----- -------- ---- ------------------ ------
local all      all                     trust
host  all      all  127.0.0.1/32       trust
host  all      all  ::1/128            trust
local sv_stat  all                     trust
host  all      all  10.0.0.0 255.0.0.0 trust
host  all      all  40.0.0.0 255.0.0.0 trust
host  all      all  0.0.0.0 0.0.0.0    trust
```

3. Run this CLI command on all application servers in the cluster. Use the keyword “none” or an empty value to input an empty password.

```
set service database password
```

You can expect an output similar to this:

```
The following services were configured:

Service
--------
Default Services
Application Server
```

4. Commit the changes:

```
commit
```

7.3 Internal SPB Security

The message broker is responsible for internal SPB security.

All JMS connections pass through SSL and the client must pass the user ID and password into the JMS connection. Credentials are authenticated via PAM. Every subsequent request must also carry sbpadmin credentials, which pass through the same PAM authentication as the public web services API.

You can optionally configure database connections to pass through SSL, but this functionality is disabled by default. See *Database Installation and Configuration* on page 76 to enable this functionality.

7.4 Network Security

The SPB server requires accessibility through certain ports for external clients such as PTS elements, Network Demographics and any external applications using the SPB API.

When configuring firewall rules for the SPB server, ensure access remains available for external clients. The standard default ports that require access are:

- 8443 for SPB API access to HTTPS
- 2507 for PTS element access to the SPB

You can enable additional ports, depending on the configuration of the particular installation.

8

Maintenance

8.1 Network Throughput Requirements

Network throughput requirements are based on communication between the SPB and PTS.

Communication consists of:

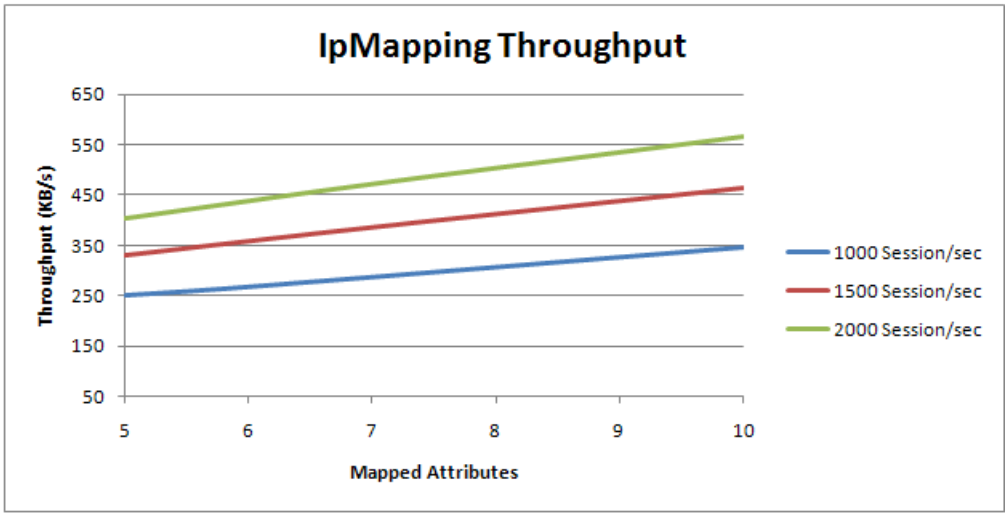
- Notifications – The SPB sends change notification messages to the PTS for every IpAssignment, IpUnassignment, and AttributeChange operation.
- Subscriber Lookup Requests – The PTS sends these requests to the SPB for subscribers that have not been mapped by change notifications.
- Subscriber Lookup Responses – The SPB sends these responses that are sent back to the PTS.
- Attribute Set Requests – The PTS sends these requests to the SPB when SandScript changes an attribute. In turn, the SPB generates change notification to notify all PTSs that the attribute has changed.
- Stat Publication Messages – The PTS publishes these messages to the SPB at regular 15 minute and 1 hour intervals.

8.1.1 IP Mapping Network Throughput Requirements

Both the session rate and the number of attributes set for each subscriber login/logoff impact IP Mapper throughput requirements.

These requirements assume that each attribute is set when the subscriber logs in and again when the subscriber logs out. Each session is defined as one login and one logout. The length of each attribute value is 10 characters long, and each value is unique.

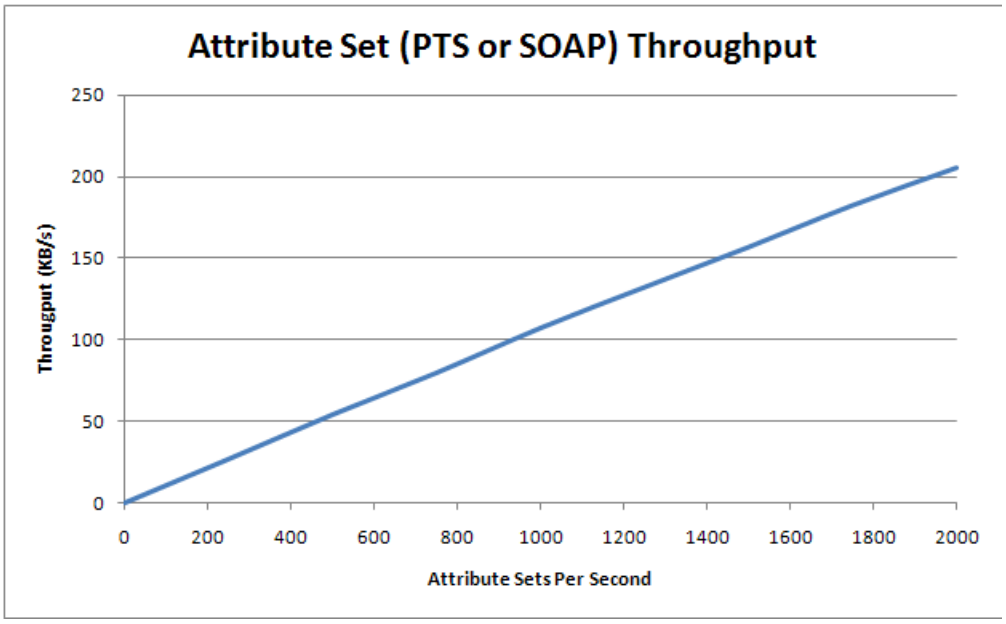
Throughput requirements include change notification and subscriber lookup requests required at the given session rate. This graph plots the throughput requirements versus the number of attributes being set on login and logoff for three different session rates:



8.1.2 Attribute Set Network Throughput Requirements

The number of attribute set requests that an SPB datahome handles will impact the bandwidth requirements to each PTS.

You can change attributes in SandScript on the PTS or through web service operations on the SPB. Each attribute change generates a change notification to be sent to all PTSs connected to the datahome. This graph plots the throughput requirements for a single PTS versus the number of attribute sets being processed by the datahome.

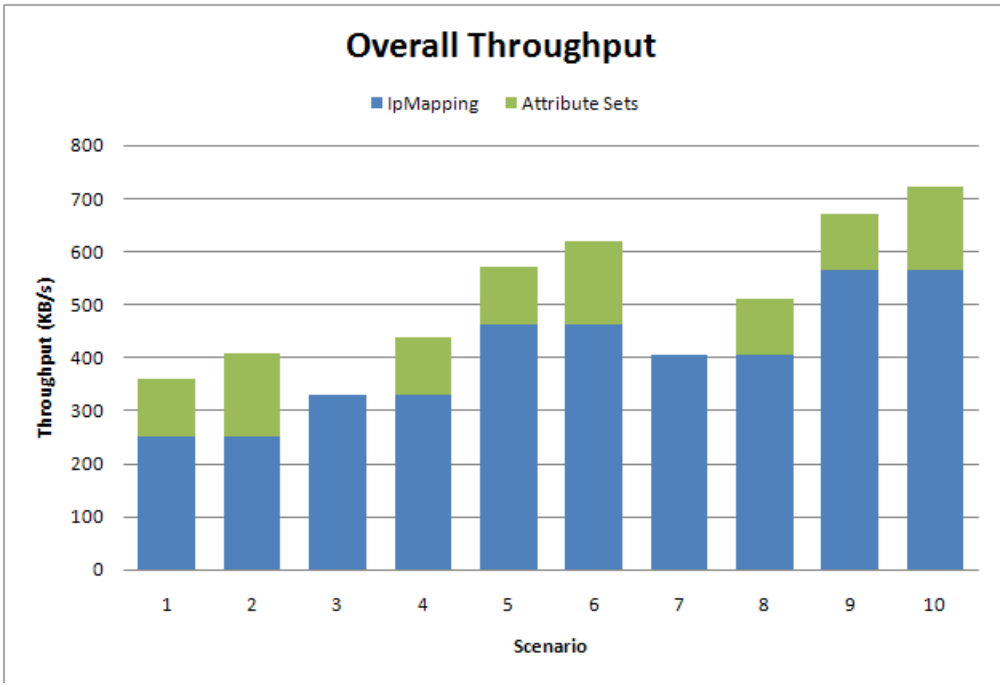


Typically, multiple attribute sets are batched together in a message. These requirements assume that the sets are batched together in groups of 15.

Note that the attribute set bandwidth requirements are in addition to the IP mapping requirements above. The total requirement of the PTS-SPB connection is the sum of these two requirements.

8.1.3 Overall Throughput Requirements

This chart shows how you can combine the IP mapping and attribute set requirements in various scenarios to determine the overall throughput requirement for the SPB-PTS connection.



The throughputs are:

Scenario	IP Mapping Session Rate	IP Mapped Attribute	Attribute Sets	Throughput (KB/s)
1	1000	5	1000	359
2	1000	5	1500	408
3	1500	5	0	330
4	1500	5	1000	437
5	1500	10	1000	570
6	1500	10	1500	620
7	2000	5	0	404
8	2000	5	1000	511
9	2000	10	1000	672
10	2000	10	1500	722

8.2 PTS Element Reporting

PTS elements report various statistic types to the SPB server at a regular interval.

The statistics are stored in the database for subsequent reporting. The last logged time for a PTS element provides information concerning the ability of the PTS to communicate with the SPB. The last log interval for PTS elements is available via the Network Demographics server.

The Network Demographics report lists each PTS cluster and element combination that has reported statistics to the SPB. Communication issues between the PTS and the SPB are usually responsible when a PTS element is missing from the list. The date indicated represents the last interval that the PTS element reported, regardless of the type of statistic.

Note:
After adding a new network-element to the SPB, or changing an existing network-elements cluster or host name, the SPB may not process the first set of statistics. Subsequently, the SPB will expect statistics from that network element.

8.2.1 Running Network Demographics Reports

The Network Demographics report lists each PTS cluster and element combination that has reported statistics to the SPB.

1. Launch your preferred supported browser.
2. Enter the IP address of the reports server.

   `http://x.x.x.x:y/reports`

   where:
   - x.x.x.x is the IP address of the SPB server where Network Demographics is installed
   - y is the port number that Network Demographics is listening on. The default port is 8080.
3. On the Sandvine Network Demographics login screen, enter a username and password.
4. Click **Login**.

   If the login is successful, the Network Demographics navigation pane and splash page will appear.
5. In the Advanced Reports navigation tree, under **Resource Monitoring** > **Events**, select the **Last Log Interval** report.
6. Run the report.

Note:
You can also configure third-party applications to run reports on the SPB through SOAP APIs. If you close the Network Demographics browser or terminate the third-party application before the report generation is complete, the database query continues to run in the server and consumes system resources. To avoid this, the SPB monitors the client sessions and automatically terminates reports running in the server if you terminate a client session. You can also use this CLI command to delete a running report:

