SC

Service Connector

SC Message Protocol V1.0

SC_1_SCMP-V1.0_E (Version V2.6V2.5)

This document describes the SC Message Protocol V1.0 (SCMP).

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

This document is a spiritual ownership of STABILIT Informatik AG, and must not be used or copied without a written allowance of this company. Unauthorized usage is illegal in terms of Chapter 23 / 5 UWG / Swiss law.

The information in this document is subject to change without notice and should not be construed as a commitment by STABILIT Informatik AG.

Copyright © 2010 by STABILIT Informatik AG
All rights reserved.

All other logos, product names are trademarks of their respective owners.

CONFIDENTIAL

This Document has been created with Microsoft Word 2003 (11) with template file C:\STABILIT\STANDARD\TEMPLATES\S_REP_E.DOT and printed at 01 July 2010 14:55.

Identification

Project:	SC
Title:	Service Connector
Subtitle:	SC Message Protocol V1.0
Version:	V2.6~~V2.5~~
Reference:	SC_1_SCMP-V1.0_E
Classification:	Confidential
Keywords:	Concepts, Communication, Protocol
Comment:	This document describes the SC Message Protocol V1.0 (SCMP).
Author(s):	STABILIT Informatik AG Jan Trnka, Daniel Schmutz, Joel Traber
Approval (Reviewed by):	Signature ..... Jan Trnka Signature ..... Francisco Gonzalez Signature ..... Walter Mörgeli
Audience:	Project team, Eurex IT management, Review team
Distribution:	Project team, SIX development team
Filename	c:\stabilit\projects\eurex\sc\documents\sc_0_scmp_e.doc

Revision History

Date	Version	Author	Description
14.06.2009	D1.0	Jan Trnka	Initial draft
09.08.2009	D1.1	Jan Trnka	Separate specification and architecture documents. Fill information from Daniel into this document.
…	…	Jan Trnka	Many changes in between not tracked
24.2.2010	V2.0	Jan Trnka	Proposal for C-API
3.3.2010	V2.1	Jan Trnka	Remove SC architecture from this document
11.4.2010	V2.2	Jan Trnka	Prepare for review
14.4.2010	V2.3	Jan Trnka	Put API into its own document
2.6.2010	V2.4	Jan Trnka	Multi-Session Server changed, ATTACH instead of CONNECT
15.6.2010	V2.5	Jan Trnka	Corrections after SIX workshop and review
30.6.2010	V2.6	Jan Trnka	Cleanup confusion detected by R. Frey Improve keepalive description Attr. *authSessionId* introduced Attr. *noDataInterval* introduced Headline format changed Chapter “Subscription monitoring” added Matrix reviewed Last header attr. also terminated with <LF> Definition of file services and http proxy.

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

Table of Contents

1 PREFACE 5
1.1 Purpose & Scope of this Document 5
1.2 Definitions & Abbreviations 5
1.3 External References 5
1.4 Typographical Conventions 5
1.5 Restrictions 6
1.5.1 Load balancing 6
1.5.2 Failover 6
1.5.3 Security 6
1.5.4 Intrusion and Virus Protection 6
1.6 Outstanding Issues 6

2 ~~COMMUNICATION SCHEMA~~ 10
~~2.1 Connection Topology~~ 10
~~2.2 Network Security~~ 11

~~3~~ SERVICE MODEL 6
2.1~~3.1~~ Session Services 7
~~3.~~2.2 Publishing Services 8
2.3~~.3~~ File Services 8

2.4~~3.4~~ ..... HTTP PROXY SERVICES 93 COMM
3.1 Connection Topology 10
3.2 Network Security 11
3.3 Connection Management 16
3.4 Session Monitoring 16
3.5 Subscription Monitoring 17
3.6 Abort and Restart 17
3.6.1 Client 17
3.6.2 Server 17
3.6.3 SC 17

4 MESSAGE PROTOCOL 19
4.1 Headline 19
4.2 Header 20
4.3 Body 20
4.4 SCMP over TCP/IP 20
4.5 SCMP over HTTP 20
~~4.6 HTTP over SCMP~~ 21

5 SEMANTIC 22
5.1 Session Service 22
5.1.1 Asynchronous Message Exchange 24
5.1.2 Large Messages 24
5.1.3 Single Session Server 26
5.1.4 Multi Connection Server 26
5.1.5 Application Server (Tomcat) 27
5.2 Publishing Service 28
5.2.1 Large Published Message 30
5.3 File Service 30
5.4 HTTP Proxy~~Redirection~~ Service 32

6 SCMP MESSAGES 34
6.1 Keepalive 34

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

6.26.1 ATTACH (ATT) 34
6.36.2 DETACH (DET) 34
6.3 KEEPALIVE (KPL) 35
6.4 INSPECT (INS) 35
6.5 MANAGE (MGT) 35
6.6 CLN_CREATE_SESSION (CCS) 36
6.7 SRV_CREATE_SESSION (SCS) 36
6.8 CLN_DELETE_SESSION (CDS) 37
6.9 SRV_DELETE_SESSION (SDS) 37
6.10 SRV_ABORT_SESSION (SAS) 38
6.11 REGISTER_SERVICE (REG) 38
6.12 DEREGISTER_SERVICE (DRG) 39
6.13 CLN_DATA (CDA) 39
6.14 SRV_DATA (SDA) 40
6.15 CLN_ECHO (CEC) 40
6.16 SRV_ECHO (SEC) 41
6.17 CLN_SUBSCRIBE (CSU) 41
6.18 SRV_SUBSCRIBE (SSU) 42
6.19 CLN_CHANGE_SUBSCRIPTION (CHS) 42
6.20 SRV_CHANGE_SUBSCRIPTION (SHS) 43
6.21 CLN_UNSUBSCRIBE (CUN) 43
6.22 SRV_UNSUBSCRIBE (SUN) 44
6.23 RECEIVE_PUBLICATION (CRP) 44
6.24 PUBLISH (SPU) 45
6.25 FILE_DOWNLOAD (FDO) ..... HTTP (HTT) 456.26 FILE_U
6.27 FILE_LIST (FLI) 46

7 SCMP HEADER ATTRIBUTES 48
7.1 appErrorCode (aec) 48
7.2 appErrorText (aet) 48
7.3 authSessionId (asi) 48
7.4 bodyType (bty) 48
7.57.4 cacheExpirationDateTime (ced) 49
7.67.5 cacheId (cid) 49
7.77.6 clnRequesterId (crq) 49
7.87.7 compression (cmp) 50
7.9 echoInterval (eci) 50
7.10 echoTimeout (ect) 50
7.117.8 ..... immediateConnect (imc) 50
7.127.9 ..... ipAddressList (ipl) 50
7.13 keepaliveInterval (kpi) 51
7.147.10 localDateTime (ldt) 51
7.157.11 messageID (mid) 51
7.167.12 messageInfo (min) 52
7.177.13 messageType (mty) 52
7.187.14 mask (msk) 53
7.197.15 maxSessions (mxs) 53
7.207.16 noData (nod) 53
7.21 noDataInterval (noi) 53
7.22 originalMessageID (omi) 54
7.237.17 portNr (pnr) 54
7.247.18 receiverTimeout (rct) 54
7.19 rejectSession (rej) 54
7.25 remoteFileName (rfn) 55
7.267.20 scErrorCode (sec) 55
7.277.21 scErrorText (set) 55
7.287.22 scReqesterId (crq) 55
7.297.23 scResponderId (crs) 55
7.307.24 scVersion (ver) 56
7.317.25 senderTimeout (snt) 56

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

~~7.26~~ serviceName (nam) 56
7.32~~7.27~~ sessionId (sid) 57
7.33~~7.28~~ sessionInfo (sin) 57
7.34~~7.29~~ srvRequersterId (srq) 57
7.35~~7.30~~ srvResponderId (srs) 57

8 GLOSSARY 58

APPENDIX A MESSAGE HEADER MATRIX 60

INDEX 62

Tables

Table 1 Abbreviations & Definitions 5
Table 2 External references 5
Table 3 Typographical conventions 6

Figures

Figure 1 ~~Communication Layers~~ 10
~~Figure 2 Connection Topology~~ 11
~~Figure 3 Network Security~~ 12
~~Figure 4~~ Synchronous Request/Response 7
Figure 2~~5~~ Asynchronous Request/Response 8
Figure 3~~6 Asynchronous~~ Subscribe / Publish ..... 8Figure 4 File service 9
Figure 5 HTTP proxy service 9
Figure 6 Communication Layers 10
Figure 7 Connection Topology 11
Figure 8 Network Security 12
Figure 9 Service Connector Message Protocol 19
Figure 10~~8~~ Synchronous Message Exchange 22
Figure 11~~9~~ Asynchronous Session Service Message Exchange 24
Figure 12~~10~~ Large Response 24
Figure 13~~11~~ Large Request 25
Figure 14~~12~~ Multi-Connection server (immediateConnect = true) 26
Figure 15~~13~~ Multi-Connection server (immediateConnect = false) 27
Figure 16~~14~~ Publishing Service 28
Figure 17~~15~~ Large Published Message 30
Figure 18~~16~~ File upload and download ..... 32Figure 19 HTTP proxy 32

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

1 Preface

1.1 Purpose & Scope of this Document

This document describes the SCMP (**SC** **M**essage **P**rotocol).

The final and approved version of this document serves as base for the publication as Open Source.

This document is particularly important to all project team members and serves as communication medium between them.

