SR-S4000 1.9.1

Functional Specification

SR-S4000

Tandem Softswitch with Limited SBC Functions

Document type	Functional Specification
Software version	1.9.1
Release date	2016-04-22
Internal ID	DOC063442
Department	Documentation Dept.

SwitchRay Inc. reserves the right to change any information contained in this document without prior notice.

Table of Contents

1 Introduction

1.1 Document Profile

The document describes the architecture of the SR-S4000 software application, provides a list of its main technical and functional specifications, as well as enumerates hardware and software requirements for correct operation of SR-S4000.

1.2 List of Abbreviations

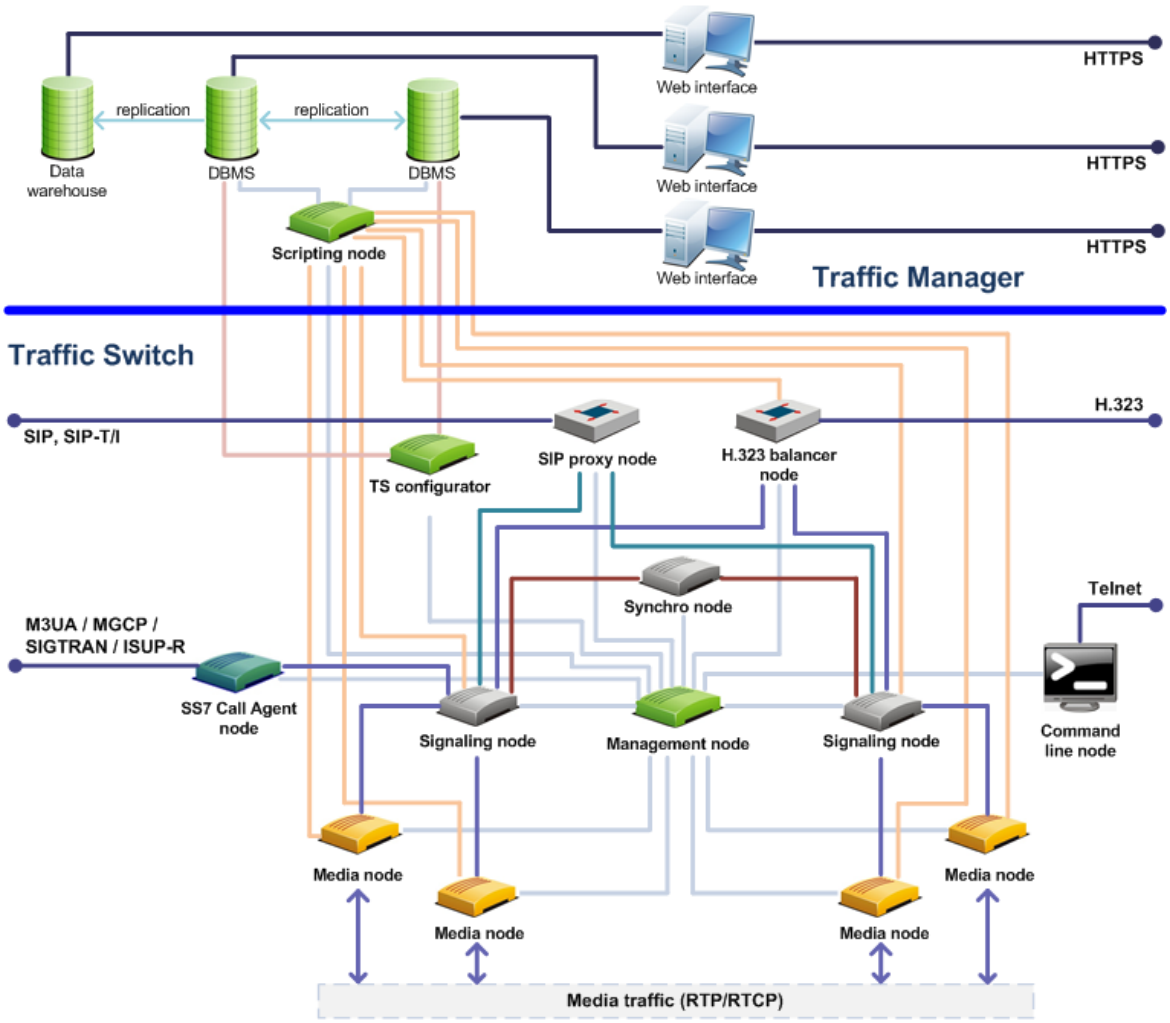
Abbreviation	Explanation
AAA	Authentication, Authorization, Accounting.
ACD	Average Call Duration. ACD is one of the operational parameters registered in SR-S4000. ACD allows the evaluation of dial peer performance.
ASP	Application Server Process.
ASR	Answer Seizure Ratio. In SR-S4000, ASR is calculated: • According to ITU-T Recommendation E.411, paragraph 3.6.3. This method is used by H.323 balancer and SIP proxy nodes to distribute workload among signaling nodes. ASR calculation is based on data received within the last 5 seconds. • According to the SR-S4000 intrinsic formulae used routing policies, statistical reports and charts. For details, see *SR-S4000 1.9.1 Web Interface Reference Guide*.
CDR	Call detail record. Set of data fields (call ID, call start and termination time, disconnect reason, etc) used for accounting and billing.
CPC	Calling Party Category.
CPS	Calls per second.
CSV	Comma Separated Values – text format used to represent data in tabular form. Each string in the file is a row of the table. The values of each column is separated by a delimiter, for example, a comma (,), semicolon (;) or a tab symbol. Text values are embraced in double quotes ("); if the text value itself contains double quotes – they are represented by two double quotes following each other.
DB	Database.
DBMS	Database management system.
DTMF	Dual Tone Multi-Frequency.
ENUM	Telephone Number Mapping (from tElephone Number Mapping.) A suite of protocols to unify the telephone numbering system E.164 with the Internet addressing domain name system.
H.323	An ITU-T recommendation that defines the protocols to provide audio-visual communication sessions on any packet network.
IPSP	IP Server Process. A process instance of an IP-based application. An IPSP is essentially the same as an ASP, except that it uses M3UA in a point-to-point fashion.
ISUP	ISDN User Part. A PSTN feature.
LAR	Look-Ahead Routing.
LNP	Local Number Portability.