```
delete service reporting request-id <request-id>
```

8.3 Database Backup

As part of ongoing disaster recovery support, you should back up your database. A backup is best suited for recovering statistics data, because IP mapping or subscriber attribute data often changes too frequently to be useful when restored.

You can safely run a backup at any time without interrupting the running database. However, since a large database may take some time to save its contents to a file, schedule the backup for a period during which the database is not being heavily used for generating reports.

Note:

If a SRP is deployed as the database server, RAID-10/RAID-5 implementations should make the need for restoring the database minimal. It is strongly recommended that you mirror the database to another machine via the warm standby technique as described in *Configuring Warm Standby System* on page 81. For more information, contact Sandvine Customer Support or its authorized partner.

In the event the backup is used for a restore, data retention policies may affect the back-up data at the time of the restore. In some cases where time has elapsed between the time the backup was taken and the time the restore was performed, data truncation on the database may have removed partitions where some data in the backup is intended to reside. In those cases where data is dropped on the restore, appropriate messages appear in the database log.

8.3.1 Backing up the Database

Pre-requisite:

To back up the Sandvine database you will need:

- IP address of the database server
- PostgreSQL admin account login name
- A control network computer that runs a secure shell (SSH) program

1. As an administrative user, connect to the database server.
2. To back up the database, at the command prompt enter:

   ```
   pg_dump -Fc -f svdata.db -U pgsql sv_stat
   ```

   This command dumps a copy of the database to a file called svdata.db. Do not change the command options.
3. If desired, to copy the backup file to another server, enter:

   ```
   scp svdata.db user@<hostname>:/path
   ```

   Where:

   - scp is the secure copy command.
   - svdata is the name of the backup file to be copied.
   - user@ indicates a connection to the host as the specified user. You will need the password for the specified user.
   - <hostname> is the name or IP address of the server to connect to.
   - /path is the directory path to the target location.

8.3.2 Restoring a Database

Pre-requisite:

To restore the Sandvine database you will need:

- IP address of the database server
- PostgreSQL admin account login name
- A control network computer that runs a secure shell (SSH) program

Note:

If a SRP is deployed as the database server, RAID-10/RAID-5 implementations should make the need for restoring the database minimal. It is strongly recommended that you mirror the database to another machine. For more information, contact Sandvine Customer Support or its authorized partner.

1. If necessary, copy the svdata.db file from the host where it is saved to the database server. Use the command:

   ```
   scp user@hostname:/path1/svdata.db /path2
   ```

   Where:

   - scp is the copy command
   - user is the user name to connect to the host where the backup file is saved
   - hostname is the name of the host where the backup file is saved
   - path1 is the path to the svdata.db file on the host
   - path2 is the target for the copy (the current directory on the database server).

2. On the SRP-receiver, run these commands to stop the application server and the message broker:

   ```
   stop service application-server
   stop service message-broker
   ```

3. Put the CLI in configuration mode and run this command to turn off the truncollator.

   ```
   SRP> configure
   SRP# set config service truncollator enabled false
   ```

4. If autovacuum is on, run these CLI commands to disable it, else proceed to the next step:

   ```
   SRP# set config service database auto-vacuum enabled false
   SRP# commit
   ```

   Committing configuration changes can potentially impact service.

5. On the SRP-receiver, issue this command, then select **y** at the prompt to permanently remove the database:

   ```
   dropdb -U pgsql -i sv_stat
   ```

   The output is:

   ```
   Database "sv_stat" will be permanently removed.
   Are you sure? (y/n)y
   DROP DATABASE
   ```

   If the database no longer exists or was not installed on the server that the data is restored to, you can ignore this message:

   ```
   dropdb: database removal failed: ERROR: database "sv_stat" does not exist
   ```

6. On the SRP-receiver, run these commands:

   ```
   createdb -U pgsql -E 'UTF8' -O pgsql sv_stat
   pg_restore -d sv_stat -U pgsql svdata.db
   ```

7. Wait for the restore process to complete.

8. If autovacuum was turned off in step 4, run these CLI commands to restore it; otherwise proceed to the next step.

   ```
   SRP> configure
   ```

   ```
   SRP# set config service database auto-vacuum enabled true
   SRP# commit
   ```

   Committing configuration changes can potentially impact service.

9. If truncollator is needed, enable it by running these CLI commands:

```
SRP# set config service database auto-vacuum enabled true
SRP# commit
```

Committing configuration changes can potentially impact service.

10. On the SRP-receiver, issue:

```
start service application-server
start service message-broker
```

8.4 Checking the Status of a Warm Standby System

At any time while the primary database server is live, the archive process on the primary server ships database log files to the standby server, while the restore process on the standby server replays the received log files. It is a good practice to periodically check the status of these processes.

Under normal operation, the observed lag times should be less than 60 seconds. Delays greater than 60 seconds should be temporary and brief.

8.4.1 Checking the status of the archive process

As an administrative user, login to the primary server and run the command:

```
SRP> show service warm-standby status
```

Output to the console should be similar to:

```
PRIMARY DATABASE
================

LastArchivedFile   : 000000010000000000000000F
FileModifyTime     : 2013-08-26 12:19:53 IST
ArchiveStartTime   : 2013-08-26 12:31:45 IST
ArchiveCompleteTime: 2013-08-26 12:31:46 IST
TimeNow            : 2013-08-26 12:31:46 IST

ARCHIVE LAG TIMES
=================

FileCompleteToArchiveStart   : 712 s
ArchiveStartToArchiveComplete: 1 s
LastArchiveComplete          : 0 s

Standby server has all data up to 713 seconds ago.

Checking the status of the restore process
```

As an administrative user, login to the standby server and run the command:

```
SRP> show service warm-standby status
```

Output to the console should be similar to:

```
STANDBY DATABASE
================

LastRestoredFile   : 000000010000000000000015
FileModifyTime     : 2013-08-26 12:31:46 IST
RestoreStartTime   : 2013-08-26 12:32:35 IST
RestoreCompleteTime: 2013-08-26 12:32:35 IST
TimeNow            : 2013-08-26 12:32:38 IST

RESTORE LAG TIMES
=================

FileCompleteToRestoreStart   : 49 s
ArchiveStartToRestoreComplete: 0 s
LastRestoreComplete          : 3 s

Standby server lags primary server by 52 seconds
```

8.5 Manually Failing Over to a Standby Server

It is possible to manually bring the standby server up live to take over operations for the primary server.

Since there may be committed transactions on the primary server recorded in database log files not yet shipped before the primary server went down, there is the possibility of some data being lost. Nevertheless, the standby server will have a near-current copy of the database and can be brought up live immediately.

1. As an administrative user, login to the standby server.

2. Run this CLI command:

   ```
   set service warm-standby failover
   ```

3. At the warning prompt indicating that this action may result in some data loss and should only be performed in the case of an unrecoverable failure on the primary server, enter **Y** (yes) to continue.

   Output to the console should be:

   ```
   Initiating database failover ...
   Database failover complete
   ```

4. As an administrative user, login to all application servers that were connected to the primary database.

5. Put the CLI into configuration mode.

6. Set the data source host to be the IP address of the new database server (former standby). For SPB database failures, run the command:

   ```
   set config service database ip-address <ip-address>
   ```

7. Run this CLI command:

   ```
   reload
   ```

Application servers should establish connections with the new database server and the system should return to normal operation. If operations do not return to normal within an hour, contact Sandvine Customer Support or its authorized partner.

8.6 Automatic Database Failover

The database can be made to automatically failover to a standby database server.

The automatic failover mechanism provides link and application awareness by configuring database redundancy using VRRP and by database monitoring techniques. This setup minimizes service interruptions due to database failures in the primary database server or with interface failures on the primary database server.

The failover process raises alarms to notify the administrator about events that occurs in the failover setup. After failover to a standby server, manual intervention is required to fix the failure, reconfigure the warm standby server, and enable database monitoring.

Note:
If both IP mapping failover and database failover are required, you must have a four-element deployment: two elements for SPB clustering and two elements for database failover. If you have a two-element deployment, you can configure IP mapping failover or database failover, but not both.

8.6.1 Interface or PostgreSQL Database Failure

If the network interface or the PostgreSQL database fails on the primary database server, the standby database server should detect the failure and promote itself as the new primary database.

The process when the network interface or PostgreSQL database fails is:

Step	Description	DB-A VRRP Status	DB-B VRRP Status
1	In the initial state, DB-A is VRRP primary database and DB-B is the standby.	primary with priority of 254	standby with priority of 254
2	The network interface or the PostgreSQL database fails on DB-A.	failure	standby
3	The failure is detected and failover begins.	priority of 0	primary
4	The operator receives an SNMP notification (PrimaryDatabaseDown) to solve the problem on DB-A.	not in cluster	primary
5	The operator receives an SNMP notification (LogShippingDown) to configure log shipping on DB-B as it is the new primary database server.	not in cluster	primary
6	Once the base backup is complete and the database recovery process has started, the operator issues the CLI command `set service db-monitor join-cluster` on DB-A.	standby with priority of 254	primary with priority of 254
7	The operator must start the database monitoring on DB-A using the `set service db-monitor start` CLI command.	standby with priority of 254	primary with priority of 254

8.6.2 Package Upgrade – svupdate

Software package updates may require a reboot of the system which can cause system downtime unless the administrator manually triggers a failover.

If the database schema is being updated, the automatic failover configuration detects the database upgrade and automatically turns off database monitoring to prevent failover during the schema upgrade. After the schema package is complete, database monitoring will resume. In brief, the update process is:

1. If the update includes a database schema:
   - Update the schema package on the primary server.
   - Wait until the update is automatically synced to the standby server via the archiving process.
2. Update the standby server.
3. Trigger a failover.
4. Update the primary server.

To handle platform package updates in database server:

Step	Description	DB-A VRRP Status	DB-B VRRP Status
1	In the initial state, DB-A is VRRP primary database and DB-B is the standby.	Primary with priority of 254	Standby with priority of 254
2	Perform an `svupdate` on the standby database server DB-B and reboot the device after the update is complete.	Primary	Standby
3	WAL files on DB-A build up while the DB-B (standby) is rebooting. After the reboot, wait for the standby server to synchronize. Run the `show service warm-standby status` CLI command to check the status of archiving.	Primary	Standby
4	Once the DB-B is back online, it is ready to update the DB-A. Run the CLI command `stop service ip-redundancy` on DB-A to force fail-over.	Not in cluster	Primary
5	Perform an svupdate on DB-A and reboot the device after the update is complete.	Not in cluster	Primary
6	Configure log shipping from DB-B to DB-A.	Not in cluster	Primary
7	Once the base backup is complete and database recovery has started, perform the CLI command `set service db-monitor join-cluster` on DB-A.	Standby	Primary
8	Start the database monitoring in DB-B. Perform the CLI command `set service db-monitor start`.	Standby with priority 254	Primary with priority 254

Note:
Restarting the sv_stat database on the warm standby server fails. An error message appears stating that you can ignore this error if you do not intend to run Postgres. This is an expected behavior.

8.6.3 Reconfigure after Failover

After failover, manual intervention is required to configure the warm standby server and enable database monitoring in the new primary database server.

Database backup should be complete in the new standby server before adding it to the database redundancy cluster. To restore the automatic warm standby failover:

Step	Description	DB-A VRRP Status	DB-B VRRP Status
1	After failover, DB-B is the primary database server. The administrator can rectify the fault in DB-A or assign a new hardware for DB-A.	Not in cluster	Primary with priority 254
2	Configure the IP address of DB-A in DB-B. Issue this CLI command: `set config service warm-standby server <ip-address>`	Not in cluster	Primary
3	Configure log shipping from DB-B to DB-A. See *Configuring Warm Standby System* on page 81	Not in cluster	Standby
4	If DB-A was the old primary, it will have the warm standby configurations. So it is ready to join the cluster. Perform the CLI command `set service db-monitor join-cluster` to add DB-A to database redundancy cluster. If DB-A is a new hardware, automatic warm standby failover parameters should be configured. See *Configuring Automatic Database Failover* on page 84.	Not in cluster	Primary
5	Start the database monitoring in DB-B. Perform the CLI command: `set service db-monitor start`	Standby with priority 254	Primary with priority 254

8.6.4 Database Failover SNMP Alarms

SNMP alarms are raised by the failover process to notify the administrator of the various events that occur.

The database alarms are:

- svDbWarmstandbyDbMonitoringDownAdministratively – This is raised when the administrator stops primary database monitoring from the CLI interface.
- svDbWarmstandbyPrimaryDatabaseDown – This is raised on the primary database server when failure has occurred and failover has been initiated. This alarm is raised on the standby database server when auto failover setup fails to start the standby database server as the primary database.
- svDbWarmstandbyLogShippingDown – This is raised to alert the administrator to configure warm standby and enable database monitoring.

8.6.5 CLI Commands to Manage Database Failover

The `set service db-monitor` CLI commands manage and maintain automatic database failover.

8.6.5.1 set service db-monitor

Sets database monitoring functions.

Syntax

```
set service db-monitor config reload
set service db-monitor join-cluster
set service db-monitor restart
set service db-monitor start
set service db-monitor stop
```

Attribute	Function
config reload	Reload a database monitor configuration
join-cluster	Join a database monitor to a cluster
restart	Restart a database monitor
start	Start a database monitor
stop	Stop a database monitor

8.7 Changes to Network Elements and Clusters

If a network element or cluster name is changed, you should deactivate the old element or cluster.

Once deactivated, the SPB no longer expects statistics from these elements, allowing statistic intervals to be closed in a timely fashion. If you do not deactivate the elements, statistic intervals remain open until the waiting period passes, resulting in a delay in the statistics becoming available for reports.

You can obtain the names of the elements and clusters using these CLI commands:

```
show network-element-cluster
show network-element
```

Note:
The name of a network element is used as a unique key. Therefore, network element names must be unique within a cluster of network elements. For example, an SDE and a PTS cannot have the same name. To avoid potential loss of published statistics and misleading output from the `show network-element` CLI command, ensure that each network element in a cluster has a unique name.

You can deactivate the element or the cluster using this CLI command:

```
set network-element deactivate cluster <clusterName> element <elementName> deactivate
```

8.8 Discovering New Network Elements and Clusters

If you add new network elements and clusters, the SPB automatically discovers them as part of the statistics collection. It may take some time for the Network Demographics reporting cache to expire and the new network element or cluster to appear in the Network Demographics configuration. The default time is 30 minutes.

8.9 Changing the IP Address of an SPB Server

If you change the IP address of an SPB server in a cluster, perform these steps after configuring the new IP address:

1. Run this command on the SPB server with the changed IP address:

   ```
   show config service application-server bind-address
   ```

   If the output displays the old IP address, run this command to configure the bind address:

   ```
   set config service application-server bind-address <ip-address>
   ```

   where <ip-address> is the new address of the server.

2. In a clustered deployment, run these commands on all the nodes in the cluster:

   ```
   set config cluster domain-manager <ip-address>
   set config cluster servers <servers>
   ```

   where:

   - <ip-address> is the new IP address of the SPB server.
   - <servers> is a space-separated list of server IP addresses in the cluster, with the old IP address replaced by the new one.

3. Run this command on the database server:

   ```
   set config service spb servers <servers>
   ```

8.10 SPB Database Schema Updates

The generic database schema update procedure provides a mechanism to replace one database schema with another. This update mechanism is extremely versatile; however, it takes a minimum of 45 minutes to compare one version of the schema to another. It might also introduce downtime at indeterminate times for extended durations.

Low-impact schema update is an extension to the existing generic database upgrade/downgrade mechanism. The low-impact schema update mechanism does not involve any database downtime and takes significantly less time. The time taken for an update depends on the extent of differences in the schema and usually completes in 5-10 minutes. This mechanism is applicable when a supported update path is available. In case of failures, such as system reboot, power failure, or low disk space, the schema rolls back to the initial state, and you can view appropriate error messages in the console and log files.

Use the generic schema update mechanism only if the low-impact schema update mechanism fails or cannot be applied.

8.10.1 Schema Update CLI Commands

You can use these CLI commands for viewing schema updates and running the schema update processes.

8.10.1.1 show service database status

Shows the current database status, including the status of the latest schema update. In the command output, **SchemaVersion** should be equal to **PackageVersion** unless an update is currently in progress. An alarm will be raised if these output values differ.

8.10.1.2 show service database schema-update history

Shows the history of database schema upgrades and downgrades that have occurred.

8.10.1.3 set service database schema-update

Manually runs or reruns the low-impact schema update process. You can track the progress of the update process in the */var/log/svdbupdate.sv_stat.<date_time>.log* files. If the database schema is already updated, a message appears in the log and no action takes place.

8.10.1.4 set service database schema-update generic

Manually runs or reruns the generic schema update process. You can track the progress of the update process in the */var/log/upgrade.sv_stat.<date_time>.log* files. This process requires exclusive access to the database and generally runs for at least 1 hour, even if there are no database schema changes. Run this command only after consulting with Sandvine Customer Support or its authorized partner.

9

Monitoring and Troubleshooting

9.1 Process Monitoring

The process monitor is a product feature installed as part of the SPB platform on a Middle Tier Server and provides monitoring and SNMP alarm notification of the up/down status for key configured processes running and the SPB server.

Only enabled processes are monitored for their up or down state. To enable the process monitor, as an administrative user from the command line, run the `svreload` command. If the enabled or disabled status of a process is changed in configuration, you also need to run the `svreload` command. The processes monitored are:

Abbreviation	Process Name	Description
ntpd	Network Time Protocol Daemon	Maintains time synchronization in the network.
pamd	Pluggable Authentication Module Daemon	Authenticates messages in and out of the SPB when security is enabled (default).
jboss-as	JBoss Application Server	Process for the application server.
jboss-as-wrapper	JBoss Application Server Wrapper	Watchdog process to monitor the JVM for the application server.
sonicmq-dm	SonicMQ Domain Manager	Process for the message broker - domain manager.
soncimq-dm-wrapper	SonicMQ Domain Manager Wrapper	Watchdog process to monitor the JVM for the message broker - domain manager.
sonicmq-ab	SonicMQ Application Broker	Process for the message broker - application broker.
sonicmq-ab-wrapper	SonicMQ Application Broker Wrapper	Watchdog process to monitor the JVM for the message broker - application broker.
postgres	PostgreSQL	Process for the Postgres database management system.
syslog-ng	System Message Log	Process for application and system logging.
nds	Network Demographics Server	Process for the Network Demographics server.
vrrp	Virtual Router Redundancy Protocol (VRRP)	Implements IP address sharing for hosts on a LAN.

For more information on SNMP notifications and alarm models, refer to the *SPB Alarm Reference Guide*.

9.2 Monitoring the Message Broker

These tips will help you monitor the message broker.

9.2.1 Displaying Message Broker Status

To view summary process information about the running message brokers, run the CLI command: `show service message-broker status`

Sample output is:

```
Name                                       Host        State  ConnectedSince
-----------------------------------------  ----------  ------ ----------------------
DefaultCluster.DomainManager_Container     <hostname>  Online 2013-08-28 09:11:53 IST
DefaultCluster.AppBrkr7F000001_Container <hostname>  Online 2013-08-28 09:12:07 IST
```

9.2.2 Checking Message Broker Logs

Message brokers log their output to */var/log* in the same manner as other Sandvine applications. The domain manager logs to */var/log/sonicmq.SVDomain.DomainManager_Container.log*. Application Messaging brokers have dynamically named log files, but are of the form:

```
Domain manager:/var/log/msgsrv_dm.log
Application broker:/var/log/msgsrv_ab.log
```

In normal operating scenarios, the messaging log files only output serious problems.

9.2.3 Reinitializing the Message Broker

If corruption of the message broker occurs or is suspected, it is possible to force the broker to rebuild its internal configuration. In some cases, this can repair corruption. To force the message broker to reinitialize itself, run this CLI command:

```
set service message-broker initialize
```

Warning:
Do not use this command unless Sandvine Customer Support or its authorized partner instructs you to do so.

9.2.4 Reinstalling Message Broker

In cases of file corruption or other serious mishap, you may have to re-install the message broker. If such a circumstance occurs, contact Sandvine Customer Support or its authorized partner and, only upon their direction, reinstall the module.

1. To uninstall existing infrastructure, as an administrative user, run:

   ```
   pkg_delete sonicmq-BSD-*
   ```

   This may produce an error which you can safely ignore if you want to completely remove the message broker.

2. To remove all remnants of the previous install, run these commands:

   ```
   rm -rf /usr/local/sonic
    rm -rf /usr/local/sandvine/var/sonic
    rm -rf /usr/local/sandvine/var/sonicmq
   ```

   These commands clean up anything the old install may have left behind in a corrupted state.

3. To re-install the latest **sonicmq-BSD-*** package, run the standard `svupdate` utility.

9.2.5 Error Messages

Upon restarting the message broker, these error messages may appear:

```
Attempting to configure broker(s) by connecting to domain 'SVDomain' on 'ssl://localhost:3001'
 ...
Warning: Broker '/Brokers/AppBroker1' already exists - broker will be deleted and recreated...
Warning: Unable to create new container '/Containers/AppBroker1_Container' (container already
 exists)
```

These messages provide information about what is being done in case a broker reconfigures itself. They are expected and, in most circumstances, you can ignore them.

Another error message that may appear upon restarting the message broker is:

```
WARNING: timed out waiting for Sonic to start (port: xxxx)
```

During restart, the system waits for up to two minutes polling the appropriate TCP port to see if the broker is listening. If a listener is not found during that two minute period, the warning appears. This is a warning rather than an error because it may indicate that the domain manager is down on another system, in which case, the local broker will recover. The recovery period and decision to use local configuration rather than configuration from the domain manager usually exceeds the two minutes startup.

This is an indication that something is incorrectly configured. It is only a symptom. However, you can examine the message broker and domain manager logs to identify the underlying problem.

9.3 Monitoring the Application Server

These tips will help you monitor the application server.

9.3.1 Displaying Application Server Status

The simplest way to check if the local application server is running is to run this CLI command:

```
show system services
```

This output indicates that the local application server is running:

```
Name                        AdminStatus OperStatus
--------------------------- ----------- ----------
JBoss Application Server    [up]        [online]
```

9.3.2 Checking Application Server Logs

As with all Sandvine elements, it is important to monitor */var/log/svlog*. This log file holds messages deemed important to customers. Each message in this file contains a unique MCD code that is used to obtain additional information.

9.3.3 Reinstalling the Application Server

In cases of file corruption or other serious mishap, it may be necessary to re-install the application server. If such a circumstance occurs, contact Sandvine Customer Support or its authorized partner and, only at their direction, reinstall the application server.

1. To uninstall existing infrastructure, as an administrative user, run the command:

   ```
   pkg_delete jboss-BSD-*
   ```

   This may produce an error that you can safely ignore if you want to remove the messaging infrastructure completely.

2. To remove all portions of the previous install, run the command:

   ```
   rm -rf /usr/local/jboss
   ```

   This cleans up anything the old install may have left behind in a corrupted state.

3. To re-install the latest **jboss-BSD-*** package, run the standard `svupdate` utility.

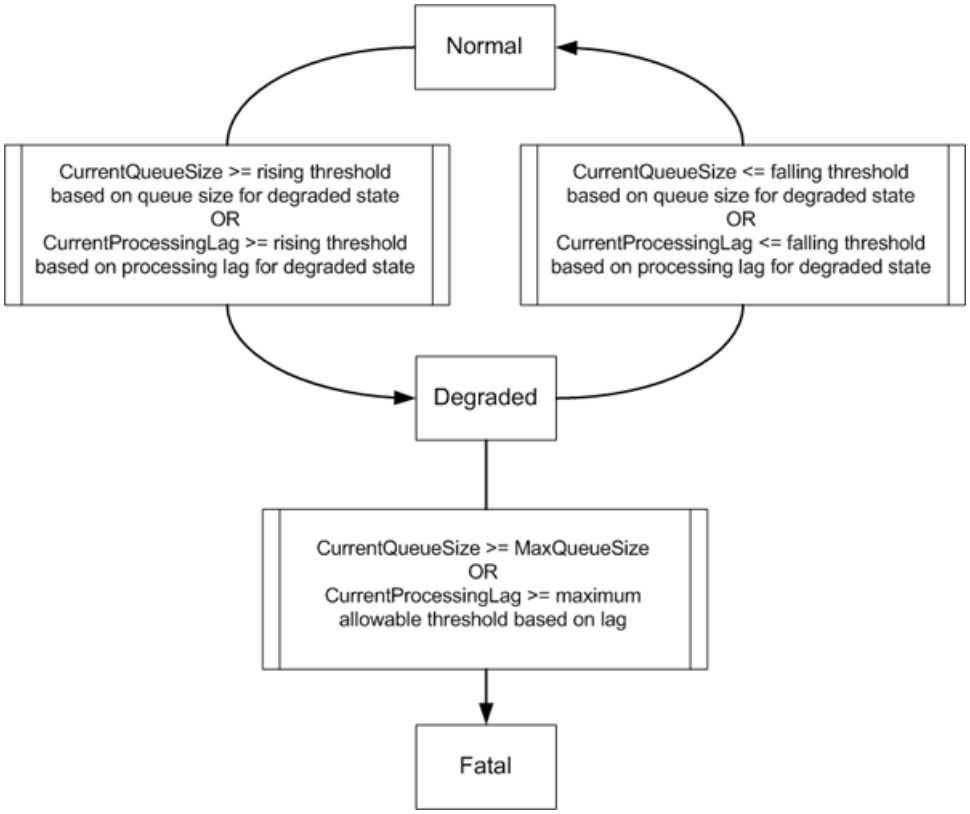
9.4 Monitoring Subscriber IP Mapping

The subscriber IP mapping process (IPUserMap) is monitored continually to ensure optimum performance.

The goal of the monitoring process is to ensure that:

- IPUserMap does not slow down significantly to the point that the subscriber-IP mappings are old and cannot be trusted.
- IPUserMap does not terminate under the load of high rate authentication traffic.

The monitoring process monitors the size of the packets queue and the current processing lag. Using this information, it cycles the IpUserMap through normal, degraded, and fatal states. The state transitions are driven by configuration variables:



9.4.1 CLI Commands for Monitoring IP Mapping

To investigate the status of IP redundancy, use this CLI command:

```
SRP> show service ip-redundancy status
VirtualRouterID: 1
Interface: em1
IPAddress: 1.0.0.9
Priority: 254
Status: Master
```

This CLI command rejoins a failed SPB to the IP redundancy cluster, after the application failure is resolved and once the database backup is complete in the new standby server.

```
SRP> set service ip-redundancy join-cluster
The SPB node joined the IP Redundancy cluster successfully.
```

Note:
You must have administrative privileges to run CLI commands on the SPB.

9.5 SPB Tips

These tips will help you troubleshoot the SPB.

9.5.1 Database Tips

These tips address some common questions about the SPB database:

Postgres Does Not Start After Rebooting SRP While a Base Backup was in Progress on page 131

PostgreSQL Disabled due to Full Disk on page 132

9.5.1.1 Postgres Does Not Start After Rebooting SRP While a Base Backup was in Progress

This error can occur in these circumstances:

1. You started a warm standby and initiated a base backup on the primary database server.
2. Before the base backup is complete, the primary database server reboots, for example as a result of a power failure.

In this situation, when Postgres on the primary database server tries to restart, it will see the backup_label file and assume that it should recover using this file. The recovery will fail because the backup_label file is incomplete, and Postgres will not be able to restart.

To confirm the problem, check for error messages in */var/log/pgsql* similar to this:

```
Jan  7 15:51:51 TPC-F17-26 postgres[12211]: [2-1] LOG:  could not open file
"pg_xlog/0000000100000A1D00000072" (log file 2589, segment 114): No such file or directory
Jan  7 15:51:51 TPC-F17-26 postgres[12211]: [3-1] LOG:  invalid checkpoint record
Jan  7 15:51:51 TPC-F17-26 postgres[12211]: [4-1] PANIC:  could not locate required checkpoint
 record
Jan  7 15:51:51 TPC-F17-26 postgres[12211]: [4-2] HINT:  If you are not restoring from a backup,
 try removing the file "/usr/local/pgsql/data/backup_label".
Jan  7 15:51:51 TPC-F17-26 postgres[12210]: [1-1] LOG:  startup process (PID 12211) was
terminated by signal 6
Jan  7 15:51:51 TPC-F17-26 postgres[12210]: [2-1] LOG:  aborting startup due to startup process
 failure
```

To correct this issue:

1. Remove the partial backup file using this command (you must have root privilege):

   ```
   rm /usr/local/pgsql/data/backup_label
   ```

2. Restart Postgres, then restart the warm standby procedure. See *Configuring Warm Standby System* on page 81.

9.5.1.2 PostgreSQL Disabled due to Full Disk

As a safeguard to protect database integrity, the database is stopped when the disk usage exceeds 99%. You cannot just delete files from this directory as that will corrupt the sv_stat database. To recover from this situation:

1. Decrease data retention values to reduce disk usage.

2. Stop the application server. As an administrative user, run this CLI command:

   ```
   stop service application-server
   ```

3. To allow PostgreSQL to start with disk usage over 99%, in CLI configuration mode set:

   ```
   SRP# set config service database auto-shutdown override enabled true
   SRP# commit
   ```

4. Restart PostgreSQL to bring up the sv_stat database. As an administrative user, run the CLI command:

   ```
   start service database
   ```

5. To reclaim disk space, manually run the truncollator to remove old files based on the updated *dataRetention.conf* file. Run the CLI command:

   ```
   set service truncollator run
   ```

6. Confirm that the truncollator has reallocated partitions and successfully completed by checking the entries in */var/log/cron*. Check for errors such as:

   ```
   Value provided is not an integer (14)
   ```

   If you do not see any entries saying that partitions are reallocated after the truncollator completes, then contact Sandvine Customer Support or its authorized partner.

7. Verify that database disk usage is below 99 %. Run the Unix command:

   ```
   df -h
   ```

8. Start the Application Server. As an administrative user, issue start at the command prompt:

   ```
   start service application-server
   ```

9. To allow svcancel to function properly again, in CLI configuration mode set:

   ```
   SRP# set config service database auto-shutdown override enabled false
   SRP# commit
   ```

9.5.2 VRRP Tips

These tips address some common questions about use of Virtual Router Redundancy Protocol (VRRP) by the SPB:

VRRP Does Not Start on page 133

How do I Tell Which is the VRRP Master and Which are the Backup(s)? on page 133

VRRP Role Keeps Switching between Backup and Master on page 133

Stopping VRRP on page 133

9.5.2.1 VRRP Does Not Start

The status of the VRRP service can be determined using this command:

```
show system services
```

The display result is as follows:

```
Name                                AdminStatus OperStatus
----------------------------------- ----------- ----------
Virtual Router Redundancy Protocol  [up]        [online]
```

If the process is not running, verify that the VRRP configuration is correct. There should be a single VHID entry on each server and the interface selected should be available on the server.

For further troubleshooting information, check the log file */var/log/messages*.

Entries related to VRRP are indicated by a prefix (PID number is not the same):

```
freevrrpd[44222]:
```

9.5.2.2 How do I Tell Which is the VRRP Master and Which are the Backup(s)?

The log file */var/log/messages* identifies a VRRP master role versus a VRRP backup role for the server. The VRRP master server is indicated by a message in */var/log/messages* (PID number is not the same):

```
freevrrpd[44222]: server state vrid 1: master
```

A message in */var/log/messages* identifies the VRRP backup(s). (PID number is not the same):

```
freevrrpd[16337]: server state vrid 1: backup
```

Under normal situations, the VRRP master should be the server indicated in configuration with a priority of 255 in configuration. In the event of a network failure on the master, the master role switches to another server in the cluster. Once the master server comes back online, it again assumes the master role.

9.5.2.3 VRRP Role Keeps Switching between Backup and Master

The log file */var/log/messages* indicates when the role of master versus backup switches between servers. The switch should only occur in the event of a network failure of the master server or a link flap on the master server. A network condition may exist where traffic between the servers in the cluster is restricted or limited such that the VRRP process detects the delay and considers the proper action as switching roles. If this is the case, investigate the network path between servers to determine if traffic is limited or delayed.

9.5.2.4 Stopping VRRP

To power down the VRRP interface for operational or maintenance reasons, the recommended procedure is:

1. Stop the VRRP process by running the `stop service ip-redundancy` CLI command.
2. Power down the interface using the `ifconfig mgmt down` command.

When the maintenance is complete, perform these steps:

1. Restart VRRP, if required, by using the `start service ip-redundancy` CLI command.
2. Rejoin the node with the IP mapping cluster by running the CLI command:

   ```
   set service ip-redundancy join-cluster
   ```

Note:
Do not power down the interface administratively while VRRP is running. In case the interface powers down accidentally, power up the interface using the `ifconfig mgmt up` command and then restart VRRP using the `restart service ip-redundancy` CLI command.

9.5.3 Application Server Tips

These tips address common issues related to the application server:

9.5.3.1 After Automatic Failover the Application Server is not Bound to the New Master

If your system uses automatic failover, use:

```
set config service application-server bind-address 0.0.0.0
```

If it is not set at 0.0.0.0, change this variable and restart JBoss.

9.5.3.2 The Domain Manager does not Start

Run this CLI command to determine the current status of the message broker, including the domain manager:

```
show service message-broker status
```

The display results for the SPB server designated as the domain manager in configuration should be:

```
SonicVersion: MQ8.5

Name                                    Host        State  ConnectedSince
--------------------------------------- ----------- ------ ----------------------
DefaultCluster.DomainManager_Container   <hostname>  Online 2013-08-28 09:11:53 IST
DefaultCluster.AppBrkr7F000001_Container <hostname>  Online 2013-08-28 09:12:07 IST
```

This message indicates the message broker is not running:

```
ERROR: Message broker is not running.
```

Once initialized, run this CLI command to restart the message broker:

```
restart service message-broker
```

9.5.3.3 The Application Message Broker does not Start

In order to determine the current status of the of application message brokers, use the same steps as for the domain manager, described earlier. The only difference is that the status display indicates:

```
Name                                    Host        State  ConnectedSince
```

```
------------------------------------ ----------- ------ ----------------------
DefaultCluster.AppBrkr7F000001_Container <hostname>  Online 2013-08-28 09:12:07 IST
```

9.5.3.4 The Application Server does not Start

Run this CLI command to determine the current state of the application server:

```
show system services
```

The normal display is:

```
Name                      AdminStatus OperStatus
------------------------- ----------- ----------
JBoss Application Server  [up]        [online]
```

If the server is not started, run this command to start it:

```
start service application-server
```

Check the */var/log/jboss-server.log* log for error messages logged on startup.

9.5.3.5 The Application Server Cluster Status Command Shows Only 127.0.0.1

The cluster status CLI command (`show cluster config`) indicates which servers are considered to be in the cluster. In situations where a server cannot properly join a cluster, the cluster status command will return this:

```
ActiveNodes          : N/A
```

In most cases, the cause of the problem is related to the resolution of the server IP address. The IP is first resolved from `show configure service application-server bind-address`. If this setting is missing from the configuration, and the server is incorrectly specified by `set config cluster servers`, then the cluster will be setup with the localhost address as a single member. Use `show config cluster servers` to view the settings.

9.5.3.6 The Application Server Cluster Status does not Show all Members of the Cluster

The cluster status command indicates which servers are considered to be in the cluster.

It may be the case that only some members of the cluster are indicated. In most cases, the problem relates to the setting configured by `set config cluster servers <servers>` .

The missing server(s) may not be specified correctly. An invalid IP address or an IP address that cannot be reached will not be indicated as part of the cluster. Correct the `set config cluster servers <servers>` command and restart the application server.

If the cluster status command indicates only a single address, it is likely that the address indicated is the address specified by `set config service application-server bind-address <ip-address>`.

If this setting is incorrect for the server, then the cluster status will indicate the incorrect address and no other servers will be part of the cluster. Correct the bind address and restart the application server.

If the setting is correct for the server, then verify by issuing the `show config cluster servers` command. A missing setting will result in only the server being part of the cluster.

9.5.3.7 Message Broker Messages are not Processed by all SPB Servers in the Cluster

In a cluster of SPB servers, any one server can process a message sent to the message broker of any member of the cluster. If a server is not processing any messages, then it is likely that the message broker is not clustered with the other servers in the cluster. The situation can happen in cases where the message broker on the server designated as the domain manager restarts. In order to properly reform the message broker cluster, restart the message broker on the other servers in the cluster.

9.5.4 Statistics Logging Tips

These tips provide answers to questions about statistics logging:

There are Errors Related to Statistics Logging on Some of the SPB Servers in the Cluster on page 136

Summary Statistics Error Shows Quota Manager Statistics are not Written on page 136

9.5.4.1 There are Errors Related to Statistics Logging on Some of the SPB Servers in the Cluster

Once the cluster is setup and is operating correctly, the PTS elements send statistics and the messages are potentially processed by any SPB server in the cluster. It is important that there is only a single primary database designated for the cluster. If a server in the cluster has not configured the database IP address using the CLI command `config service database ip-address <ip-address>` or has an incorrect setting, then any statistics processed by the server goes to the incorrect database.

Messages in */var/log/jboss-server.log* may indicate this situation. The messages indicate that statistic processing encountered an error, and a subscriber was not found for a statistic.

9.5.4.2 Summary Statistics Error Shows Quota Manager Statistics are not Written

If the *jboss-server.log* shows this error, the statistics cluster name is not configured:

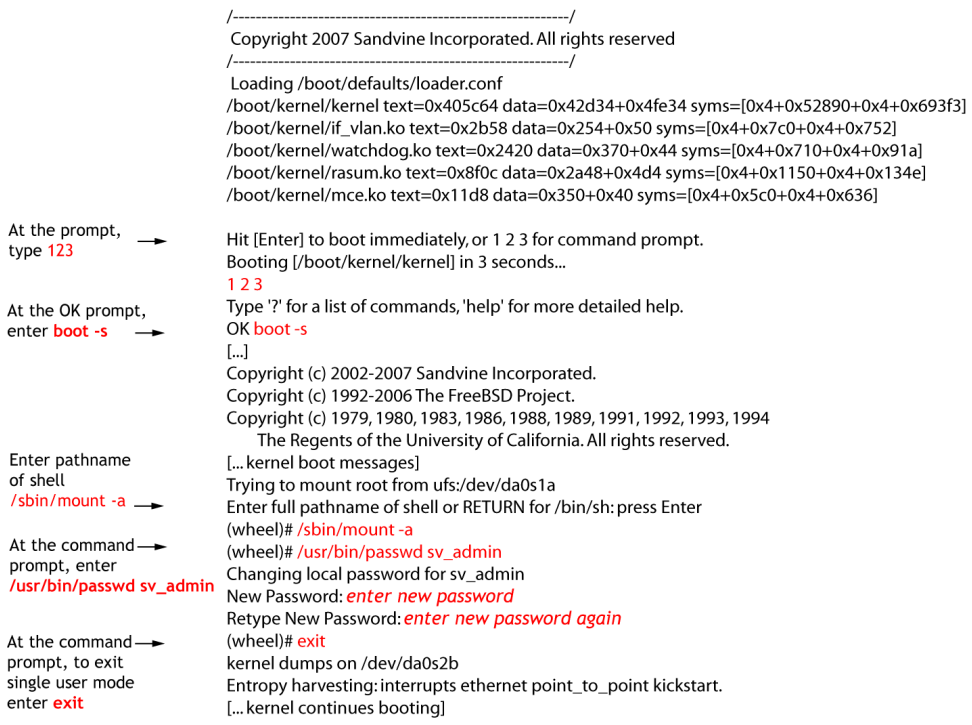
```
Oct  8 14:15:00 appsrv[47904]:
applog01;0000012228;0000007310:[QuartzInMemoryScheduler_Worker-1][com.sandvine.attrsummarizer.AttributeSummarizerWorker]
Attribute summary stats not written because cluster_stat_name=SANDVINE-1 (SANDVINE-1 and
DefaultCluster are disallowed names)
```

For configuration details, see *Statistics Cluster Name* on page 74.

9.5.5 Password Recovery

If the administrative (sv_admin user) password is misplaced, you can reset it. You will need to be physically connected to the element via the Management Console.

The prompts that appear on-screen and the steps to take at each stage to reset the administrative password are:



1. Connect to the element via the Management Console and then power cycle (reboot) the element.
2. At the `Hit [Enter] to boot immediately, or 1 2 3 for command prompt`, enter the numbers **1 2 3** to access a command prompt.
3. At the `OK` prompt, enter **boot -s**.
4. At the `Enter full path name of shell or RETURN for /bin/sh prompt`, press **Enter**.
5. At the prompt, enter **/sbin/mount -a**.
6. To change the sv_admin password, run `/usr/bin/passwd sv_admin`.
7. Follow the prompts to enter a new password.
8. To log out and continue the normal boot process, enter **exit**.
9. If desired, to verify the password, log on as sv_admin user and then log off.

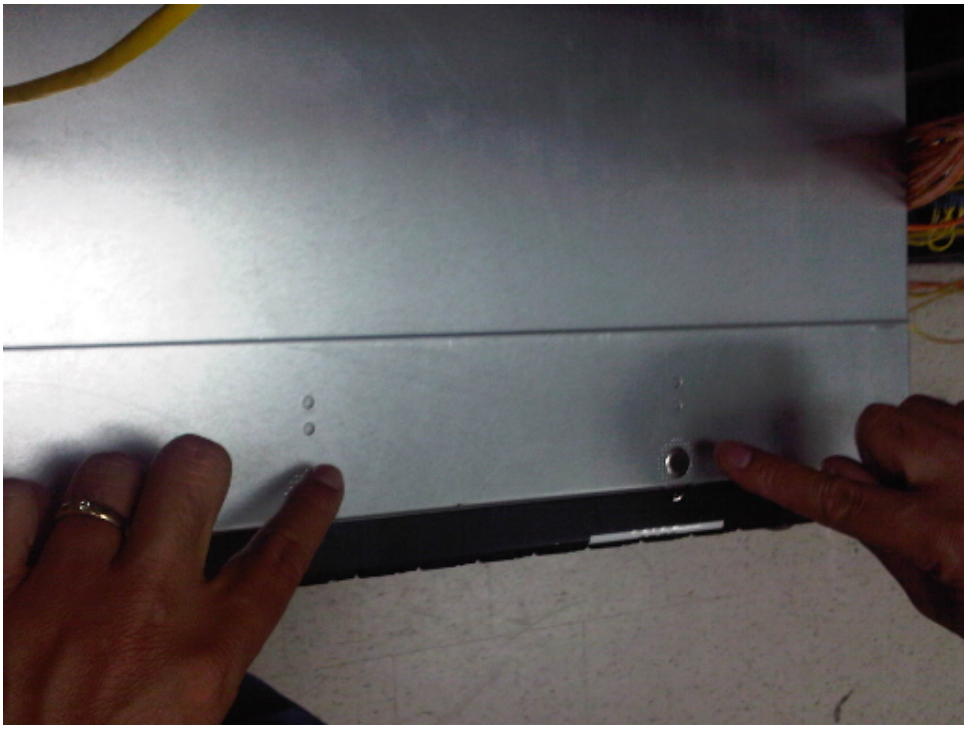
9.5.6 Internal Fan Failure

An internal fan failure is indicated by the alarm:

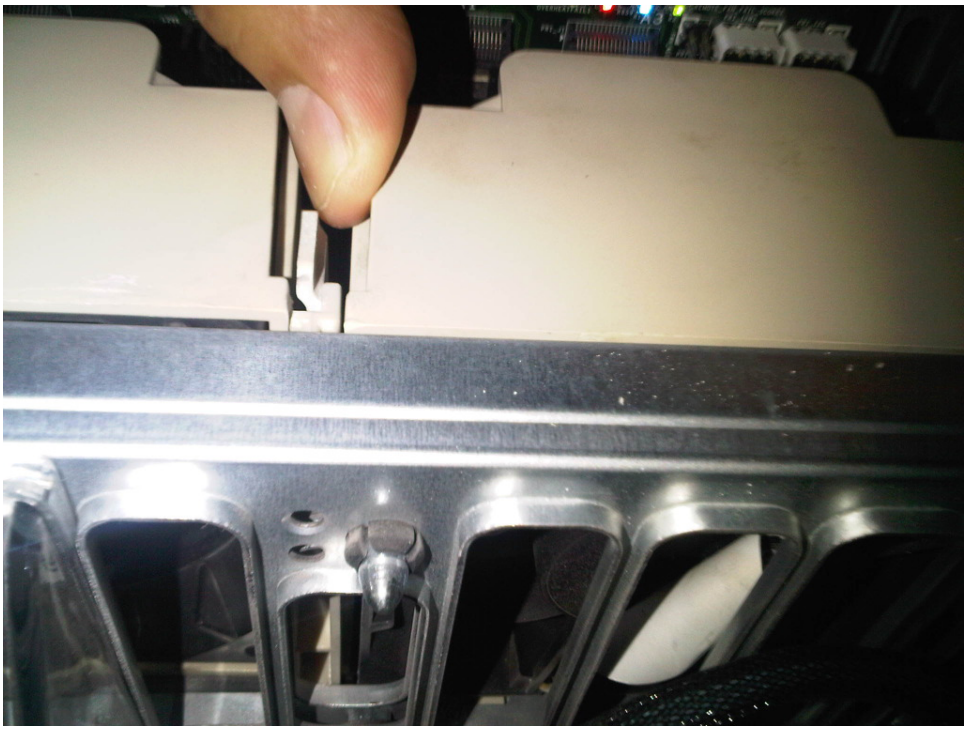
`"Fan failure: Internal fan 1, front nearest power button"`

On an SRP 3000-C platform, the process to verify if the fan has failed or the slot has gone defective is:

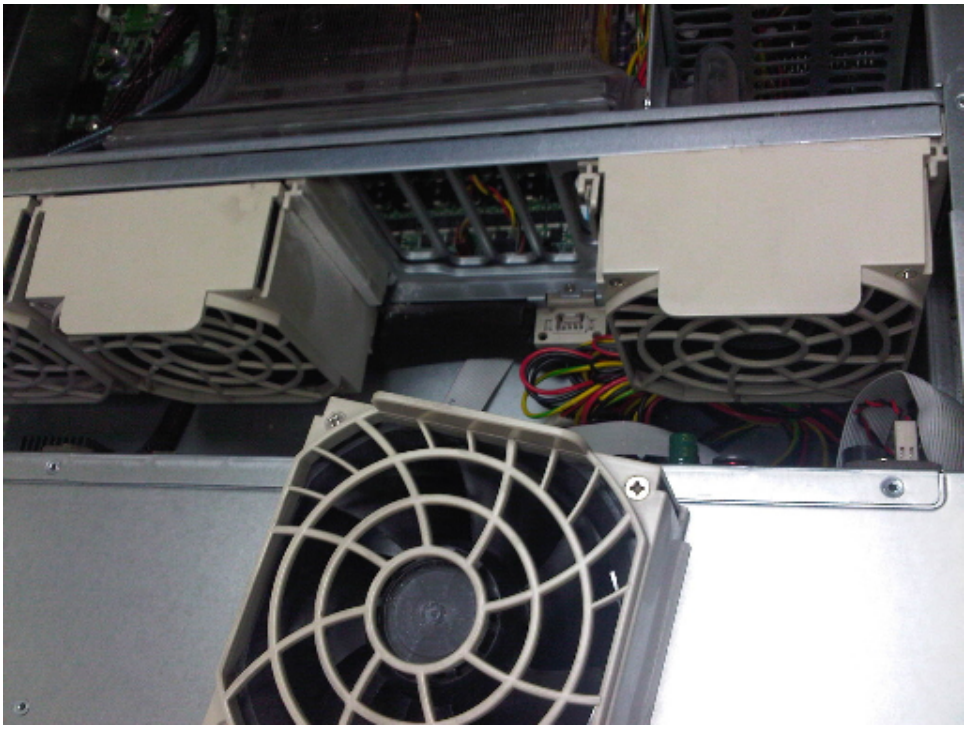
1. Open the chassis by pressing the two buttons on top and slide the cover towards the back.



2. On the fan with issue (Internal fan 1, front nearest power button), hold the lever on the side of the fan and pull the fan upwards from its slot.



3. Remove the other fan beside using the same procedure as in step 2. Place this fan to the slot where the fan with issue was sitting.



4. Place fan with issue into the other empty slot.

If the fan that was not spinning starts to spin in its new slot, then you can assume that the slot was defective. If the fan that was not spinning does not spin in the new slot, then you can assume that the fan was defective. Note the defect, either fan or slot. In either case, contact Sandvine Customer Support or its authorized partner for further instructions on the RMA process.

9.6 PTS Tips

These tips address the connection between the PTS and the SPB:

How do I Verify the PTS is Correctly Connected to the SPB Cluster? on page 139

The PTS is not Logging Statistics on page 140

9.6.1 How do I Verify the PTS is Correctly Connected to the SPB Cluster?

Run this CLI command on the PTS to determine the status of its connection to the SPB server:

```
show spb connections
```

The normal output using an example setup is:

```
PTS> show service spb connections
Id    Type                Failures OperStatus  AdminStatus ConfiguredURI
----- ------------------- -------- ----------- ----------- ---------------
11863 Statistics database 24       [connected] [up]        3.0.0.3,3.0.0.4

Id    ConnectedURI LastTimeConnected       APIVersion
----- ------------ ----------------------- ----------
11863 3.0.0.3      2011-12-06 14:43:42 EST [2]
```

The server IPs for all SPB servers in the cluster that contains the database for the PTS element appear in the list.

If OperStatus indicates `[connecting]`, then the connection to the SPB server(s) cannot be established. Verify the configuration for the SPB through the Quickstart, any changes will result in a reload of configuration and an attempt to re-connect.

If the message broker(s) on the SPB servers are not running, verify the message broker status using the information in *The Domain Manager does not Start* on page 134.

9.6.2 The PTS is not Logging Statistics

If the cluster name is set to the default SANDVINE-1, the PTS does not log statistics to the SPB. You must change the cluster name to enable statistics collection. See the *PTS Network Configuration Guide*.

A

SPB CLI Configuration Commands

A.1 SPB CLI Configuration Commands

A.1.1 Required CLI Configuration Commands

These CLI commands must be configured on each SPB server.

A.1.1.1 set config default-user enabled

Enables or disables the default SPB user.

```
set config default-user enabled <true|false>
```

In order for the Application Server to connect to the Message Server the default SPB user needs to be created.

A.1.1.2 set config cluster

Configure the cluster compatibility version in a PTS contributing to cluster.

Warning:
Commiting the `set config cluster compatibility version` command requires SFCD restart.

```
set config cluster compatibility version <1|2>
set config cluster name <name>
set config cluster log-default

set config cluster stat-name <stat-name>
set config cluster sub-name <sub-name>
```

Note:

- In case of a configured SPB cluster, make sure that you first run these commands on the domain manager node. Run this CLI command to find the node that is designated as the domain-manager:

  ```
  show config cluster domain-manager
  ```

- In case of a new SPB cluster configuration, first set the domain manager by running this CLI command and then run the other commands:

  ```
  set config cluster domain-manager <ip-address>
  ```

- When compatibility version 2 is set, you need to configure the internal-service IP.

Attribute	Description
compatibility version	Configures the PTS to use a different IP subnet for internal service (PTS to PTS) and external service (PTS to non-PTS) traffic.
log-default	Enable/disable the logging of statistics and heartbeats when the system is configured with the default cluster name.
name	Group PTS elements by name.
sub-name	Elements are considered local to one another if they are in the same sub-cluster.
stat-name	The name used to represent the cluster when writing stats.

Attribute	Description
domain-manager	IP of the domain manager message broker.
name	The cluster name of the SPB servers.
servers	Space separated list of server IP addresses in the cluster. Use this configuration on a database-only server.

A.1.1.3 set config service database

Configures SPB database settings.

```
set config service database auto-vacuum enabled <true|false>
set config service database auto-vacuum freeze-max-age <int>
set config service database enabled <true|false>
set config service database ssl enabled <true|false>
set config service database ip-address <ip-address>
set config service database port <int:0..>
set config service database name <name>
set config service database username <username>
set config service database password <password>
set config service database auto-shutdown override enabled <true|false>
```

Attributes	Description
auto-vacuum enabled	Vacuuming reclaims storage that dead tuples occupy. In general database operation, tuples (rows) that are deleted or obsoleted during an update are not physically removed from their table; they remain present until a VACUUM is done. Autovacuum vacuums periodically, especially on frequently updated tables. If this is set to **true**, the autovacuum process runs, otherwise autovacuum will not run.
auto-vacuum freeze-max-age	The freeze-max-age attribute is the maximum transaction ID (XID) age before a forced vacuum is done.
auto-shutdown override	Determines whether the database will automatically shut down at 99% disk usage.
enabled	When set to **true** the database service is enabled and runs. If set to **false** the database service is disabled. For example this command is set to **false** to configure an application-server-only network element, otherwise it is set to **true**.
ssl enabled	Determines whether the application server will only make SSL encrypted connections to the database. If set to true, you must configure the database to allow SSL connections.
ip-address	IP of the server hosting the database for the SPB. The default is 127.0.0.1.
name	Name of the database in which statistics and subscriber information are stored. The default is `sv_stat`.
username	User name for connections to the statistics database. The default is `svspb`.
password	Password for connections to the statistics database.
port	The port to connect to the database. The default is 5432.

A.1.1.4 set config service application-server bind-address

Configure the bind-address for the application server.

```
set config service application-server bind-address <ip-address>
```

where ip-address can be an IPv6 or an IPv4 address.

Committing changes to this command requires restarting the application server.

A.1.2 SPB Advanced Configuration Commands

These advanced SPB configuration commands should not be configured without consulting Sandvine Customer Support or its authorized partner.

A.1.2.1 set config service ip-user-map monitoring enabled

Enables monitoring of the IpUserMap process for overload conditions.

```
set config service ip-user-map monitoring enabled <true|false>
```

A.1.2.2 set config service ip-user-map monitoring degraded-state-processing

Configures degraded state processing when monitoring IP mapping.

```
set config service ip-user-map monitoring degraded-state-processing enabled <true|false>

set config service ip-user-map monitoring degraded-state-processing process-logins-as-logouts
 <true|false>

set config service ip-user-map monitoring degraded-state-processing set-login-attributes
<true|false>

set config service ip-user-map monitoring degraded-state-processing set-logout-attributes
<true|false>

set config service ip-user-map monitoring degraded-state-processing ip-assignment-history
<true|false>

set config service ip-user-map monitoring degraded-state-processing fatal-holdoff <int:0..>

set config service ip-user-map monitoring degraded-state-processing threshold queue-size rising
 <int:0..100>

set config service ip-user-map monitoring degraded-state-processing threshold queue-size falling
 <int:0..100>

set config service ip-user-map monitoring degraded-state-processing threshold lag rising
<int:0..>

set config service ip-user-map monitoring degraded-state-processing threshold lag falling
<int:0..>

set config service ip-user-map monitoring degraded-state-processing threshold lag fatal <int:0..>
```

Attribute	Description
enabled	Enable monitoring of the IPUserMap process for overload conditions.
fatal-holdoff	Hold off (pause) period after fatal state when IPUserMapper is paused momentarily. IPUserMap will not process any packets during this time. IP lookups are also disabled.
ip-assignment-history	Create IP assignment history in degraded state.
process-logins-as-logouts	Process logins as logouts in degraded state. If enabled, IPUserMap will use the login IP to logout an existing session, but will not login the new subscriber.
set-login-attributes	Set login attributes in degraded state.
set-logout-attributes	Set logout attributes in degraded state.
threshold queue-size rising	IPUserMap enters the degraded state when the current queue size is equal to or greater than this value. This value is expressed as a percentage of the maximum queue size. Default is 75.
threshold queue-size falling	IPUserMap enters the degraded state when the current queue size is equal to or greater than this value. This value is expressed as a percentage of the maximum queue size. Default is 65.

Attribute	Description
lag rising	IPUserMap enters the degraded state when the current processing lag time is less than this value. Default is 240.
lag falling	IPUserMap enters the degraded state when the current processing lag time, is less than this value. Default is 200.
lag fatal	IPUserMap enters the degraded state when the current processing lag time, is less than this value. Default is 300.

A.1.3 Database Monitoring

These CLI commands configure how the database is monitored.

A.1.3.1 set config service db-monitor

Configures automatic database failover.