1.2 Definitions & Abbreviations

Item / Term	Definition / Description
HTTP	Hypertext Transport Protocol
HTTPS	HTTP over SSL, encrypted and authenticated transport protocol
Java	Programming language and run-time environment from SUN
JDK	Java Development Kit
Log4j	Standard logging tool used in Java
OpenVMS	HP Operating system, platform for existing ERM application
RMI	Remote Method Invocation - RPC protocol used in Java
RPC	Remote Procedure Call
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer – secure communication protocol with encryption and authentication
TCP/IP	Transmission Control Protocol / Internet Protocol
SC	Service Connector
USP	Universal Service Processor – predecessor of SC
Wireshark	Open source product to capture and analyze network traffic

Table 1 Abbreviations & Definitions

1.3 External References

References	Item / Reference to other Document
[1]	SC_0_Specification_E – Requirement and Specifications for Service Connector
[2]	

Table 2 External references

1.4 Typographical Conventions

Convention	Meaning
text in italics	features not implemented in the actual release
`text in Courier font`	code example
[phrase]	In syntax diagrams, indicates that the enclosed values are optional
{ phrase1 | phrase2 }	In syntax diagrams, indicates that multiple possibilities exists.
…	In syntax diagrams, indicates a repetition of the previous expression

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

Table 3 Typographical conventions

The terminology used in this document may be somewhat different from other sources. The chapter Glossary includes a list of often used terms with the explanation of their meaning in this document.

1.5 Restrictions

1.5.1 Load balancing

The SC does not provide any load balancing features. Established communication session will not be redirected to another server node ~~initially or~~ during its life time.

1.5.2 Failover

The SC does not provide any failover features. Aborted communication must be re-established by the communicating partners. The client application must find out a service which is alive.

1.5.3 Security

The SC does not implement any security feature. The environment where SC is used must provide all required authentication, authorization, encryption, tunneling etc. features. Message transport over https will not be supported.

The IP address of the client and the IP of the incoming TCP/IP traffic will~~is~~ be available in the message header and can be evaluated by the server. This can be used to authenticate and authorize the client when VPN tunnel is used.

1.5.4 Intrusion and Virus Protection

The entire network where SC is used is assumed to be safe and secure. No virus protection is embedded in SC. The customer may use screening firewall to protect the SC components. It is recommended to use SC within a DMZ.

SC is not designed to withstand network attacks like DOS or SYNC flood, or any other.

1.6 Outstanding Issues

Following issues are outstanding at the time of the document release:

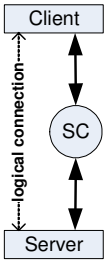
- Body structure for INSPECT and MANAGE message
- How is HTTP over SCMP implemented?
- chunked transfer encoding for SCMP over HTTP
- pipelining for SCMP over HTTP
- State diagram for client and server
- ~~Impact of a restart, what is to do~~
- Describe files services ~~(better)~~
- ~~Describe how keepalives are running and processed and what happens if not.~~
- Describe strategies how the SC chooses a free session server instance
- ~~Different Header Key PRQ/PRS for large request and large responses for better traceability~~
- ~~Possibly merge CLN_... and SRV_ messages.~~
- Describe caching of messages (not in this document?)

Describe how file service returns the list of files Service ModelThe SC supports message exchange between requesting application (client) and another application providing a service (server). The client and the server are the logical communication end-points. The SC never acts

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

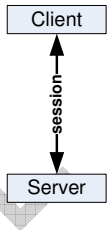
as a direct executor of a service. The client can to communicate to multiple services at the same time.



Server application can provide one or multiple service. Serving multiple services within one application is possible only for multithreaded or multisession servers. Multiple server applications are running on the same server node, each providing different service. All services are independent on each other. Server application may request another service and so play the client role.

1.7 Session Services

Request/Response (client initiated communication). For session services the client and the server exchange messages in context of a logical session through the SC.



Synchronous The client sends a request to a service that invokes an application code. Upon completion the service sends back a response message. The client waits for the arrival of the response message. The request and response message length is not limited in size.

The communication occurs in a scope of a logical session. SC will choose a free server and pass this and subsequent requests from this client to the same server. Session information is always passed as a part of the message header. The client may have only one outstanding request per session.

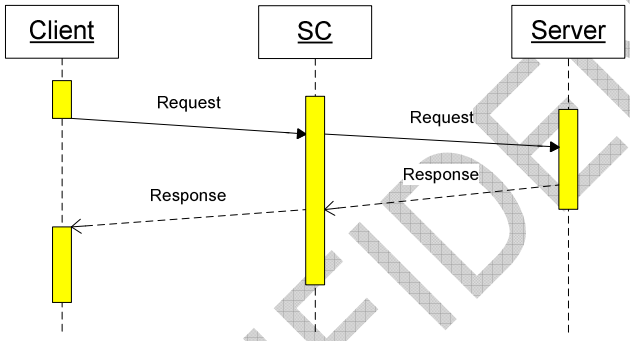
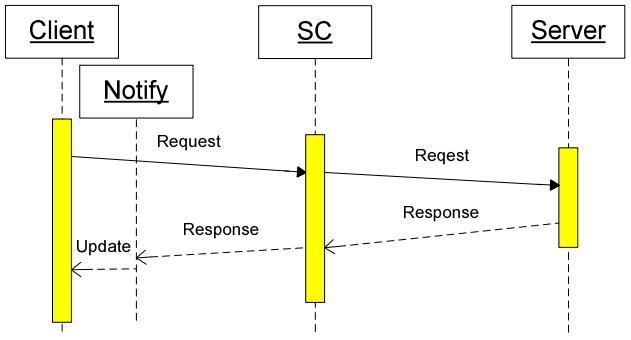


Figure 1 Synchronous Request/Response

Multiple clients may request the same service at the same time. The service execution is in parallel, each one in a separate thread or process. The server decides how many sessions it can serve.

This communication style is the most often used for getting data from the server or sending a message that triggers a transaction on the server.

Asynchronous Asynchronous execution is functionally equal to the synchronous case with the exception that the client does not wait for the arrival of the response message. The client must declare a notification method that is invoked when the response message arrives. The client may have only one outstanding request per session. When client issues a request before the previous one was completed, the send method blocks until the previous request is satisfied.



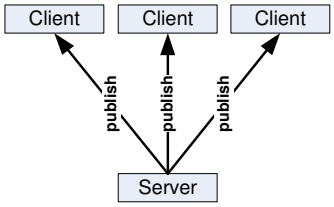
CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

Figure 2 Asynchronous Request/Response

This communication style will be used to load data while other activities are in progress, e.g. to get large amount of static data at startup. It can be also used as fire-and-forget when the response is not meaningful.

1.8 Publishing Services



Subscribe/Publish (server initiated communication). Publishing services allows the server to send single message to many clients through the SC.

The client sends a subscription mask to the service, and so declares its interest on certain type of a message. The application service providing the message contents must designate the message with a type. When the message type matches the client subscription mask, the message will be sent to the client. Multiple clients may subscribe for the same service at the same time. In such case multiple clients can get the same copy of the message. Message that does not match any client subscription is discarded.

The client must declare a notification method that is invoked when the message arrives. The client may have only one outstanding subscription per service. The message delivery must occur in guaranteed sequence. Messages from the same service will arrive in the sequence in which they have been sent.

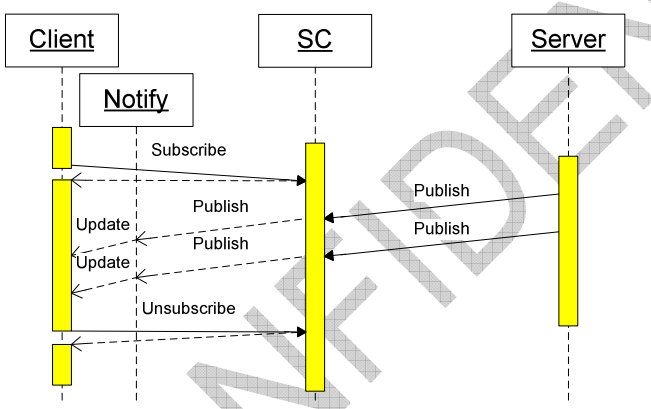


Figure 3 Subscribe / Publish

The client may change the subscription mask or unsubscribe. Initial subscription, subscription change or unsubscribe operation is always synchronous, even through a cascaded SCs.

Such communication style is used to get asynchronously events notifications or messages that are initiated on the server without an initial client action. It can be also used to distribute the same information to multiple clients.

1.9 File Services

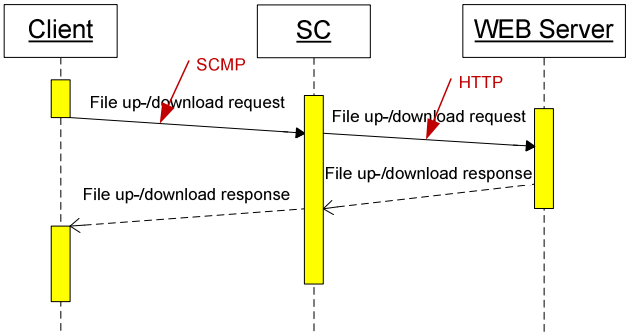
This SC service provides API for these file operations:

- Download file from the web server to the client.
- Upload file from the client to the web server.

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

List files in a file repository on the web



server.

Figure 4 File serviceHTTP Proxy ServicesThe SC supports redirecting of regular HTTP traffic to another server. It is acting like normal HTTP proxy without caching.

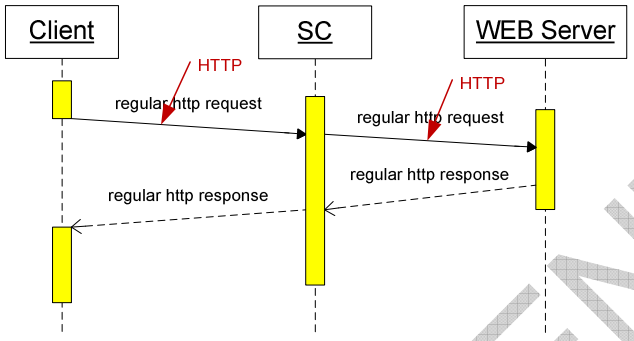


Figure 5 HTTP proxy service

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

2 Communication Schema

The SC implements peer-to-peer messaging above OSI layer-7 (application) network model between client and server applications. The SC is always in between the communicating partners, controlling the entire message flow.