Abbreviation	Explanation
M3UA	Message Transfer Part 3 User Adaptation Layer.
MGCP	Media Gateway Control Protocol
MNP	Mobile Number Portability.
NAT	Network Address Translation
OoDRPS	Out-of-dialog requests per second (SIP). Out-of-dialog requests are: • all new requests except INVITEs and REGISTERs; • requests with no tag in the To header field. For example, OPTIONS is generally considered to be an out-of-dialog request. However, received within an already established dialog it does not take part in the OoDRPS limitation.
PoD	Packet of Disconnect (in RADIUS Accounting).
PSTN	Public Switched Telephone Network.
QoS	Quality of Service. It is a statistical parameter calculated with the the following formula: *QoS = old_QoS + (100 * received / (received + late + lost) - old_QoS) / EMA* where: – old_QoS – QoS value calculated previously. Initial value is 100. – received – total number of received media packets. – late – number of late media packets. – lost – number of lost media packets. – EMA – value of the "Number of calls for EMA calculation system" global setting. The bigger is the calculated QoS value, the better is QoS.
RADIUS	Remote Authentication Dial-In User Service.
RFC	Request For Comments.
RPS	Registrations per second.
RTP/RTCP	Real-Time Protocol / Real-Time Control Protocol.
SBC	Session Border Controller.
SIGTRAN	(from SIGnaling TRANsport) a family of protocols, which is an extension of the SS7 protocol family.
SIP	Session Initiation Protocol.
SIP-I	SIP with encapsulated ISUP.
SIP-T	SIP for Telephones.
SNMP	Simple Network Management Protocol.
SS7	Signaling system 7.
TS	Traffic Switch, an application functioning as a session border controller that handles calls under the control of Traffic Manager.
UDP	User Datagram Protocol. One of the core members of the Internet protocol suite (the set of network protocols used for the Internet).
VSA	Vendor-specific attribute.
VoIP	Voice over Internet Protocol.