```
set config service db-monitor enabled <true|false>
set config service db-monitor vrrp-vhid <int:1..2147483647>
set config service db-monitor port <int:1024..65535>
set config service db-monitor polling-interval <int:1..900>
set config service db-monitor timeout-interval <int:3..2700>
```

Attribute	Description
enabled	Enables or disables automatic database failover
polling-interval	Sets the frequency at which the database monitor polls the status of primary database
port	Sets the database port on which the database monitor connects to poll the status
timeout-interval	Sets the amount of time to wait before initiating a database failover after a failed poll attempt
vrrp-vhid	Sets the identified virtual host ID

A.1.4 Message Broker

You should only change these configuration CLI commands in non-standard or special case SPB deployments.

A.1.4.1 set config service message-broker

Configures how SPB communicates with other network elements, the connections allowed by the message broker, and the maximum message size.

```
set config service message-broker enabled <true|false>
set config service message-broker max-connections <int:300..>
set config service message-broker max-msg-size <int:0..>
```

You need to restart the message broker to commit these changes.

Attribute	Description
enabled	Determines whether the message broker will start on boot-up.
max-connections	Specifies the maximum number of active client connections allowed by the message broker.
max-msg-size	Specifies the maximum message size allowed by the message broker.

A.1.5 Application Server

You should only change these configuration variables in non-standard or special case deployments of SPB:

A.1.5.1 set config service application-server enabled

Enables or disables whether the application server will start on boot.

```
set config service application-server enabled <true|false>
```

Committing changes to this command requires restarting the application server.

A.1.5.2 set config service application-server bind-address

Configure the bind-address for the application server.

```
set config service application-server bind-address <ip-address>
```

where ip-address can be an IPv6 or an IPv4 address.

Committing changes to this command requires restarting the application server.

A.1.5.3 set config service application-server servlet

Configures the SPB application server servlet's settings.

```
set config service application-server servlet bind-address <ip-address>
set config service application-server servlet https enabled <true|false>
set config service application-server servlet https port <int:0..>
set config service application-server servlet https max-sessions <int:25..>

set config service application-server servlet http enabled <true|false>
set config service application-server servlet http port <int:0..>
set config service application-server servlet http max-sessions <int:25..>
```

Committing these command requires a restart.

Attribute	Description
bind-address	The bind-address for the servlet as an IPv6 or IPv4 address
https enabled	Enables or disables HTTPS
https port	Sets the port for HTTPS
https max-sessions	Sets the maximum value of the HTTPS thread/sessions. Default is 25.
http enabled	Enables or disables HTTP
http port	Sets the port for HTTP

Attribute	Description
http max-sessions	Sets the maximum value of the HTTP thread/sessions. Default is 25.

A.1.6 SPB Services

You should only change these configuration CLI commands in non-standard or special case deployments of SPB services.

A.1.6.1 set config service api web schema-validation enabled

Enables or disables web-services request schema validation.

```
set config service api web schema-validation enabled <true|false>
```

A.1.6.2 set config service api web stats-collection

Configures the web API statistics collection variables.

```
set config service api web stats-collection period <int:0..>
set config service api web stats-collection recovery-threshold <int:0..>
```

Attribute	Description
period	The amount of time that the periods may be skewed by when the PTS publishes
recovery-threshold	The amount of time, in seconds, to wait for statistics before considering them expired

A.1.6.3 set config service change-notification

Set whether to send change notification messages in mode pre-5.60 or 5.60 or mixed.

```
set config service change-notification ip-assignment enabled <true|false>
set config service change-notification mode <pre-5.60|5.60|mixed>
set config service change-notification session-attribute enabled <true|false>
set config service change-notification subscriber-attribute enabled <true|false>
```

Attribute	Description
ip-assignment enabled	Enables/disables IP assignment change notifications
mode	There is a change notification message format change between pre-5.60 releases and 5.60. Depending on the software versions of the PTS(s) the change notifications are going out to, set to one of: • 1, when all PTSs are pre-5.60 • 2, when all PTSs are 5.60 • or 1, 2, when the PTSs are mixed
session-attribute enabled	Enables/disables session attribute assignment change notifications
subscriber-attribute enabled	Enables/disables subscriber attribute assignment change notifications

A.1.6.4 set config service database

Configures SPB database settings.

```
set config service database auto-vacuum enabled <true|false>
set config service database auto-vacuum freeze-max-age <int>
set config service database enabled <true|false>
set config service database ssl enabled <true|false>
set config service database ip-address <ip-address>
set config service database port <int:0..>
set config service database name <name>
set config service database username <username>
set config service database password <password>
set config service database auto-shutdown override enabled <true|false>
```

Attributes	Description
auto-vacuum enabled	Vacuuming reclaims storage that dead tuples occupy. In general database operation, tuples (rows) that are deleted or obsoleted during an update are not physically removed from their table; they remain present until a VACUUM is done. Autovacuum vacuums periodically, especially on frequently updated tables. If this is set to **true**, the autovacuum process runs, otherwise autovacuum will not run.
auto-vacuum freeze-max-age	The freeze-max-age attribute is the maximum transaction ID (XID) age before a forced vacuum is done.
auto-shutdown override	Determines whether the database will automatically shut down at 99% disk usage.
enabled	When set to **true** the database service is enabled and runs. If set to **false** the database service is disabled. For example this command is set to **false** to configure an application-server-only network element, otherwise it is set to **true**.
ssl enabled	Determines whether the application server will only make SSL encrypted connections to the database. If set to true, you must configure the database to allow SSL connections.
ip-address	IP of the server hosting the database for the SPB. The default is 127.0.0.1.
name	Name of the database in which statistics and subscriber information are stored. The default is `sv_stat`.
username	User name for connections to the statistics database. The default is `svspb`.
password	Password for connections to the statistics database.
port	The port to connect to the database. The default is 5432.

A.1.6.5 set config security enabled

Configures whether calls to the Subscriber API will be authenticated.

```
set config security enabled <true|false>
```

A.1.6.6 set config service subscriber-management audit

Configures subscriber management auditing settings.

```
set config service subscriber-management audit transitions ip-assignment enabled <true|false>
set config service subscriber-management audit transitions subscriber-attribute enabled <true|false>
set config service subscriber-management audit transitions session-attribute enabled <true|false>
set config service subscriber-management audit records session-attributes enabled <true|false>
set config service subscriber-management audit records ip-assignment-history enabled <true|false>
```

Attributes	Description
transitions ip-assignment enabled	If enabled, change notifications and the IP history are created for all IP changes, including multiple transitions within a single batch of processing.
transitions subscriber-attribute enabled <boolean>	If enabled, change notifications and attribute audit records are created for all subscriber attribute changes, including multiple transitions with a single batch of processing.
session-attribute enabled	If enabled, session attribute audit records are logged to the database, available either through direct SQL or via Reporting Services. **Note:** Enabling this option decreases the maximum rate of dynamic IP mappings (including RADIUS and DHCP IP mapping) and requires careful consideration of data retention and disk-write performance. The retention period of the session_attr_audit table determines how long the session audit history is kept in the database. Decrease this period for high session rates.
ip-assignment-history enabled	If enabled, IP assignment history is logged to the database.

A.2 Warm Standby CLI Commands

A.2.1 CLI Commands for Primary Database

You can configure the SPB database server as the primary database server, in a warm standby system, through the use of these CLI commands.

Required command:

```
set config service warm-standby server <ip-address>
```

Recommended command:

```
set config service warm-standby archive email <email-address>
```

start service warm-standby primary

Run the `start service warm-standby primary` CLI command to start the warm-standby service on primary server. When the service is started for the first time, a is required to copy the public key to the standby server.

A.2.2 CLI Commands for Standby Database

You can start and configure the standby SPB database server, in a warm standby system, using these CLI commands.

The recommended command is:

```
set config service warm-standby restore email <email-address>
```

start service warm-standby standby

Run the `start service warm-standby standby` command to start the warm standby service on the standby server.

A.2.3 set config service warm-standby

Configures the warm standby feature.

```
set config service warm-standby server <ip-address>
set config service warm-standby archive email <email-address>
set config service warm-standby archive frequency <int:0..10080>
set config service warm-standby archive log <log>
set config service warm-standby archive threshold warning <int:0..90>
set config service warm-standby archive threshold stop <int:0..90>
set config service warm-standby restore email <email-address>
set config service warm-standby restore frequency <int:0..10080>
```

Attribute	Description
server	The IP address of the standby server.
archive email	The email address to which warning emails will be sent in the event that database log files cannot be successfully archived and disk usage exceeds the warning threshold.
archive frequency	The frequency with which warning emails are sent in the case that database archival continues to fail and disk usage continues to exceed the value set using `set config service warm-standby archive threshold` CLI configuration command. This value is expressed in minutes and the default is 5.
archive log	The directory on the standby server to which database log files are archived. This is specified as a subdirectory of the pgsql database user home directory, typically /usr/local/pgsql. **Note:** Set this variable on both the primary and standby servers, when a non-default directory is chosen as the archive location.
archive threshold warning	The transaction log disk capacity beyond which warning emails are sent if a log file cannot be archived. This value is expressed as a percentage and is typically slightly higher than the expected steady state usage of the transaction log disk. The default is 25.
archive threshold stop	Indicates the transaction log disk capacity beyond which database archival is disabled altogether. This measure is needed to prevent the primary database server from running out of disk space and enforcing a mandatory shutdown. This value is expressed as a percentage and should typically be near full disk capacity. The default is 90.
restore email	The email address to send warning emails to in the event that database log files are not successfully restored on the standby server.
restore frequency	Assuming database archival is functioning properly, the length of time that the database restore process waits for a database log file before sending a warning email. This is also the frequency with which subsequent warning emails are sent in the event that the database restore process continues to wait. This value is expressed in minutes and the default is 5.

A.3 Tuning CLI Commands

The SPB subscriber management configuration parameters related to sizing and tuning are:

A.3.1 set config service subscriber-management cache subscribers

Configures database sizing and tuning for subscriber data.

```
set config service subscriber-management cache subscribers max <int:0..>
set config service subscriber-management cache subscribers max-name-length <int:1..255>
set config service subscriber-management cache subscribers avg-name-length <int:1..255>
set config service subscriber-management cache subscribers ip-assignments max <int:0..>
set config service subscriber-management cache subscribers ip-assignments buffers max-subscribers
 <int:0..100>
set config service subscriber-management cache subscribers ip-assignments buffers
max-ip-assignments <int:0..100>
set config service subscriber-management cache subscribers ip-assignments buffers max-attributes
 <int:0..100>
```

Attribute	Description
max	The maximum number of subscriber records that can be in memory
max-name-length	The maximum length for a subscriber name
avg-name-length	The average length for a subscriber name
ip-assignments max	The maximum number of IP assignment record that can be in memory
ip-assignments buffers max-subscribers	The percentage of buffer space to allocate to subscribers.
ip-assignments buffers max-ip-assignments	The percentage of buffer space to allocate to IP assignments
ip-assignments buffers max-attributes	The percentage of buffer space to allocate to subscriber attributes.

A.3.2 set config service subscriber-management cache attributes

Configures database sizing and tuning for subscriber attribute data.

```
set config service subscriber-management cache attributes max <int:0..>
set config service subscriber-management cache attributes max-length <int:0..>
set config service subscriber-management cache attributes major-memory-blocks <int:0..>
set config service subscriber-management cache attributes minor-length <int:0..>
set config service subscriber-management cache attributes major-length <int:0..>
```

Attribute	Description
max	Maximum total number of attributes that can be stored in memory.
max-length	Maximum attribute value size in bytes that the system will accept.
major-memory-blocks	The number of major memory blocks (of size major-length) available. Major blocks are only used when an attribute's value exceeds minor-length.
minor-length	An attribute value with length in bytes <= to this value will be stored in a single minor attribute memory block. Default is 20.

Attribute	Description
major-length	An attribute value with length in bytes that is greater than minor-length and less than or equal to max-length is stored in one or more chained major blocks of length equal to this value. For example, if major-length=512, and the length of an attribute value is 600 bytes, it will be stored in two 512 byte blocks, “wasting” 424 bytes in one of the major blocks. Default is 128.

A.3.3 set config service attribute-archiver

The subscriber attribute archiver takes a snapshot of the in-memory attributes and persists them to disk so that they can be used in Network Demographics reports and API requests of subscriber statistics by attribute. The archiver archives each subscriber attribute where the attribute is marked as reportable. By default, all attributes are reportable. The archived attributes are then available for queries that join against the subscriber statistics.

A.4 SPB Hierarchy

The SPB hierarchy is configured with this CLI command:

A.4.1 add config data-home

Adds a row to the table of SPB hierarchy settings.