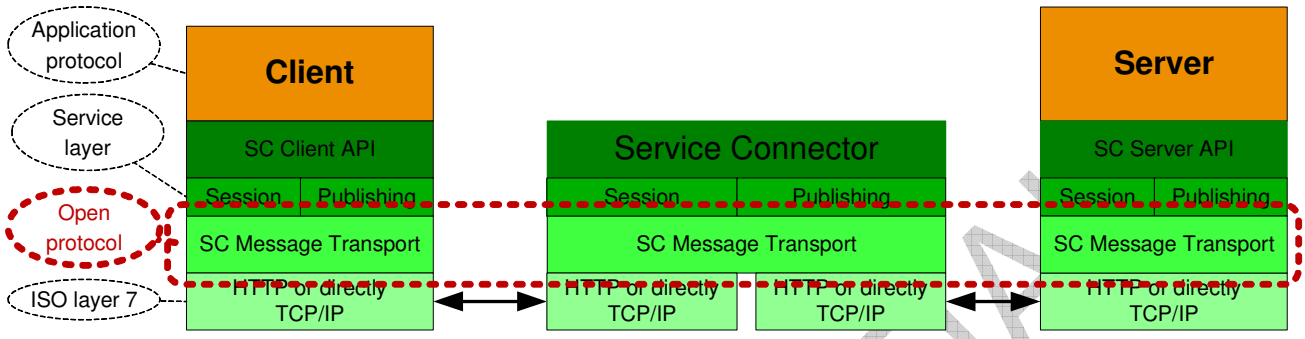


Figure 6 Communication Layers

The SC acts like a broker, passing messages between the client and the server. The communicating parties must agree on the application protocol i.e. format and content of the message payload.

2.1 Connection Topology

Client application, server application and the SC may reside on the same node or on separate nodes. The connection can either utilize HTTP protocol or direct TCP/IP communication. ~~connected via TCP/IP network.~~ No assumption about the physical network topology is done. Multiple firewalls can be located on the path between the communicating partners.

The SC supports following connection topology:

- Client ⇔ SC ⇔ Server = Direct connection
- Client ⇔ SC ⇔ SC ⇔Server = Connection via cascaded SC.
  Multiple SC ~~Proxies~~ may be placed on the path between the client and service.

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

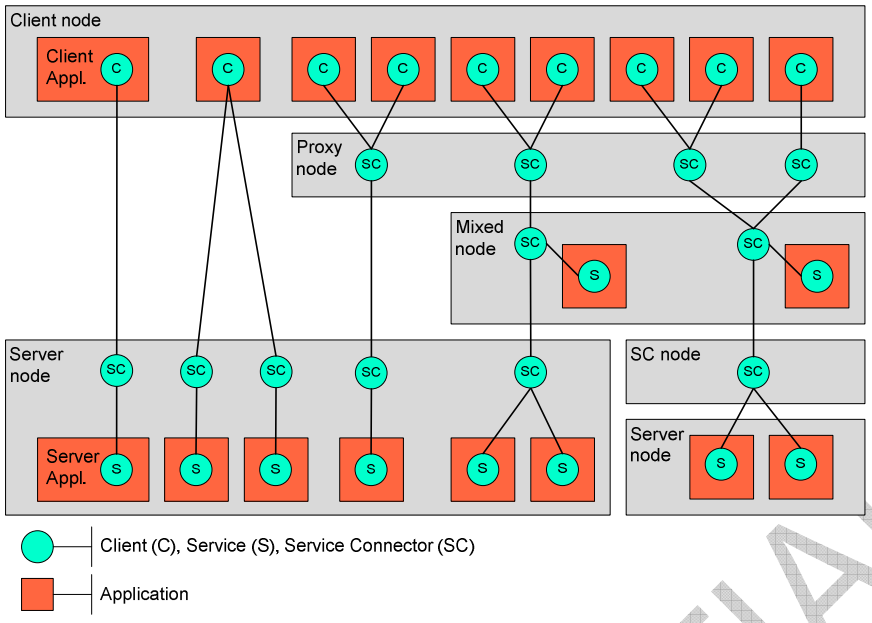


Figure 7 Connection Topology

Different connection topology types from left to right:

1. Client connected to one service
2. Client connected simultaneously to SCs and two services
3. Two clients connected to one service via proxy service and cascaded SC
4. Two clients connected to three services via proxy service on different server nodes
5. Complex configuration with three clients connected to three services on different server nodes via cascaded SCs and SC offloaded to its own node. One server can be registered to multiple services and different SCs. However this is possible for multisession servers only.

Limitation: The same service can be accessed by one SC only. When the same service should be used on different nodes, it must have a different name (e.g. node suffix).

Two different transport types can be individually configured for each network segment i.e. between the Client ⇔ SC, SC ⇔ SC or SC ⇔ Server.

HTTP
Such~~The~~ connection may pass screening firewalls and is appropriate for~~can either utilize HTTP protocol or direct TCP/IP~~ communication within the customer organization e.g. Client ⇔ SC or SC ⇔ SC.~~.~~
TCP/IP
Such connection would not pass firewalls without explicit security rules. It is useful for connection within the same node e.g. SC ⇔ Server.

SC cascading is used for performance and/or for security reasons. It is transparent for the application.

2.2 Network Security

From the security viewpoint~~, on the network,~~ the number of clients or server is not relevant. Meaningful are connections between nodes and security measures taken to protect legal subjects to which the particular network segment belongs. The following schema shows some possible networks that may be configured to pass SC messages.

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

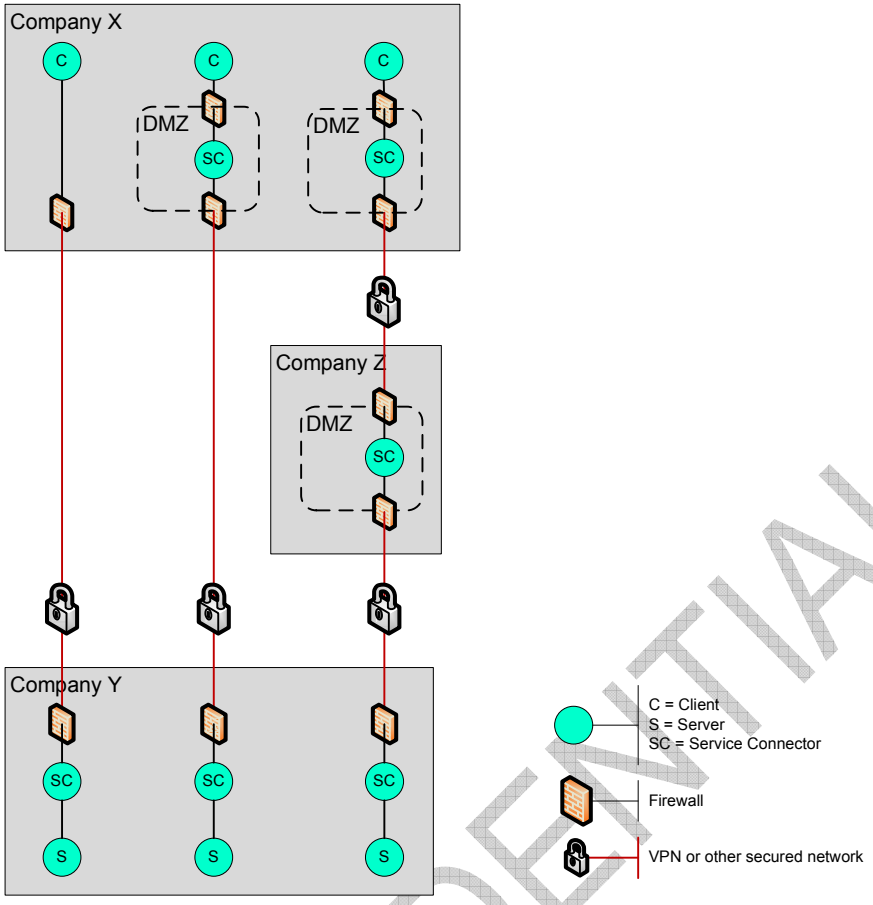


Figure 8 Network Security

Protocol

The message transport between each of the SC components (green bullet) may be configured as plain TCP/IP or HTTP. The connection is always initiated by the client (top-down in the picture above). The client defines which transport (TCP/IP or HTTP) it will use. The transport protocol between SC and the next downstream component is configured in the SC configuration. TCP/IP is strongly recommended between SCs through VPN tunnels as well as between SC and the Server for performance reasons. HTTP is recommended between the client and SC. For connection between SC and Web Server or Application Server (Tomcat) only HTTP can be used.

Firewall

Firewall with a proper configuration may be placed on any path between two SC components. Firewall between SC and the server is possible, but not recommended for performance reasons. For HTTP protocol the firewall can be configured to perform statefull packet inspection with HTTP filtering. For TCP/IP the appropriate port must be configured in the firewall.

When the message traffic will pass a firewall, HTTP protocol is recommended. In such case the SC can be seen as a regular Web-Server. The firewall can be configured to perform statefull packet inspection with HTTP filtering. For connection between SC and the server and for communications though VPN tunnels direct TCP/IP is recommended for performance reasons.