2 System Overview

SR-S4000 (also known as MVTS Pro) integrates the functionality of a class 4 switch with the capability of a session border controller designed for comprehensive management of IP telephony traffic flowing across the ITSP's network.

From the design viewpoint SR-S4000 comprises two sets of functional nodes: Traffic Switch (TS) and Traffic Manager.



2.1 Traffic Switch

Traffic Switch is the switching layer of the SR-S4000 system. Traffic Switch handles SIP, H.323, SIP-T/I, ITU-ISUP and MGCP protocols, and performs two-way conversion of signaling protocols and voice codecs when necessary. Additionally, Traffic Switch is the primary source of call statistics that is analyzed and visualized by means of Traffic Manager, provides monitoring of the system and is responsible for notifications.

Traffic Switch comprises the following functional nodes, each one being an individual process:

- **Management node** ensures distribution of configuration data between other TS nodes, provides centralized control over them and serves as a collection point for SR-S4000 statistics.
- **H.323 Balancer node** serves as the entry point for H.323 traffic. The node handles H.323 registration (RAS) requests and provides load balancing among signaling nodes. When a user (calling device) tries to register with SR-S4000, the H.323 balancer node forwards relevant data to Traffic Manager. Depending on the response received, the registration request is either accepted or rejected. Load balancing is based on the current ASR value of each signaling node.
- **SIP proxy node** balances arriving SIP calls among signaling nodes, and serves as the single exit point for SIP traffic.
- **Signaling node** provides two-way conversion of SIP/H.323/SIP-T/SIP-I signaling protocols and traffic distribution (load balancing) among media nodes (based on the current CPU load of each media node), as well as between scripting nodes (based on the number of serviced calls on each scripting node). Also, the signaling node handles SIP registrations.
- **Media node** handles media flows, functions as an RTP media proxy and performs conversion of voice codecs. The number of media nodes needed in SR-S4000 depends on the anticipated number of concurrent call sessions that involve RTP media proxy operation.
- **Command line node** is a telnet server that allows logging to a switching host using any telnet client.
- **SS7 Call Agent node** interworks with signaling gateways over M3UA, manages media gateways over MGCP SIGTRAN/MGCP, handles ISUP-R.
- **TS configurator** transfers configuration data from the DB to internal TS tables, as well as monitoring data from internal TS tables to the web interface. Monitoring data is viewed and configuration is edited in the **Traffic Switch** category of objects in theweb interface. The TS configurator interacts only with two DBs (primary and failover).
- **Synchro node** ensures control over the used resources.

2.2 Traffic Manager

Traffic Manager carries out authentication and authorization of VoIP endpoints, performs call routing, call analysis, validation and transformation of call numbers, traffic load balancing and interoperates with external routing servers. In addition, Traffic Manager performs QoS control functions and generates information required for external billing systems.

Traffic Manager consists of the following parts:

- **Database Management System (DBMS)** used to handle information about system settings and all data necessary for call routing, online billing and statistical analysis. Traffic Manager can contain maximum two DBMSs used for routing. To perform resource-intensive tasks (generation of reports, CDRs processing), it is possible to install the third "slave" DBMS used only as a data warehouse.
- **Web interface** provides a convenient graphical interface for administration tasks. Each web interface connects to its own database.

- **Scripting node** manages the execution of scripts that enable the System's routing and its interoperation with external routing and accounting hosts. The number of scripting nodes is limited only by hardware resources of the system.

3 Technical Data and Specification

Carrier-to-Carrier/Carrier-to-Enterprise Connectivity

- Conversion of media codecs:
  - G.729;
  - G.729A;
  - G.729B;
  - G.729AB;
  - G.723.1;
  - G711A-Law;
  - G.711μ-Law;
  - GSM FR;
  - Speex (information about its limitations is in the *SR-S4000 1.9.1 Administrator's Manual*);
  - iLBC;
  - AMR NB;
  - G.726;
  - G.722;
  - G.722.1;
  - G.722.2;
  - Opus.
- Support for and conversion of H.323 and SIP dialects, as well as ITU ISUP and SIP-I/T;
- T.38 fax pass-through;
- Transfer to the originator of SIP 181 message sent by the called party;
- SIP and H.323 video pass-through using H.261, H.263, H.264 codecs;
- Interoperation with SS7 signaling gateways over M3UA;
- Management of SS7 media gateways via MGCP;
- Connection to the PSTN through gateways Audiocodes Mediant-2000, -3000, -5000, Protei ITG, Proton-SSS, Quintum Tenor-DX, Tenor-CMS, Zyxel MSAP2000;
- Support of the majority of methods for DTMF transfer, including RFC 2833, SIP INFO, Inband DTMF in G.711 codec (for receiving only), signaling DTMF in H.245, Q.931.