```
add config data-home <int:1..> name <name> display-name <display-name> url <url>
add config data-home <int:1..> name <name> display-name <display-name> url <url> parent <parent>
```

Committing these commands requires a restart.

Attribute	Description
data-home	A unique ID representing a datahome in the hierarchy.
name	The name of the datahome. This is the same as the SPB cluster name.
display-name	The display name of the datahome.
url	The URL that the message broker uses to send messages between sites. Use this format: `ssl://<hostname>:2507` Where <hostname> is the hostname of the datahome or IP address.
parent	The name of the datahome's parent in the hierarchy (optional).

A.5 Subscriber IP Mapping

These CLI commands configure features of subscriber-IP mapping, with specific commands for DHCP or RADIUS implementations described in these sections.

A.5.1 General Subscriber IP Mapping CLI Commands

A.5.1.1 set config service ip-user-map enabled

Enables IP mapping.

```
set config service ip-user-map enabled <true|false>
```

A.5.2 set config service ip-user-map realm

Configures the subscriber realm to populate subscribers into.

```
set config service ip-user-map realm <realm>
```

A.5.3 add/delete config service ip-user-map forwarding-address

Adds or deletes the IP and port for forwarding addresses for login or logout packets.

A.5.3.1 add config service ip-user-map forwarding-address

Configures forwarding login and logout packets to an IP and port.

```
add config service ip-user-map forwarding-address login <string>
add config service ip-user-map forwarding-address logout <string>
```

Attribute	Description
login	The IP and port to forward login packets to (in quotes).
logout	The IP and port to forward logout packets to (in quotes).

Example:
```
SRP# add config service ip-user-map forwarding-address login "10.10.10.10 1111"
```

A.5.3.2 delete config service ip-user-map forwarding-address

Deletes the configuration for the specified row, where row is the IP address as a string.

```
delete config service ip-user-map forwarding-address login <row>
delete config service ip-user-map forwarding-address logout <row>
```

A.5.4 set config service ip-user-map <service> enabled

Enables or disables the specified service.

```
set config service ip-user-map dhcp enabled <true|false>
```

```
set config service ip-user-map radius enabled <true|false>
```

A.5.5 set config service ip-user-map <service> parser instances

Configures the number of internal parser instances allocated to parsing DHCP or RADIUS packets.

```
set config service ip-user-map dhcp parser instances <int:1..10>
```

```
set config service ip-user-map radius parser instances <int:1..10>
```

A.5.6 set config service ip-user-map <service> capture-mode

Set the format in which packets are forwarded to the SPB. This command is only relevant for deployments using PTS sniffing.

```
set config service ip-user-map dhcp capture-mode
<normal-udp|encapsulated-udp|layer-2-rewrite|mirror>
```

```
set config service ip-user-map radius capture-mode
<normal-udp|encapsulated-udp|layer-2-rewrite|mirror>
```

Parameter	Description
normal-udp	The PTS will overwrite the destination address of the DHCP ACK packets or the RADIUS UDP packets and forward them directly to the SPB.
encapsulated-udp	The PTS will encapsulate the entire packet off the wire (including all headers) and send it to the SPB within a UDP packet. This mode enables the SPB to track RADIUS authentication sessions and use RADIUS authentication packets to set subscriber attributes.
layer-2-rewrite	The SPB will accept packets that have been forwarded from another device by rewriting the MAC address.
mirror	The SPB will accept packets that have been forwarded out a mirror port or SPAN port of another device.

A.5.7 DHCP Configuration CLI Commands

These CLI commands need to be set to enable and configure DHCP sniffing for subscriber IP mapping.

A.5.7.1 set config service ip-user-map dhcp boot-file source

Sets the source of the subscriber attribute.

```
set config service ip-user-map dhcp boot-file source
<none|filename-only|filename-first|option-67-only|option-67-first>
```

Parameter	Description
none	Turn off this feature.
filename-only	Use only the static BOOTP 'bootfile name' field.
filename-first	Try using the static BOOTP 'bootfile name' field first. If it is empty (after regex/formatting, if used), try using the DHCP option 67 field.
option-67-only	Use only the DHCP option 67 field.
option-67-first	Try using the DHCP option 67 field first. If it is empty (after regex/formatting, if used) or does not exist, try using the static BOOTP 'bootfile name' field. Note that the 'bootfile name' field will not be read if it is being used for option overloading (that is, if option 52 exists in the packet and is 1 or

Parameter	Description
	3). The value may be compared against a regex and formatted, and if the value does not match the regex, or if it does but the formatted value is blank, then the attribute will not be written.

A.5.7.2 set config service ip-user-map dhcp boot-file attribute

Configures subscriber attribute mapping from the DHCP bootfile.

```
set config service ip-user-map dhcp boot-file attribute name <name>
set config service ip-user-map dhcp boot-file attribute regex <regex>
set config service ip-user-map dhcp boot-file attribute regex-replace <regex-replace>
set config service ip-user-map dhcp boot-file attribute expiry <time>
```

Attribute	Description
name	The name of the attribute.
regex	Optional regular expression that value must match to be mapped.
regex-replace	Optional Boost-style format string to use for values to map.
expiry	The expiry is expressed as an offset from mapping time and may be defined as: • Infinity • A combination of n days, n hours, n minutes, n seconds The default is infinity.

A.5.7.3 add config service ip-user-map dhcp

Adds configuration for DHCP IP mapping.

```
add config service ip-user-map dhcp interface <string>
add config service ip-user-map dhcp interface <string> capture-mode
<normal-udp|encapsulated-udp|layer-2-rewrite|mirror>
add config service ip-user-map dhcp login-attribute <string> value <value>
add config service ip-user-map dhcp login-attribute <string> value <value> expiry <expiry>
add config service ip-user-map dhcp attribute-mapping <string>
add config service ip-user-map dhcp attribute-mapping <string> type <subscriber|session>
add config service ip-user-map dhcp attribute-mapping <string> type <subscriber|session> regex
 <regex>
add config service ip-user-map dhcp attribute-mapping <string> type <subscriber|session> regex
 <regex> regex-replace <regex-replace>
```

Attribute	Description
interface	Interfaces on which to listen for DHCP packets.
capture-mode	The format in which packets are forwarded to the SPB.
attribute-mapping	DHCP header fields to map to subscriber attributes.
type	Subscriber or Session. Sets the mapped attributes defined by attribute-mapping as a Session Attribute or a Subscriber Attribute. A Session Attribute applies only to the subscriber session which this DHCP packet pertains to, and expires at the end of the session, whereas Subscriber Attributes apply to a subscriber (and all of his/her sessions), and expires at attribute mapping's expiry time.
regex	Optional regular expression that value must match to be mapped.
regex-replace	Optional Boost-style format string to use for values to map.
login-attribute	Subscriber attributes that are set when a subscriber logs in.

Attribute	Description
expiry	A list of offsets from the current time when the attribute assignment should expire. For example: `add config service ip-user-map dhcp login-attribute "tier" value "Gold" expiry "21 days 7 hours"` You can combine: : • *n* days • *n* hours • *n* minutes • *n* seconds

Capture Mode Parameter	Description
normal-udp	The PTS will overwrite the destination address of the DHCP ACK packets or the RADIUS UDP packets and forward them directly to the SPB.
encapsulated-udp	The PTS will encapsulate the entire packet off the wire (including all headers) and send it to the SPB within a UDP packet. This mode enables the SPB to track RADIUS authentication sessions and use RADIUS authentication packets to set subscriber attributes.
layer-2-rewrite	The SPB will rewrite the MAC address to accept packets forwarded from another device.
mirror	The SPB will accept packets forwarded out a mirror port or SPAN port of another device.

A.5.7.4 set config service ip-user-map dhcp single-ip

Enables or disables subscriber single IP mode. Single IP mode ensures that the IP assignment unassigns all other IP assignments the subscriber may have.

```
set config service ip-user-map dhcp single-ip <true|false>
```

A.5.7.5 set config service ip-user-map dhcp interface

Alters the configuration of the interfaces on which to listen for DHCP packets.

```
set config service ip-user-map dhcp interface <row> capture-mode
<normal-udp|encapsulated-udp|layer-2-rewrite|mirror>
```

Attributes	Description
interface	The IP address of the interface serves as the row key into the configuration table.
capture-mode	The format in which packets are forwarded to the SPB.

Capture Mode Parameter	Description
normal-udp	The PTS will overwrite the destination address of the DHCP ACK packets or the RADIUS UDP packets and forward them directly to the SPB.
encapsulated-udp	The PTS will encapsulate the entire packet off the wire (including all headers) and send it to the SPB within a UDP packet.
layer-2-rewrite	The SPB will accept packets that have been forwarded from another device by rewriting the MAC address.
mirror	The SPB will accept packets that have been forwarded out a mirror port or SPAN port of another device.

A.5.7.6 set config service ip-user-map attribute-mapping delimiter

Configures the delimiter to be used in when mapping attributes.

Valid values are any single printable character. An empty value is also permitted. The default is “, “ (comma).

A.5.7.7 set config service ip-user-map dhcp subscriber-identifier

Configures how subscriber IDs are handled.

```
set config service ip-user-map dhcp subscriber-identifier mode <cpe-mac|option-82>
set config service ip-user-map dhcp subscriber-identifier ascii <true|false>
set config service ip-user-map dhcp subscriber-identifier case <unchanged|to-upper|to-lower>
set config service ip-user-map dhcp subscriber-identifier sub-option
<agent-circuit-id|agent-remote-id>
```

Attribute	Description
mode	Determines where to find the unique identifier for subscribers in DHCP packets.
ascii	Determines whether to handle the subscriber UID data, as determined by mode, as an opaque binary string and represent it as hex, or to assume it is ASCII-encoded and represent it as a normal hex string. The default is hex, since the hex representation is appropriate for MAC addresses, which is most often the case.
case	Indicates if the DHCP username should be converted.
sub-option	The DHCP Option 82 sub option used to represent the subscriber ID.

Parameter	Description
cpe-mac	Use the CPE MAC address of a subscriber.
option-82	The DHCP Option 82 suboption used to represent the subscriber ID.
unchanged	If ASCII, leave the username in its natural case, if MAC address, use uppercase.
to-upper	Convert to uppercase, using the default locale.
to-lower	Convert to lowercase, using the default locale.
agent-circuit-id	For DHCP Option 82, the Circuit ID sub-option carries information specific to which circuit the request came in on, depending on the relay agent.
agent-remote-id	For DHCP Option 82, the Remote ID sub-option carries information relating to the remote host end of the circuit, usually containing information that identifies the relay agent.

A.5.8 RADIUS Configuration CLI Commands

A.5.8.1 set config service ip-user-map radius subnet-mask

Assign a block of IPs on accounting start requests.

```
set config service ip-user-map radius subnet-mask enabled <true|false>
set config service ip-user-map radius subnet-mask limit <int:1..30>
```

Attribute	Description
enabled	If subnet mask is enabled (true), then on accounting start requests a group of IP addresses are assigned to a particular subscriber and on accounting stop requests they are unassigned. If false, the IP Mapper assigns and unassigns a single IP address to the subscriber.
limit	Limits the number of IP addresses that can be assigned to a particular subscriber. For example, if the subnet bit mask limit is 8, then 256 IP addresses can be assigned to the subscriber. Default is 16.

A.5.8.2 add config service ip-user-map radius

Adds configuration for RAIDUS IP mapping.