When HTTP connection is used and multiple parallel requests are in progress, SC will create multiple connections for each pending request in order to keep them balanced and so satisfy firewall inspection rules. (Statefull inspection rejects two subsequent GET/POST request without response from the server)

~~*Keepalive*~~

~~Each connection between two SC components is supervised by an algorithm using keepalive messages exchanged in regular (configurable) intervals. The sender monitors the arrival of the echoed message within a timeout; the receiver monitors the interval in which keepalive~~

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

~~messages should arrive. These two methods allow independent detection of broken connections on both sites in case the communication will be interrupted without notice. E.g. firewall swallows the traffic. This algorithm is essential for detection of broken sessions. Keepalive messages are very important to preserve the connection state in the firewall and reset their internal timeout. Only traffic to the outside may refresh the internal firewall timeout. That's why keepalive message is always initiated by the client. Using of keepalive messages can be disabled.~~

IP address list

Multiple SCs may be placed on the communication path between the client and the server. In order to allow comprehensive authorization all IP addresses are collected and made available to the server as a list. The list contains of ~~pairs of~~ IP addresses in the form 999.999.999.999. The order in the list has a dedicated meaning. The list has at least three~~four~~ entries.

1. IP of the client at Company X~~,~~
2. Incoming IP received by SC = IP of the VPN Tunnel~~.~~
3. IP of the SC at Company Y
4. ~~Incoming IP received by server~~

Client connected via cascaded SC placed in company's X DMZ will have the list in the format:

1. IP of the client at Company X~~,~~
2. Incoming IP received by SC in company's X DMZ.
3. IP of the SC in company's X DMZ
4. Incoming IP received by SC = IP of the VPN Tunnel.
5. IP of the SC at Company Y
6. ~~Incoming IP received by server~~

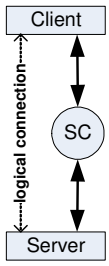
If ~~any of~~ the pairs 1,2 or 3,4 have ~~has~~ different values, then the corresponding~~in this~~ network segment uses VPN or NAT. As long as there is only one SC behind the VPN, the second~~third~~ last address is always the tunnel IP used for the authentication.

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

3 Service Model

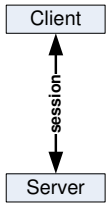
The SC supports message exchange between requesting application (client) and another application providing a service (server). The client and the server are the logical communication end points. The SC never acts as a direct executor of a service. The client can to communicate to multiple services at the same time.



Server application can provide one or multiple service. Serving multiple services within one application is possible only for multithreaded or multisession servers. Multiple server applications are running on the same server node, each providing different service. All services are independent on each other. Server application may request another service and so play the client role.

3.11.1 Session Services

Request/Response (client initiated communication). For session services the client and the server exchange messages in context of a logical session through the SC.



Synchronous

The client sends a request to a service that invokes an application code. Upon completion the service sends back a response message. The client waits for the arrival of the response message. The request and response message length is not limited in size.

The communication occurs in a scope of a logical session. SC will choose a free server and pass this and subsequent requests from this client to the same server. Session information is always passed as a part of the message header. The client may have only one outstanding request per session.

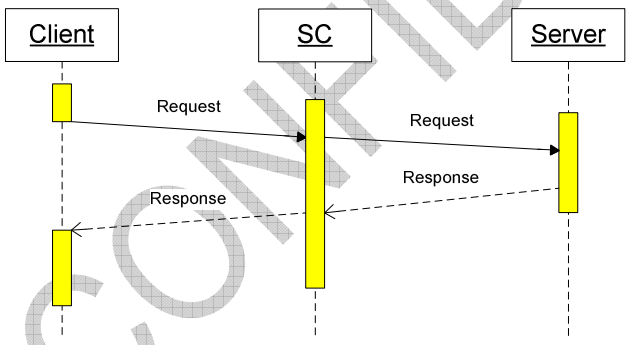


Figure 4 Synchronous Request/Response

Multiple clients may request the same service at the same time. The service execution is in parallel, each one in a separate thread or process. The server decides how many sessions it can serve.

This communication style is the most often used for getting data from the server or sending a message that triggers a transaction on the server.

Asynchronous

Asynchronous execution is functionally equal to the synchronous case with the exception that the client does not wait for the arrival of the response message. The client must declare a notification method that is invoked when the response message arrives. The client may have only one outstanding request per session. When client issues a request before the previous one was completed, the send method blocks until the previous request is satisfied.

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

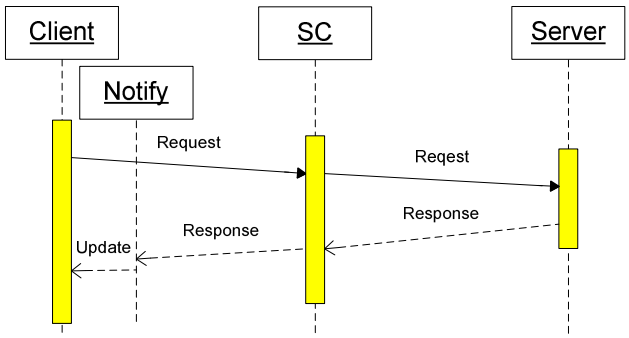
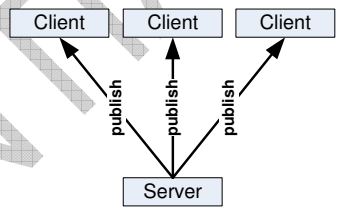


Figure 5 Asynchronous Request/Response

This communication style will be used to load data while other activities are in progress, e.g. to get large amount of static data at startup. It can be also used as fire-and-forget when the response is not meaningful.

3.21.1 Publishing Services

Subscribe/Publish (server initiated communication). Publishing services allows the server to send single message to many clients through the SC.



The client sends a subscription mask to the service, and so declares its interest on certain type of a message. The application service providing the message contents must designate the message with a type. When the message type matches the client subscription mask, the message will be sent to the client. Multiple clients may subscribe for the same service at the same time. In such case multiple clients can get the same copy of the message. Message that does not match any client subscription is discarded.

The client must declare a notification method that is invoked when the message arrives. The client may have only one outstanding subscription per service. The message delivery must occur in guaranteed sequence. Messages from the same service will arrive in the sequence in which they have been sent.

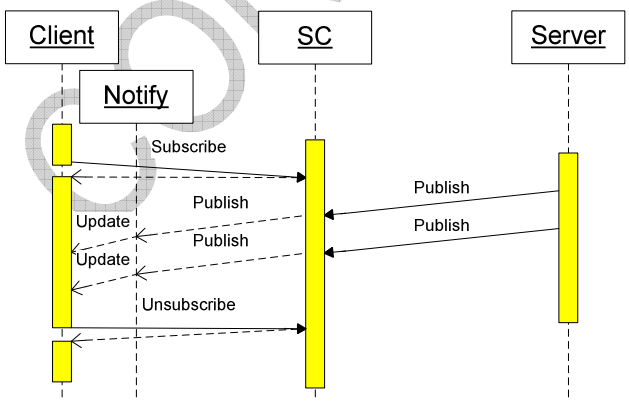


Figure 6 Asynchronous Subscribe / Publish

The client may change the subscription mask or unsubscribe. Initial subscription, subscription change or unsubscribe operation is always synchronous, even through a cascaded SCs.

Such communication style is used to get asynchronously events notifications or messages that are initiated on the server without an initial client action. It can be also used to distribute the same information to multiple clients.

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

~~3.31.1 File Services~~

~~This SC service provides API for these file operations:~~

- ~~Download file from the web server to the client.~~
- ~~Upload file from the client to the web server.~~
- ~~List files in a file repository on the web server.~~

~~3.43.1 HTTP Proxy Services~~

3.2 ~~The SC supports redirecting of regular HTTP traffic to another server.~~Connection Management

The network connections between client ⇔ SC or SC ⇔ SC is managed in a connection pool. New connections are created when necessary and deleted when they are idle for a long time.

Keepalive messages are sent in regular intervals on all idle connections initiated by a network peer. They are not sent on busy connections currently used for message exchange. E.g. while client is waiting for server response, the connection is busy and no keepalive message will be sent. On http connection statefull firewall inspection would reject two subsequent GET/POST request without previous response from the server. Using of keepalive messages can be disabled.

The only purpose of keepalive messages is to preserve the connection state in the firewall placed between the communicating peers and resets its internal timeout. Keepalive message is always initiated by the peer which has initiated the connection, because only outbound traffic may refresh the firewall timeout.

Client connections used for session or file services are mostly idle and will utilize the keepalive mechanism. Client connections used for publishing services are mostly busy. The meachnism to refresh the firewall timeout is built in the SCMP layer.

When an error occurs while sending or receiving a keepalive message, or the response does not timely arrive a log entry is created, the connection is closed and deleted from the pool. No error is signalled to the application.

The message has only a headline and no attributes and no body. The format is:

KRQ 0000000 00000 1.3

for request and

KRS 0000000 00000 1.3

for response.

3.3 Session Monitoring

Session monitoring is built on ECHO messages, exchanged during the active session between the client and the server in periodic intervals. Only a message exchanged between the logical communication end-points allows reliable signalling of an error to them. It is independent on the keepalive messages.

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

The client sends ECHO message in periodic intervals for each session service when no other request is in progress. It receives the echoed message back from the server.

SC monitors the traffic related to this session and takes actions when the messages exchange is disturbed. For the client side it monitors the interval in which echo messages are sent and notifies the server (SRV_ABORT_SESSION) when the session expires. Then SC cleans up the session. For server side SC monitors the response time of the echo message and informs the client (EXC response causing an exception) when the timeout expires. Then SC cleans up the session.

3.4 Subscription Monitoring

Subscription monitoring is built on RECEIVE_PUBLICATION messages, exchanged during the active subscription between the client and the SC in periodic intervals.

The client sends RECEIVE_PUBLICATION message in order to get the published data. The SC sends either the requested data or an empty response with the *noData* flag when no data is available and the *noDataInterval* is exceeded. The client starts then automatically a new RECEIVE_PUBLICATION request.

3.5 Abort and Restart

3.5.1 Client

When client aborts its activity abruptly (without a neat detach), then SC will not detect the session breakdown before the echo message interval is not exceeded. During this time new sessions can be created by the restarted client.