Supported protocols

The following ITU-T standards are supported:

- H.323 v.2-v.4 “Packet-based multimedia communications systems”;
- H.245 v.7 “Control protocol for multimedia communication”;
- H.225 v.4 “Call signalling protocols and media stream packetization for packet-based multimedia communication systems”.

SIP (the current version of SR-S4000 uses TCP and UDP as transport protocols for SIP):

Basic signaling protocols:

- RFC 3261 “SIP: Session Initiation Protocol”;
- RFC 3326 “The Reason Header Field for the Session Initiation Protocol (SIP)”;
- RFC 2976 “The SIP INFO Method”.

Privacy:

- RFC 3323 “A Privacy Mechanism for the Session Initiation Protocol (SIP)”;
- RFC 3324 “Short Term Requirements for Network Asserted Identity”;
- RFC 3325 “Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks”;

- SIP Extensions for Caller Identity and Privacy (Cisco proprietary way to handle privacy (Remote-Party-ID).

SIP extensions:

- RFC 3581 “An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing”;
- RFC 4028 “Session Timers in the Session Initiation Protocol (SIP)”;
- RFC 4694 “Number Portability Parameters for the "tel" URI”;
- RFC 5168 “XML Schema for Media Control” (picture_fast_update is supported);
- RFC 5806 “Diversion Indication in SIP”;
- The Calling Party's Category tel URI Parameter;
- ANSI ISUP Originating Line Info Support (Dialogic specification).

Access Authentication:

- RFC 2069 “An Extension to HTTP : Digest Access Authentication”.

SIP-T/I:

- RFC 3204 “MIME media types for ISUP and QSIG Objects”;
- RFC 3372 “Session Initiation Protocol for Telephones (SIP-T): Context and Architectures”;
- RFC 3398 “Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping”;
- Q. 1912.5 “Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part”.

SDP:

- RFC 3264 “An Offer/Answer Model with Session Description Protocol (SDP)”;
- RFC 3551 “RTP Profile for Audio and Video Conferences with Minimal Control”;
- RFC 3555 “MIME Type Registration of RTP Payload Formats”;
- RFC 4566 “SDP: Session Description Protocol”..

DTMF:

- RFC 2833 “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals” (only in SIP and MGCP);
- SIP INFO Method for DTMF Tone Generation (Cisco specification);
- Inband DTMF in G.711 codec (detection and/or transparent pass-through);
- H.323 signaling messages:
  – by an alphanumeric H.245 User Input message (as digits);
  – by an alphanumeric H.245 User Input message (as string);
  – by H.245 signal;
  – by a Q.931 Facility message with field Keypad.

RTP/RTCP:

- RFC 3550 “RTP: A Transport Protocol for Real-Time Applications”;
- RFC 3551 “RTP Profile for Audio and Video Conferences with Minimal Control”.

SS7:

- ITU-ISUP 2000;
- M3UA (as ASP and IPSP, refer to RFC 4666);
- MGCP (management of media gateways, as per RFC 3435).

Monitoring over SNMP:

- SNMP v1 (RFC 1157);
- SNMP v2c, (RFC 1901);

- GET, GETNEXT, GETBULK requests to get counters and dispatch of SNMP traps using Net-SNMP application in Linux OS. For detailed description refer to http://www.net-snmp.org;

RADIUS (AAA, Routing, Packet of Disconnect):

- RFC 2865 “Remote Authentication Dial In User Service (RADIUS)”;
- RFC 2866 “RADIUS Accounting”;
- RFC 3576 “Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)”;
- RFC 3580 “IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)”;
- RFC 5080 “Common Remote Authentication Dial In User Service (RADIUS)”.