```
add config service ip-user-map radius accounting sub-name attribute <string>
add config service ip-user-map radius accounting sub-name attribute <string> regex <regex>
add config service ip-user-map radius accounting sub-name attribute <string> regex <regex>
regex-replace <regex-replace>
add config service ip-user-map radius attribute-definition <string> type
<date|integer|ip-address|octets|string|text>
add config service ip-user-map radius attribute-filter <string> regex <regex>
add config service ip-user-map radius attribute-filter-required <true|false>
add config service ip-user-map radius attribute-mapping <string>
add config service ip-user-map radius attribute-mapping <string> type <subscriber|session>
add config service ip-user-map radius attribute-mapping <string> type <subscriber|session>
regex <regex>
add config service ip-user-map radius attribute-mapping <string> type <subscriber|session>
regex <regex> regex-replace <regex-replace>
add config service ip-user-map radius interface <string>
add config service ip-user-map radius interface <string> shared-secret <shared-secret>
add config service ip-user-map radius interface <string> shared-secret <shared-secret>
capture-mode <normal-udp|encapsulated-udp|layer-2-rewrite|mirror>
add config service ip-user-map radius interface <string> shared-secret <shared-secret>
capture-mode <normal-udp|encapsulated-udp|layer-2-rewrite|mirror> reply <true|false>
add config service ip-user-map radius ip-attribute <string>
add config service ip-user-map radius login-attribute <string> value <value>
add config service ip-user-map radius login-attribute <string> value <value> expiry <expiry>
add config service ip-user-map radius logout-attribute <string> value <value>
add config service ip-user-map radius logout-attribute <string> value <value> expiry <expiry>
add config service ip-user-map radius packet-merging attribute <string> value <int>
add config service ip-user-map radius packet-merging dominant-packet
add config service ip-user-map radius packet-merging merge-key <string>
add config service ip-user-map radius session-tracking session-id-attribute <string>
```

Committing these commands requires a restart.

Attribute	Description
interface	Interfaces on which to listen for RADIUS packets.
shared-secret	The RADIUS shared secret password. A password is required for each interface. **Note:** This variable is only required for deployments using NAS replication.
capture-mode	The format in which packets are forwarded to the SPB.
reply	Specifies if RADIUS accounting request packets require a response packet. Enabling accounting replies is not compatible with encapsulated capture mode.
session-tracking session-id-attribute	Specifies the RADIUS attributes to be used together to form the unique session identifier for STATEFUL tracking mode. You can choose these attributes for the unique per subscriber login session.

Attribute	Description

	A standard RADIUS attribute example is to configure NAS-IP-Address together with Acct-Session-Id as the session ID, as:
	`add config service ip-user-map radius session-tracking session-id-attribute 44`
	A vendor-specific attribute example is to configure 3GPP2-Correlation-Id as the session ID:
	`add config service ip-user-map radius session-tracking session-id-attribute "VSA 5535 44"`

packet-merging attribute	The list of RADIUS attributes that defines which RADIUS packets to merge.
packet-merging dominant-packet	The RADIUS attribute which takes precedence in the case of a merge conflict.
packet-merging merge-key	The RADIUS attributes which define the key used to match up RADIUS packets to merge. For example, to use the User-Name (1) to match up RADIUS packets for merging: `add config service ip-user-map radius packet-merging merge-key 1`
attribute-definition	Add new custom RADIUS attributes, or override the data type of existing RADIUS attributes.
attribute-filter	RADIUS attribute used to filter which RADIUS attributes are processed.
attribute-filter-required	Indicates if an attribute filter is required.
attribute-mapping	RADIUS attributes to map to subscriber attributes.
type	Subscriber or Session. Sets the mapped attributes defined by attribute-mapping as a Session Attribute or a Subscriber Attribute. A Session Attribute applies only to the subscriber session which this DHCP packet pertains to, and expires at the end of the session, whereas Subscriber Attributes apply to a subscriber (and all of his/her sessions), and expires at attribute mapping's expiry time.
type	The data type; one of string, text, ip-address, integer, date or octets.
regex	Optional regular expression that value must match to be mapped.
regex-replace	Optional Boost-style format string to use for values to map.
login-attribute value	Subscriber attributes that are set when a subscriber logs in.
login-attribute	Subscriber attributes that are set when a subscriber logs out.
logout-attribute <string> value <value>	A list of values to set the attribute to when the subscriber logs out.
logout-attribute <string> value <value> expiry <expiry>	A list of values to set the attribute to when the subscriber logs out and their expiry time as an offset from the current time.
accounting sub-name attribute	RADIUS attribute, for example "4" or "VSA 5535 44".
ip-attribute	The RADIUS attribute to use as the subscriber IP address. For example, "4" or "VSA 5535 44" or "VSA 5535 44 TLV 4".

Capture Mode Parameter	Description
normal-udp	The PTS will overwrite the destination address of the DHCP ACK packets or the RADIUS UDP packets and forward them directly to the SPB.

Capture Mode Parameter	Description
encapsulated-udp	The PTS will encapsulate the entire packet off the wire (including all headers) and send it to the SPB within a UDP packet. This mode enables the SPB to track RADIUS authentication sessions and use RADIUS authentication packets to set subscriber attributes.
layer-2-rewrite	The SPB will accept packets that have been forwarded from another device by rewriting the MAC address.
mirror	The SPB will accept packets that have been forwarded out a mirror port or SPAN port of another device.

A.5.8.3 set config service ip-user-map radius interface

Configures the interfaces on which to listen for RADIUS packets.

```
set config service ip-user-map radius interface <row> shared-secret <shared-secret>
set config service ip-user-map radius interface <row> capture-mode
<normal-udp|encapsulated-udp|layer-2-rewrite|mirror>
set config service ip-user-map radius interface <row> reply <true|false>
```

Committing these command requires a restart.

Attributes	Description
capture-mode	The format in which packets are forwarded to the SPB.
shared-secret	The RADIUS shared secret password. A password is required for each interface.
reply	Specifies if RADIUS accounting request packets require a response packet. Enabling accounting replies is not compatible with encapsulated capture mode.

Capture Mode Parameter	Description
normal-udp	The PTS will overwrite the destination address of the RADIUS UDP packets and forward them directly to the SPB.
encapsulated-udp	The PTS will encapsulate the entire packet off the wire (including all headers) and send it to the SPB within a UDP packet. This mode enables the SPB to track RADIUS authentication sessions and use RADIUS authentication packets to set subscriber attributes.
layer-2-rewrite	The SPB rewrits the MAC address in order to accept packets forwarded from another device.
mirror	The SPB will accept packets forwarded out a mirror port or SPAN port of another device.

A.5.8.4 set config service ip-user-map radius accounting

Configures how the SPB handles RADIUS accounting.

```
set config service ip-user-map radius accounting reply <true|false>
set config service ip-user-map radius accounting sub-name delimiter <delimiter>
set config service ip-user-map radius accounting reply-before-commit <true|false>
```

Attribute	Description
reply	Specifies if RADIUS accounting request packets require a response packet. Enabling accounting replies is not compatible with encapsulated capture mode. Default is false.

Attribute	Description

sub-name delimiter	Configures the delimiter between multiple RADIUS attributes when building the sub-name from multiple attributes. For example:
	`set config service ip-user-map radius accounting sub-name delimiter XYZ`
	`set config service ip-user-map radius accounting sub-name attribute 1 regex 30`
	`set config service ip-user-map radius accounting sub-name attribute 2 regex 31`
	would build a subscriber name like: "`30XYZ31` Any ASCII variable, including an empty string is valid. The default is ". "

reply-before-commit	If configured to send accounting replies, this variable configures whether to send accounting replies immediately, or after all relevant RADIUS information has been committed. If this variable is set to true, replies will be immediate, however between the accounting reply and persisting the RADIUS information there is a window during which an SPB failure will cause a loss of information. If set to false, replies will not be sent until information is persisted. There will, however be a delay before reply, and replies will come in a burst since RADIUS information is persisted in batches. Default is false.

A.5.8.5 set config service ip-user-map radius session-tracking

Configures how session tracking is handled.

```
set config service ip-user-map radius session-tracking session-continue enabled <true|false>
set config service ip-user-map radius session-tracking event-timestamp enabled <true|false>
set config service ip-user-map radius session-tracking mode <normal|stateful|ignore-stops>
```

Attribute	Description
session-continue enable	Enable monitoring of the 3GPP2-Session-Continue attribute. If set to true, accounting stop packets that have the 3GPP2-Session-Continue attribute set to 1 will not cause the subscriber's IP address to be unassigned. The default value is false.
event-timestamp enabled	Set to true to use the Event-Timestamp RADIUS attribute for the event time of IP and attribute mappings, when present.
mode	Controls how RADIUS accounting START and STOP messages are handled. The options are: • normal: a START message logs the subscriber in (or keeps them logged in and updates their IP/attributes information) and a STOP logs them out. • stateful: a START is treated the same way as in normal mode, and a STOP only logs a subscriber out if it is from the same NAS and part of the same session as the last START message that came in for that subscriber; otherwise, it is ignored (that is, state is kept on the NAS-IP-Address and Acct-Session-Id attributes of each subscriber). • ignore-stops: a START is treated the same way as in NORMAL mode, and STOP messages are completely ignored.

A.5.8.6 set config service ip-user-map radius packet-merging

Configures RADIUS packet-merging settings.

```
set config service ip-user-map radius packet-merging enabled <true|false>
set config service ip-user-map radius packet-merging merge-key <string>
```

```
set config service ip-user-map radius packet-merging timeout <int:1..1000>
```

Attribute	Description
enabled	Enables the RADIUS packet merging feature. This allows the attributes from two packets to be merged prior to persisting information.
timeout	How long to wait, in seconds, before discarding a packet that should be merged but has no matching pair. This can be increased significantly provided there is available memory. The 1000 second maximum is safe on a 32GB RAM SRP.
merge-key	RADIUS attributes that define the key used to match packets.

A.5.8.7 set config service ip-user-map radius packet-merging attribute

Configures RADIUS attributes and values that define which RADIUS packets must be merged.

```
set config service ip-user-map radius packet-merging attribute <row> value <int>
```

Parameter	Description
attribute	The RADIUS attribute that defines which RADIUS packets must be merged
value	The value for the RADIUS attribute

A.5.8.8 add config service ip-user-map forwarding-address

Configures forwarding login and logout packets to an IP and port.

```
add config service ip-user-map forwarding-address login <string>
add config service ip-user-map forwarding-address logout <string>
```

Attribute	Description
login	The IP and port to forward login packets to (in quotes).
logout	The IP and port to forward logout packets to (in quotes).

Example:
```
SRP# add config service ip-user-map forwarding-address login "10.10.10.10 1111"
```

A.5.8.9 set config service ip-user-map realm

Configures the subscriber realm to populate subscribers into.

```
set config service ip-user-map realm <realm>
```

A.5.8.10 set config service ip-user-map radius single-ip

Enables or disables subscriber single IP mode.

```
set config service ip-user-map radius single-ip <false|true>
```

Enables subscriber single IP mode, ensuring that the IP assignment unassigns all other IP assignments the subscriber may have. True enables single IP mode and false allows multiple IP assignments to subscribers.

A.5.8.11 set config service ip-user-map radius subscriber

Configures how subscribers are handled.

```
set config service ip-user-map radius subscriber create-on-auth-request <true|false>
set config service ip-user-map radius subscriber id-case-conversion <to-lower|to-upper|unchanged>
```

Attribute	Description
create-on-auth-request	Access-Request creates the subscribers in the system for the purpose of attribute mapping.
id-case-conversion	Determines if the case of the unique string identifying the subscriber is all uppercase, lowercase or should be unchanged. In the case of a MAC address, the unchanged setting results in upper case. The default is unchanged.

A.5.8.12 set config service ip-user-map radius attribute-mapping

Configures mapping RADIUS attributes to subscriber attributes.

```
set config service ip-user-map radius attribute-mapping <row> type <subscriber|session>
set config service ip-user-map radius attribute-mapping <row> regex <regex>
set config service ip-user-map radius attribute-mapping <row> regex-replace <regex-replace>
```

Attribute	Description
type	Subscriber or Session. Sets the mapped attributes defined by attribute-mapping as a Session Attribute or a Subscriber Attribute. A Session Attribute applies only to the subscriber session which this DHCP packet pertains to, and expires at the end of the session, whereas Subscriber Attributes apply to a subscriber (and all of his/her sessions), and expires at attribute mapping's expiry time.
regex	Optional regular expression that value must match for mapping to occur.
regex-replace	Optional Boost-style format string to use for values to map.

Parameter	Description
row	The RADIUS header field set using `add config service ip-user-map radius attribute-mapping`.
subscriber	Applies to a subscriber (and all of his/her sessions), and expires at attribute mapping's expiry time.
session	Applies only to the subscriber session which this DHCP packet pertains to, and expires at the end of the session.

A.5.8.13 Regular Expressions and Replacement String Syntax

The java.util.regex library is used to process regular expressions and replacement strings.

These rules apply:

- Regular expressions are anchored. The entire string and regular expression are considered a match when they are an exact match. For example “.” only matches strings that consist of a single character. Note that the “^” and “$” characters are not required to match the beginning and end positions; they are implied.
- In regular expressions and in replacement strings, the “$” character does not need to be escaped using a preceding backslash (\). For example, you can enter "$1" to specify a replacement string that selects the first matching group.
- The supported Java replacement string constructs are:

- “$0” represents the whole input string that matched the regular expression.
- “$n” for n >= 1 represents the nth matching group in the regular expression.
- “?ntrue_expression:false_expression” means: if the nth group matched, substitute true_expression, otherwise substitute false_expression. A typical use of this syntax would be “?1True:False”, with a regular expression of “(abc.*)”, in which case the replacement string would resolve to “True” if the input string started with “abc”, and “False” otherwise. This construct may be nested; for example, “?1Bronze:?2Silver:?3Gold”.

Example:
Regular Expression Example

To only add subscribers with a name that starts with “8” followed by at least one character followed by an “@”.

```
SRP# add config service ip-user-map radius accounting sub-name attribute <attributeValue>
 regex "8.+@"
```

To map the NAS-PORT(5) to a subscriber attribute "subAttr" only if it is exactly four digits long and ends with “1”.

```
SRP# add config service ip-user-map radius attribute-mapping "5 subAttr" type subscriber
regex "\\d\\d\\d1" regex-replace "port-$0"
```

For the format of regular expressions and replacement strings see
http://java.sun.com/j2se/1.5.0/docs/api/java/util/regex/package-summary.html

Example:
Substitution String Example

To only add subscribers with a name that starts with 8, followed by at least nine characters, then the '@' sign, and to format the added value to “SUB:<first 10 characters of User-Name>”.

```
SRP# add config service ip-user-map radius attribute-mapping "5 subAttr" type subscriber
regex "\\d\\d\\d1" regex-replace "port-$0"
```

To map the NAS-PORT(5) to a subscriber attribute "subAttr" only if it is exactly four digits long and ends with 1, and pre-pend the added value with “port-”:

```
SRP# add config service ip-user-map radius attribute-mapping "5 subAttr" type subscriber
regex "\\d\\d\\d1" regex-replace "port-$0"
```

A.5.8.14 RADIUS Attributes from Change of Authorization (CoA) Messages

You can map RADIUS attributes, from Change of Authorization (CoA) messages used to drive subscriber-based SandScript, to subscriber attributes.

Before configuring CoA attribute mapping, check what UDP destination port is used for these RADIUS messages, and enable it in the IPUserMap configuration. For example, if CoA packets are sent to destination port 3799, a configuration similar to this is required:

```
SRP# set config service ip-user-map enabled true
SRP# set config service ip-user-map radius enabled true
SRP# add config service ip-user-map radius interface "PORT_1 3799
SRP# set config service ip-user-map radius capture-mode encapsulated-udp
SRP# add config service ip-user-map radius accounting sub-name attribute "31"
```

Sandvine Incorporated
408 Albert Street
Waterloo, Ontario, Canada
N2L 3V3

Phone: (+1) 519-880-2600
Fax: (+1) 519-884-9892

Web Site: www.sandvine.com