After client restart new connections to SC will be established, new sessions will be created and new servers will be allocated. Old sessions may exist on SC some time until they expire when the client exits disorderly.

When an idling client loses all its connection to SC due to short temporarily network unavailability then the connection can be recovered, respectively re-established. When the breakdown lasts longer than the echo message interval, the current operation will fail and signalled to the application. Client subscribed to a publishing server has always a busy connection. In such case the receipt of the messages will fail immediately. The SC will take notice and clean up the subscription.

3.5.2 Server

When server aborts its activity abruptly (without a neat deregister), then SC will detect the connection breakdown immediately (on the connection on which the server registers) and will clean up all its sessions. Subsequent client messages for the deleted sessions will return “Invalid Session ID”.

After server restart, new connections to and from SC will be established. The server can then be allocated to the sessions.

3.5.3 SC

When SC aborts its activity abruptly, client will detect the connection breakdown when a new message (keepalive echo or other) is sent. It can perform session cleanup followed by a reconnect.
Server will detect the connection breakdown immediately (on the connection on which the server registers) and can perform a cleanup followed by a reconnect.

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

After SC restart, new connections will be established. The servers should register prior to any client sessions of subscriptions. Otherwise the client gets message “no free server available” or “server not available”. ~~It is acting like normal HTTP Proxy without caching.~~

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

4 Message Protocol

The Service Connector Message Protocol (SCMP) defines how the messages are transmitted. It uses a simple header – body pattern.

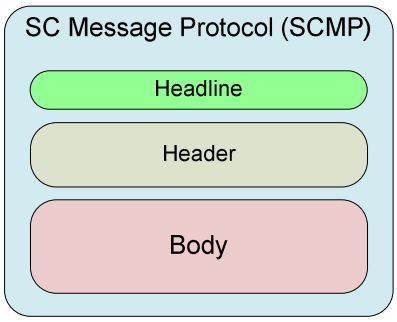
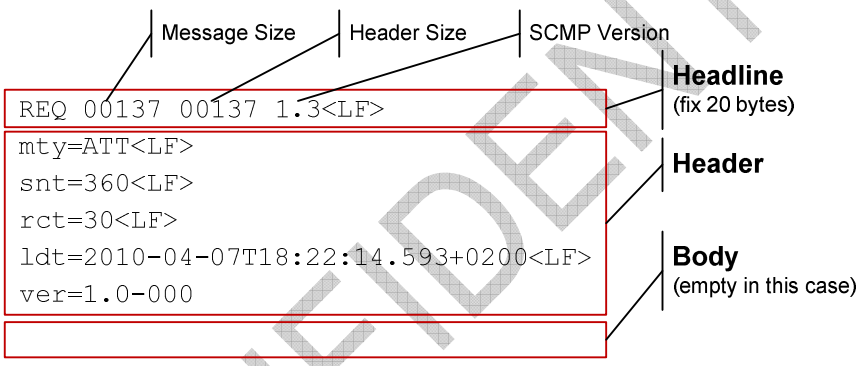


Figure 9 Service Connector Message Protocol

Wireshark example:



4.1 Headline

The fix size (22~~(20~~ bytes) headline defines the header key, the total size of the message, size of the header and the SCMP version. It is encoded in ISO-8859-1 (Latin 1) and terminated by <LF>.

HeaderKey The header key defines the purpose of the message and can be:

- REQ – Request from client or server to SC or request from SC to server
- RES – Response from server to SC or SC to client or to server
- PRQ – Large request part from client or server to SC or part request from SC to server
- PRS – Large response part from server to SC or SC to client
- KRQ – Keepalive request
- KRS – Keepalive responseEXC – Exception returned after REQ or PRQ in case of an error

Message size The complete size of the message in bytes counted from the beginning of the header until the end of the message body. The number has leading zeros.

Header Size The size of the message header in bytes counted from the beginning of the header until the end of the message header. The number has leading zeros.

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

Version

The SCMP version is the version of the protocol specification to which this message adheres. It has fix the format 9.9 and it ensures that the receiver knows how this message is structured. The version number (e.g. 1.3) means: 1 = Release number, 3 = Version number.
The receiver may implement multiple protocol versions, thus "understand" older versions. The following matching rule~~s~~ applies:

- Message: 1.0 + receiver implements: 1.0 => compatible
- Message: 1.0 + receiver implements: 1.1 => compatible
- Message: 1.3 + receiver implements: 1.0 => not compatible
  (message may have new headers unknown to the receiver)
- Message: 1.4 + receiver implements: 2.0 => not compatible
  (old message structure and possibly not understood here)
- Message: 2.0+ receiver implements: 1.8 => not compatible
  (new message and surely not understood here)

4.2 Header

Message header has variable length and contains attributes of variable number and length. Each attribute is on a separate line e.g. delimited by <LF>. Attributes and values are encoded in ISO-8859-1 (Latin 1) character set. The sequence order of the attributes is meaningless.

4.3 Body

The message body has variable length and contains binary data or ISO-8859-1 (Latin 1) encoded text. The attribute *bodyType* defines the format. It is under control of the applications. When compression is enabled, body is ZIP-compressed during transmission.

4.4 SCMP over TCP/IP

For direct transport over TCP/IP the headline, messages header and the body is directly written to the network connection.

4.5 SCMP over HTTP

For transport over HTTP the headline and messages header have content type **text/plain** and the message body the content type **application/octet-stream**.
The request message uses method POST, the response is regular HTTP response.

In order to distinguish regular (plain) HTTP traffic from SCMP over HTTP, the following HTTP headers are used for request and response:

```
Pragma: SCMP
Cache-Control: no-cache
```

Actually chunked transfer encoding and pipelining are not used.

Wireshark example:

```
POST / HTTP/1.1
Content-Length: 178
Content-Type: text/plain
Host: 192.234.123.33
Pragma: SCMP
Cache-Control: no-cache

REQ 00000081 00081 1.3
mty=ATT
kpt=10snt=360
rct=30
ldt=2010-04-07T18:22:14.593+0200

HTTP/1.1 200 OK
Content-Length: 74
```

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

```
Content-Type: text/plain
Pragma: SCMP
Cache-Control: no-cache

RES 00000041 00041 1.3
mty=ATT
ldt=2010-04-07T18:22:14.593+0200
```

~~4.6 HTTP over SCMP~~

~~The flexible SC topology allows placement of multiple SC Proxies on the path between the client and the server. Therefore HTTP may pass a network section configured as TCP/IP. In such section HTTP over SCMP is used. The traffic is transferred as regular messages with bodyType = http. The maximal body size limit of 64kB does not apply for HTTP over SCMP~~

~~Wireshark example:~~

```
REQ 00071 00017 1.3
mty=HTT
bty=http
GET /wiki/Main_Page HTTP/1.1
Host: en.wikipedia.org

RES 59448 00017 1.3
mty=HTT
bty=http
HTTP/1.0 200 OK
Content-Length: 74
Content-Type: text/html
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" dir="ltr">
<head>
<title>Main Page - Wikipedia, the free encyclopedia</title>
...
```

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

5 Semantic

The sequence of the messages exchanged between the components is shown in the following diagrams.

5.1 Session Service

The following schema shows message exchange with single threaded session server.

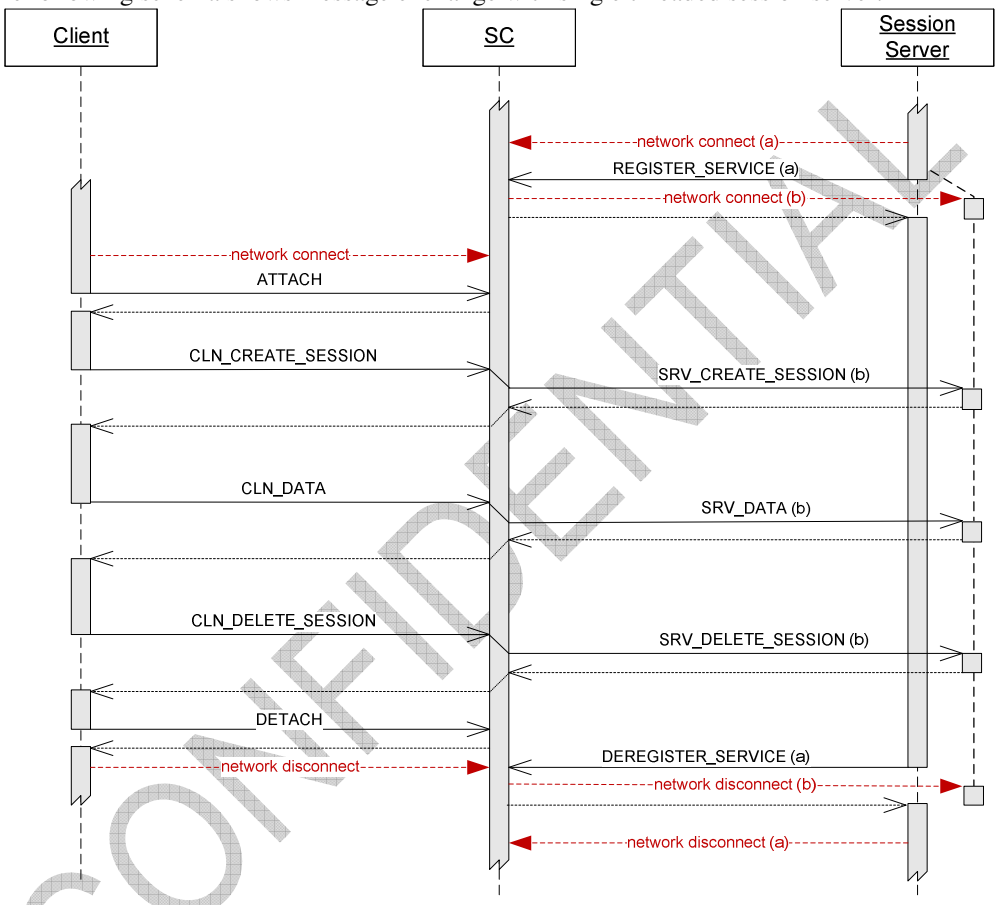


Figure 10 Synchronous Message Exchange.