ENUM, RFC 3761 “The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery system (DDDS) Application (ENUM)”.

Network security and SBC functions

- NAT traversal:

  The system automatically detects hosts behind NAT devices. For this, it checks a host address written in the last network packet coming from a device. If it differs from the actual address where the packet comes from, the device is considered to be behind a NAT. In this case the system sends all further packets to the address from which this last packet originates.
  Media flow processing is the same. If media source address differs from the one specified in the signaling messages, the system transmits the media stream to the address from which the opposite stream comes.
  Please note that calls to H.323 terminal can't be placed if NAT router ports are defined dynamically.

- Concealment of the owner's network topology.
- Limitation of incoming traffic: the SIP proxy node can be configured to receive traffic only from trusted realms.
- Caller authentication by IP or username based on data stored in the DB.
- Caller authentication by a set of parameters based on:

  — data stored in the DB.
  — data received from RADIUS servers.

- Prevention of calls looping.
- Limitation of incoming calls by their rate (CPS).
- Limitation of incoming SIP and H.323 registrations by their rate (RPS).
- Limitation of the number of concurrent calls.
- Limitation of the number of out-of-dialog requests per second (OoDRPS).
- Limitation of the number of simultaneous calls from/to a certain phone number.

Anti-fraud functions

- FAS (False Answer Supervision) prevention.

  If SR-S4000 receives an Alerting/Progress or Connect message earlier than it is defined in the equipment configuration, the call is considered fraudulent and rejected with a specific predefined LDC.

Call routing

- Rerouting on route unavailability;
- Routing of calls to telephone numbers that were ported within landlines (Local Number Portability, LNP) or wireless networks (Mobile Number Portability, MNP).

Native routing capabilities

- Routing based on the calling/called number;
- Day-of-week and time-of-day based routing;
- Least busy (gateway/route) alternative routing;
- Routing policies based on route health parameters (ASR, ACD, etc);
- Gateway group ID (one gateway may belong to several groups);
- Route selection based on CPC and other parameters;
- URI-based routing.

External routing (including external Least Cost Routing systems)

- ENUM-aided routing;
- RADIUS-aided routing;
- SIP 302-aided routing.

Statistics and network analysis

- Display of CDRs meeting user-defined parameters;
- Export of CDRs into a text file (including scheduled export);
- Real-time monitoring of ASR, QoS, ACD, etc.;
- Monitoring of selected gateway/route performance statistics;
- Automated log file management (archiving, file size and file rotation control).

Billing

- Single CDR collection point;
- Great number of fields in CDRs for detailed analysis and debugging;
- Generation of interim CDRs to store accounting data on active calls;
- Integration with external billing systems using RADIUS protocol with an option to configure the contents and dispatch sequence of Accounting packets;
- Generation and dispatch of interim Accounting packets to the RADIUS server;
- Cisco VSA;
- Authorization of users in the external billing system based on the data provided by SR-S4000;
- Support of PoD.

Number and URI translation

- Flexible number translation options based on regular expressions;
- Separate number translations for routing, billing and SORM LI (on gateways, when calls enter/leave the system, for pre-routing and post-routing);
- Translation of CPC and other call parameters.

Configuration management

- Managing configuration via web interface supporting a flexible system of roles;
- Secure authentication and authorization of the system users', including configurable web password policies;
- Console interface via telnet;
- Provisioning the DB via web API over SOAP;
- Importing data into the DB from CSV & XLS files;
- Exporting data from the DB into CSV files.

Logging and debugging

- System trace logs with selectable information detail level;
- Call log viewing through the web interface;
- Call simulation;
- Logs of users' actions in the web interface.

Fault tolerance and availability

The fault tolerance of TS is achieved due to its modular architecture. It is possible to run a whole set of nodes of the same type that increase the overall system performance and backup each other.

The fault tolerance of the DBMS is ensured by installing an additional DBMS and configuring replication between DBMSs.

Geographically distributed configuration

- Modular design;
- Locations intended to unite geographically close nodes that should interoperate with each other only;
- Dynamic distribution of licenses among locations.