Client

1. The client establishes a network connection to SC and starts communication with the ATTACH message. Keepalive~~KEEPALIVE~~ messages can be sent on this connection.
2. Then it starts a session with a service with the CLN_CREATE_SESSION message
1. The SC allocates a server providing this service and notifies it about the session start with the SRV_CREATE_SESSION message. It also creates a unique sessionId for this session. If there is no free server instance available to this service, the client gets an error “no free server available”.
3. Then the client can exchange messages with the server via CLN_DATA messages.
4. When the session with this service is no longer needed, it will be deleted with the CLN_DELETE_SESSION message. The server is notified with the SRV_DELETE_SESSION message.
5. Before the client terminates, it should send DETACH message and then terminate the network connection to SC.

When session is abnormally terminated, the client is notified and will receive and error message. The reasons for this can be:

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

- Server sends DEREGISTER_SERVICE or DETACH message
- Unexpected server exit ~~(e.g. keepalive timeout expiration)~~
- Expiration of the session timeoutUnderlying communication error (e.g. unreachable node)~~keepalive timeout expiration)~~

Note **The client may have multiple SCs connected at the same time. Per connected SC the client may have multiple active sessions at the same time. For each particular session only one request may be pending at any time.**

Server

1. The server establishes a network connection (a) to SC and starts communication and registers itself as an instance of a service with the REGISTER_SERVICE message. Keepalive~~KEEPALIVE~~ messages can be sent on this connection. At that time it should have a listener that will accept the connection (b) initiated by the SC to this server.
2. The SC registers the server instance and will create network connection (b) back to it. Keepalive~~No KEEPALIVE~~ messages will also~~can~~ be sent on this connection, depending on the *keepaliveInterval* set in REGISTER_SERVICE.~~connection!~~
3. When a client creates a session the server is notified with the SRV_CREATE_SESSION message. The message contains additional information about the client and the sessionId. The server can accept or reject the session.
4. The server receives messages from the client as SRV_DATA and sends them back after execution of the service that it implements.
5. When the client deletes the session, the appropriate server is notified with the SRV_DELETE_SESSION message.
6. When the server is no longer needed it sends the message DEREGISTER_SERVICE. From this point the SC will not allocate it for a session and terminates the connection (b) to it. Then it can terminate the network connection (a) to SC.

When the session is abnormally terminated before, the server is notified with the SRV_ABORT_SESSION message. The reasons for this can be:

- Client sends DETACH message while it has a pending session
- Unexpected client exit ~~(e.g. keepalive timeout expiration)~~
- Expiration of the session timeoutUnderlying communication error (e.g. unreachable node)~~keepalive timeout expiration)~~

The network connection (a) must not be dropped until DEREGISTER_SERVICE message is sent! Otherwise SC will treat this as server termination and clean-up its sessions and its registration.

Note **The server must be active before the client will create a session. Otherwise the client will receive an error message. ~~The server may have only one SCs connected at the same time.~~ The server instance may serve single or multiple sessions at the same time as described later. Single session server may have only one SCs connected at the same time. For each particular session only one request may be pending at any time.**

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

5.1.1 Asynchronous Message Exchange

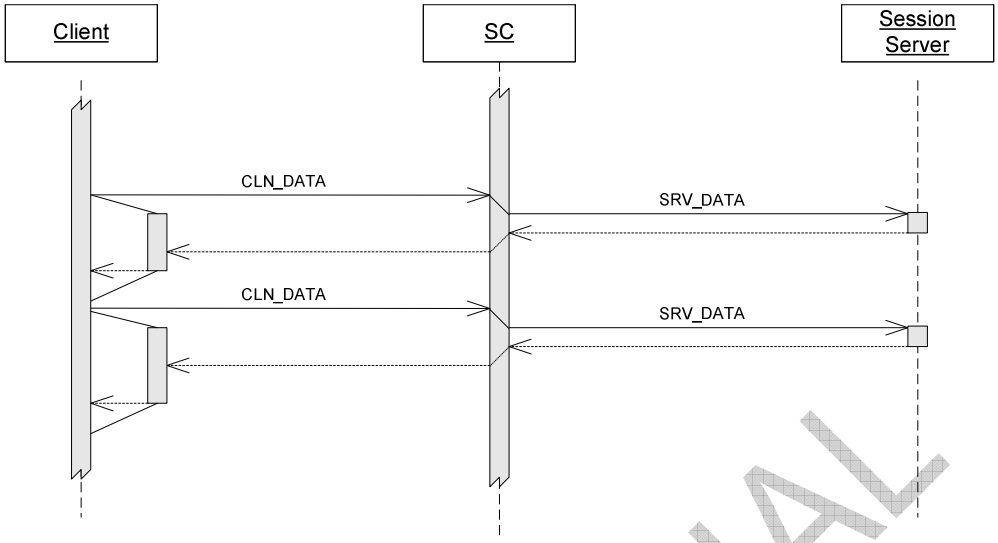


Figure 11 Asynchronous Session Service Message Exchange.

Fully asynchronous message is not possible because the server execution is always synchronous. For this reasons only the receipt of the server response can be asynchronous.

1. The client sends a CLN_DATA message and declares a notification method that will receive the response. It then can continue processing
2. When the response arrives, the notification method is invoked and can process it.

Note! **Only one request may be pending at any time. Subsequent request will block until the response for the previous message arrives.**

5.1.2 Large Messages

Regular request / response messages have a REQ / RES headerKey in the head line. Large messages are broken into parts with its own headerKey PRQ (part request) and PRS part response) see 4.1.

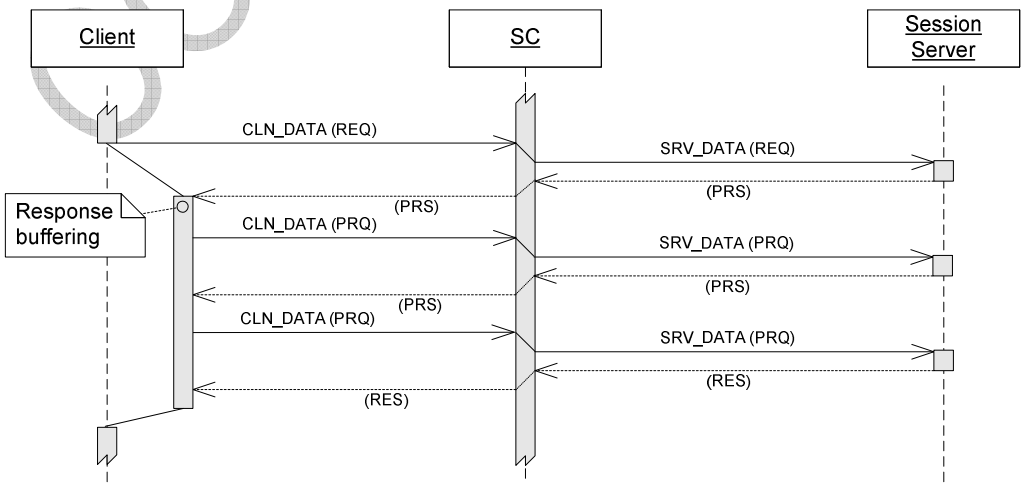


Figure 12 Large Response.

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

1. The client sends a regular request to the service.
2. The server receives the request messages and start producing the response.
3. When it reaches the max allowed length (60kB) it send the message part (PRS) and waits for the next part (PRQ)
4. At the end the server sends the last message part as a regular response (RES)
5. The message parts are buffered on the client side
6. When the final response arrives, the message is made available to the client.

In order to put together all message parts the server must allocate a unique partId and use it for all parts of one message.

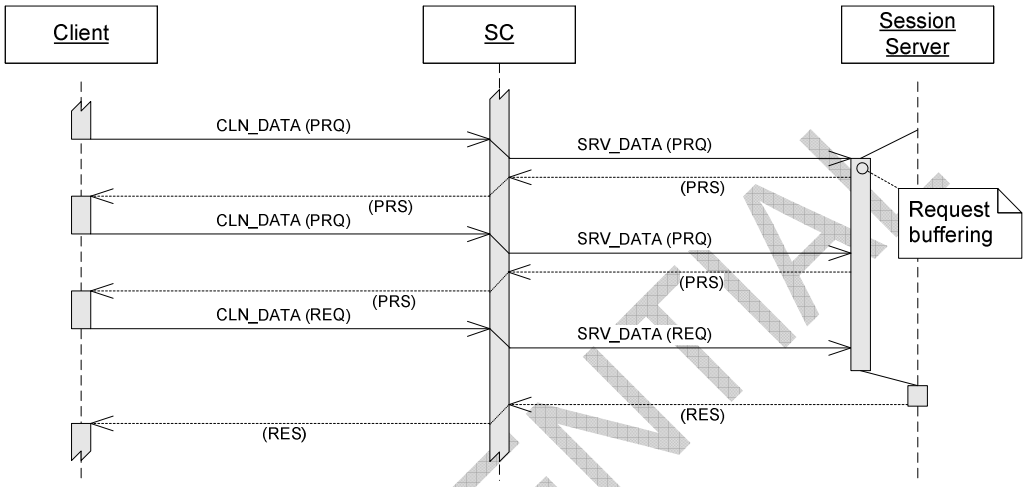


Figure 13 Large Request.

1. The client collects the request data and when it reaches the max allowed length (60kB) it sends the message part (PRQ) to the service.
2. The message part transported to the server and buffered here
3. When the final message part (REQ) arrives, the complete is made available to the server.
4. This will process the message and send back the response message.

Combination of large request and large response is possible.

For large messages the messageId contains additional counter called part sequence number. This allows putting ~~together~~ all message parts together. Message traffic with large request followed by a large response looks like (simplified):

```
REQ ..   mid=3
RES ..   mid=64
...
PRQ ..   mid=4/1
PRS ..   mid=65/1
PRQ ..   mid=4/2
PRS ..   mid=65/2
PRQ ..   mid=4/3
PRS ..   mid=65/3
REQ ..   mid=4/4
PRS ..   mid=66/1
PRQ ..   mid=5/1
PRS ..   mid=66/2
PRQ ..   mid=5/2
RES ..   mid=66/3
...
REQ ..   mid=6
RES ..   mid=67
```

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

5.1.3 Single Session Server

Single-session server registers itself for one service and may serve only one session at the same time. It must define *maxSession = 1* and *immediateConnect* = true. The required parallelism is reached by starting multiple instances of the same server. The SC keeps track of the registered servers and allocates / de-allocates sessions to them.

5.1.4 Multi Connection Server

In opposite to single session server, multi connection server may serve multiple sessions at the same time. It uses individual connection for each session. The server registers itself for one or more services and defines reasonable high *maxSession* > 1 and *immediateConnect* = true/ false. The connections are created by SC immediately after the service was registered or when the session is started depending on the *immediateConnect* flag. It is terminated after the service is deregistered, or after the session is deleted.

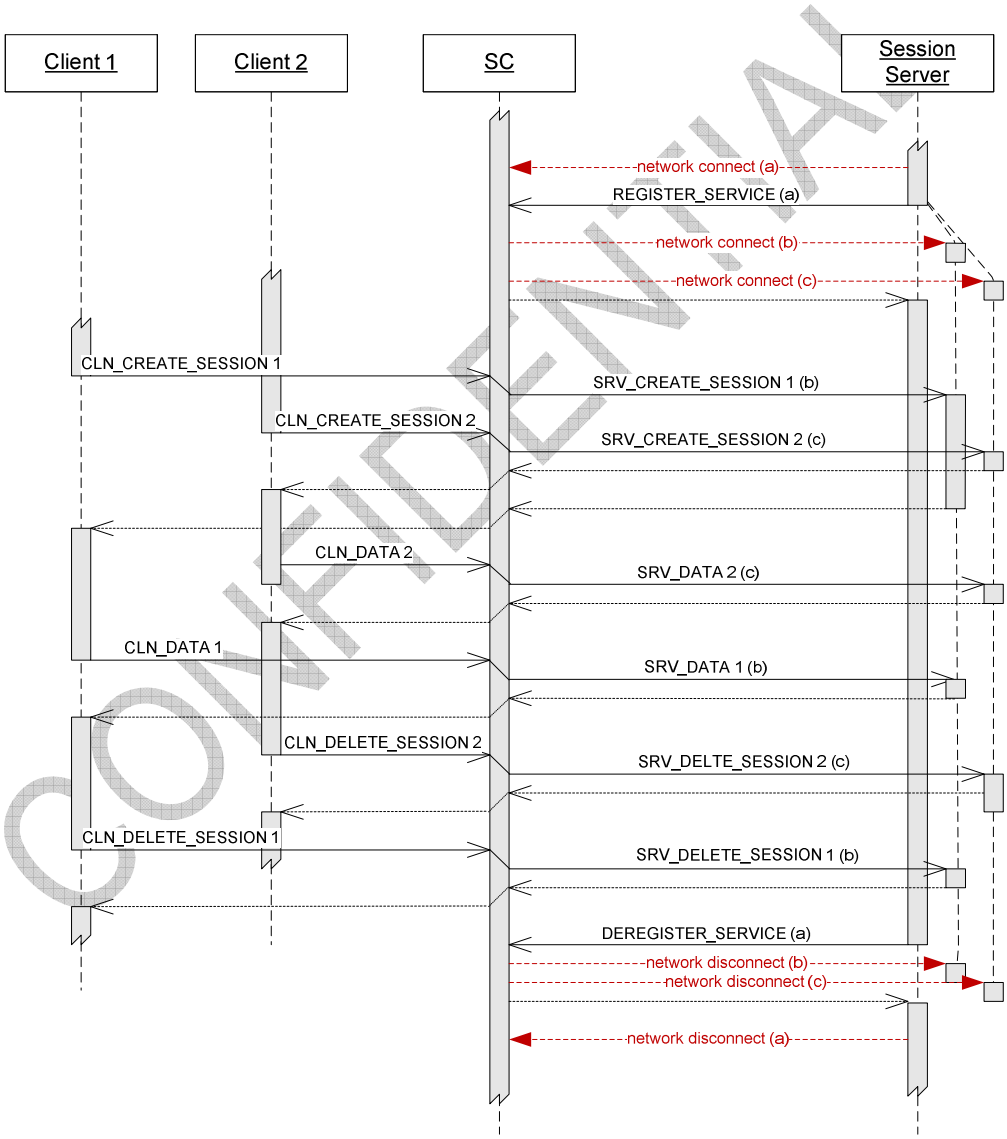


Figure 14 Multi-Connection server (immediateConnect = true).

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

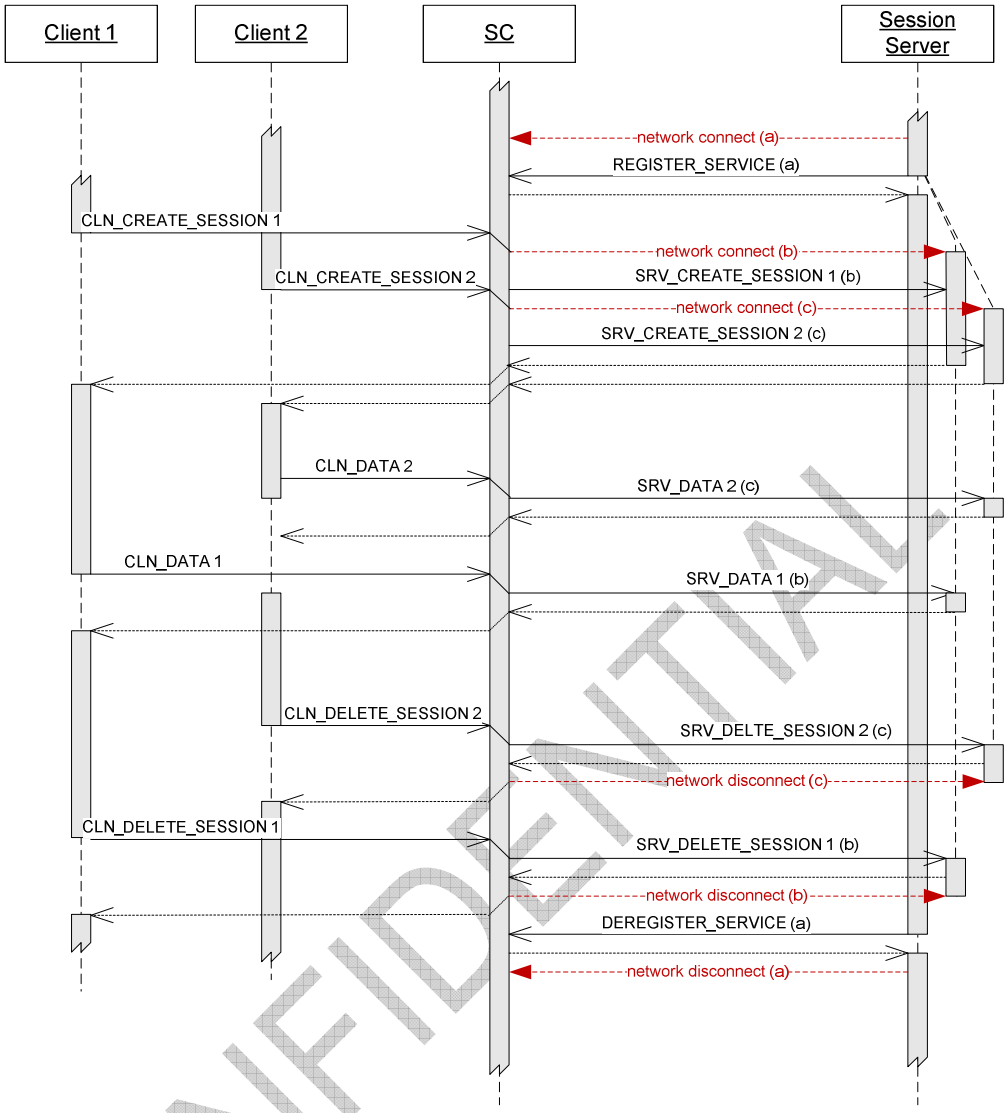


Figure 15 Multi-Connection server (immediateConnect = false).

Multi-Connection server receives SC requests on the network connection that is allocated to the particular session. It may use any available technique (e.g. multithreading), but must ensure that all requests are processed in parallel.

The network connection (a) must not be dropped until DETACH message is sent! Otherwise SC will treat this as server termination and clean-up all its sessions and registration.

5.1.5 Application Server (Tomcat)

SCMP Messaging with an application server (e.g. Tomcat) utilizes the HTTP protocol and works exactly like a multi-connection server. The server must register itself for at least one service. It can register for multiple services! It must define reasonable high *maxSession* and *immediateConnect* = false.