4 Software Requirements

The system is supplied as a bundle of software applications running on Debian GNU/Linux 7.0 (amd64 Wheezy) with 64-bit kernel and 64-bit operating environment.

The SR-S4000 database server uses the MySQL DBMS.

Supported web browsers:

- Mozilla Firefox starting from 40.x
- Google Chrome starting from 44.x
- Microsoft Internet Explorer 11

Other versions of web browsers may not be fully compatible with the web interface.

5 Hardware Requirements

The minimum hardware requirements for SR-S4000 are as follows:

- 8 core CPU.
- 16 GB of RAM.

The recommended platform is **HP Proliant DL360**.

Deployment of the system in virtualization environments is only allowed at the testing stage. For commercial usage it is only permitted to run the system on physical servers. Otherwise, the manufacturer does not guarantee failure-free operation of the system.

If system redundancy is employed, each server used in the redundancy scheme should have at least two network interfaces.

6 Version History

Below are major changes and improvements implemented in previous versions of SR-S4000. For the full list of changes and improvements, refer to Release Notes available on our Help Desk.

6.1 1.8.1 > 1.9.1

- All SR-S4000 components now run on a 64-bit platform. System operation on a 32-bit platform is no longer supported.

Traffic Switch

- SIP messages can be transferred over TCP.
- Traffic Switch includes two new nodes: SIP proxy node and TS configurator.
- Mechanism for setting limits for SIP and H.323 traffic is more flexible.
- The System is capable of transferring SIP 181 responses "Call is being forwarded" from called device to calling device working over SIP or SIP-T/I protocol.
- RFC 4028 standard is supported to keep the SIP session alive by sending periodic re-INVITE or UPDATE requests.

Traffic Manager

- The new version can work with telephone numbers that were ported within landlines (Local Number Portability, LNP) or wireless networks (Mobile Number Portability, MNP).
- The traffic can be distributed among dial peer devices according to their "weight".
- The navigation tree, tables, and tools have two working modes: simple (limits the displayed content to a predefined items) and advanced (displays the full version of the navigation tree or an object).
- It is easier to configure filtering of pre-routing translation rules and dial peers. In previous versions, for a number of settings, pairs of allowed and forbidden values could be set, now it is possible to set only forbidden values. All values that are not present in a list of forbidden values are considered to be allowed.
- It is easier to delete DB tables with CDRs.
- The **Inaccurate CDRs** category was removed from the web interface: SR-S4000 automatically restores call data in case of problems and deletes duplicate CDRs.
- New functionality was added to prevent possible looping of calls.
- It is possible to limit the number of outgoing CPS.
- It is possible to configure rerouting (LAR) globally, that is, for all devices without individual settings.
- The mechanism used to check configuration of SS7 Call Agent nodes was improved: incorrect settings can no longer be saved and the wizards work better. Due to that, Class 4 switch is more stable now while interacting with SS7.
- It is possible to edit disconnect codes not only for all gateways interacting with the System, but also for a particular gateway.
- It is possible to configure replacement of **Screening Indicator** and **Presentation Indicator** values of incoming calls in pre-routing translation rules, as well as forbid selection of pre-routing translation rules for calls with specific values of these parameters.

6.2 1.7.4 > 1.8.1

Traffic Manager

- Call routing according to URIs (Uniform Resource Identifiers).
- CDRs storage in daily tables.
- Flexible call debug logging.

6.3 1.7.3 > 1.7.4

Traffic Switch

- The original duration of DTMF signals can be saved and transmitted now when they pass through the system.
- Now it is possible to transmit key frame within video stream as per RFC 5168, to enhance video quality.

6.4 1.7.2 > 1.7.3

Traffic Manager

- SIP 302-aided routing.

6.5 1.6.0 > 1.7.2

Traffic Switch

- Support of codecs G.722, G.722.1 (including Annex C), AMR-WB/G.722.2.
- Ability to dispatch SNMP traps.

Traffic Manager

- Changed the mechanism for system interoperation with RADIUS servers, including the procedure for resending of undelivered packets and the method for switching between RADIUS servers in case in case the active one is unavailable.
- The configuration of the SS7 Call Agent node has been moved to the web interface.