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

5.2 Publishing Service

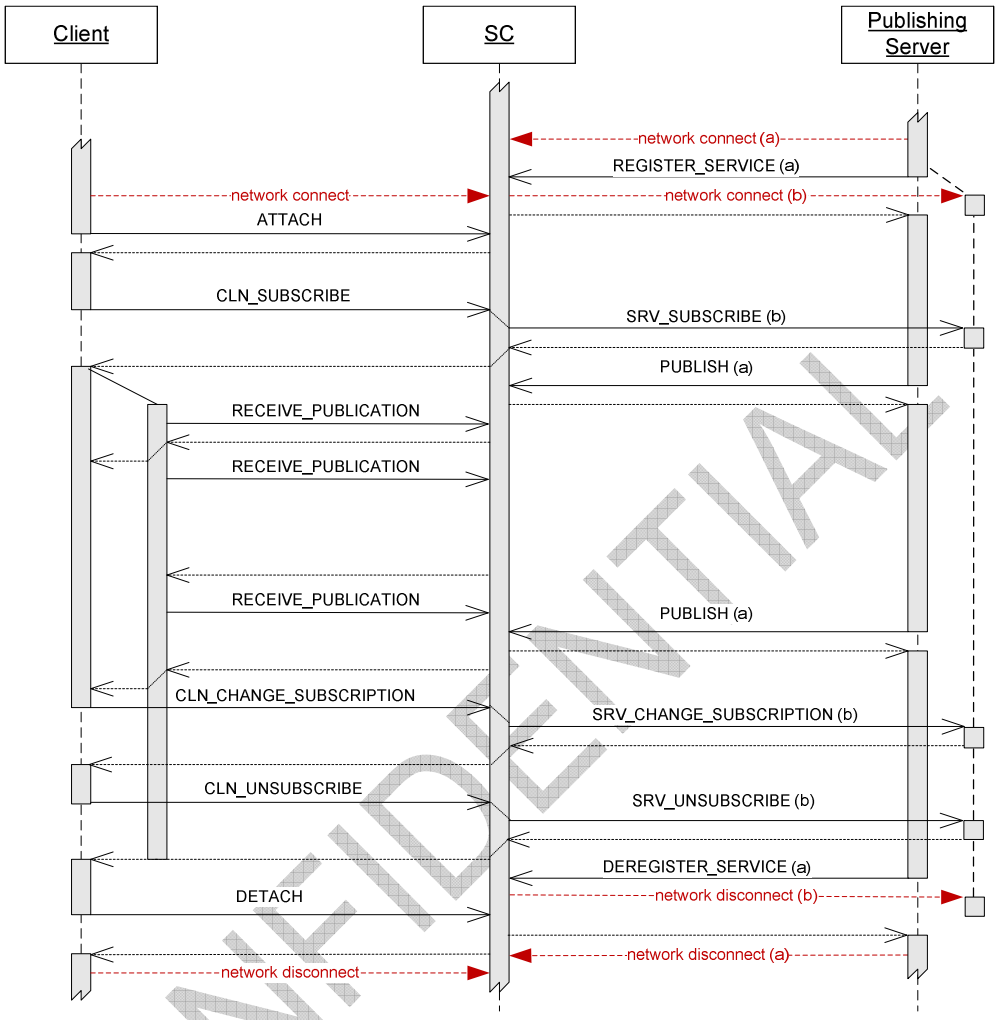


Figure 16 Publishing Service

Client

2. The client establishes a network connection to SC and starts communication with the ATTACH message. Keepalive messages can be sent on~~On~~ this connection. ~~KEEPALIVE message can be sent.~~
3. Then it subscribes to a service with the CLN_SUBSCRIBE message and starts a listener that will receive the incoming messages.
4. The SC remembers the subscription and also creates a unique ~~subscriptionID (~~sessionId~~)~~ for it. It also notifies the server registered to this service with the SRV_SUBSCRIBE message. If there is no server, the client gets an error.
5. When a message is published, SC compares the message mask with the subscription mask and based on the matching result delivers the message to the client. The client receives and processes the message and initiates the next receipt with the RECEIVE_PUBLICATION message.
6. When no message is published within a period of time (defined by *noDataInterval*)~~*senderTimeout*)~~ then SC sends an empty message to the client and this initiates the next receipt with the RECEIVE_PUBLICATION message.
7. The client can change the publication mask with the CLN_CHANGE_SUBSCRIPTION message or terminate the subscription with CLN_UNSUBSCRIBE message. In both cases the server is notified with the SRV_CHANGE_SUBSCRIPTION~~SRV_CHANGE_SUBSCRIBTION~~ or

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

SRV_UNSUBSCRIBE message. The client should ignore errors resulting from the unavailability of the server when sending CLN_UNSUBSCRIBE.

8. Before the client terminates, it should send DETACH message and then terminate the network connection to SC.

When the client terminates abnormally, the SC will clear its subscription, discard all messages not delivered yet and notify the server with the SRV_UNSUBSCRIBE message. The reasons for this can be:

- Client sends DETACH message
- Unexpected client exit ~~(e.g. keepalive timeout expiration)~~
- Underlying communication error (e.g. unreachable node)~~keepalive timeout expiration)~~

Note **The client may have multiple SCs connected at the same time. Per connected SC the client may have multiple subscriptions to different services at the same time. For each subscription only one receipt request may be pending at any time.**

Server

1. The server establishes a network connection to SC and starts communication and registers itself as an instance of a service with the REGISTER_SERVICE message. Keepalive~~On this connection KEEPALIVE~~ messages can be sent on this connection.~~.~~
2. The SC registers the server instance and will create network connection (b) back to it. Keepalive~~No KEEPALIVE~~ messages will also~~can~~ be sent on this connection, depending on the *keepaliveInterval* set in REGISTER_SERVICE.~~connection!~~
3. When a client subscribes or changes the subscription the server is notified with the SRV_SUBSCRIBE or SRV_CHANGE_SUBSCRIPTION message. The message contains the subscription mask and additional information about the client. The server can accept or reject the subscription or its change. In opposite to session services the server instance is not allocated for the session, but just processes the notification.
4. Now the server can publish messages to the service. SC immediately responds when the PUBLISH message has been queued. The server does not wait for message delivery to the clients. The published message must have a mask designating its contents.
5. The SC compares the mask with the subscription mask of the clients and delivers the message to them. Messages that do not match any subscription are discarded. The server does not know how many clients did get the message or if any at all.
6. Messages are delivered in the order of their publishing. E.g. in order SC receives them. For this reason they are queued within SC.
7. When the client unsubscribes, the server is notified with the SRV_UNSUBSCRIBE message.
8. When the server is no longer needed it sends the message DEREGISTER_SERVICE. Then it can terminate the network connection (a) to SC.

When the client terminates abnormally, the server is notified with the SRV_UNSUBSCRIBE message. In cascaded SC topology the server is notified with the SRV_CHANGE_SUBSCRIPTION instead of the SRV_UNSUBSCRIBE message. This is because of the fan-out within SC. The reasons for this can be:

- Client sends DETACH message while it has a pending subscription
- Unexpected client exit ~~(e.g. keepalive timeout expiration)~~
- Underlying communication error (e.g. unreachable node)~~keepalive timeout expiration)~~

Note **The server must be active before the client will create the subscription. Otherwise the client will receive an error message.** When the server terminates timely before the client, the client should ignore the error resulting from the unavailability of the server.

Multiple publishing servers may register to the same service. Also like a session server multiple sessions per server are allowed. SC chooses one server instance which is not busy when a notification must be processed. Unlike a session server the chosen server instance is allocated only for the time of the notification processing (one request).

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

5.2.1 Large Published Message

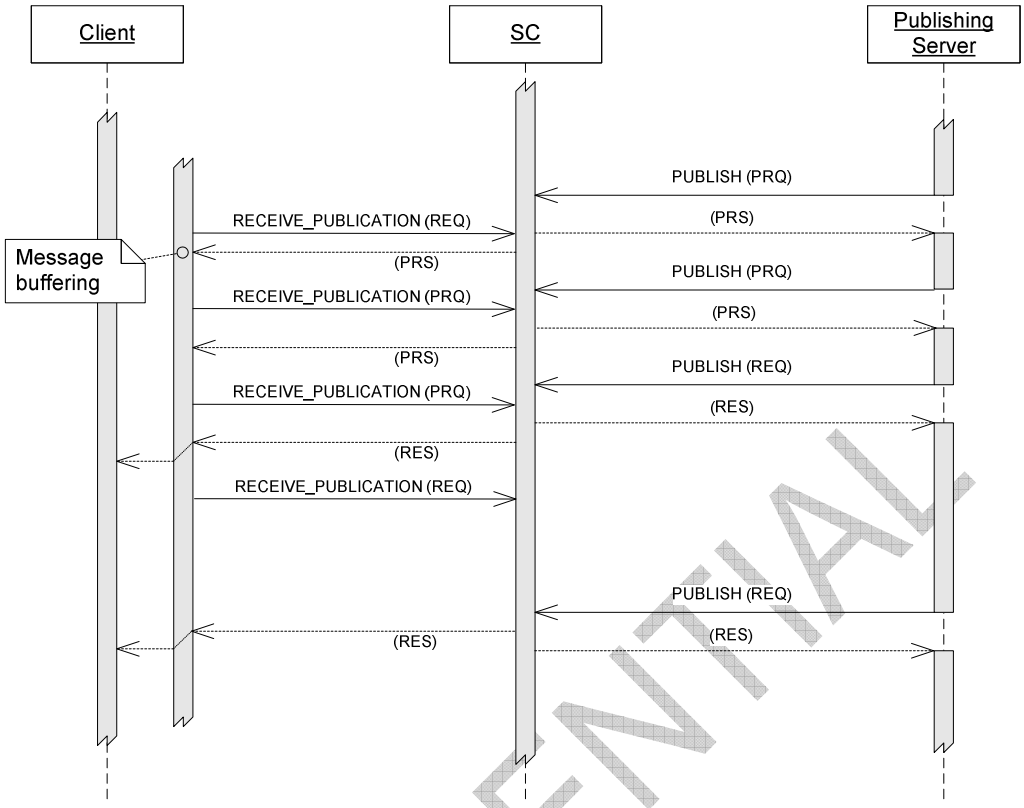


Figure 17 Large Published Message

Publishing of large messages works like sending a large request. The parts are passed through SC and buffered on the client.

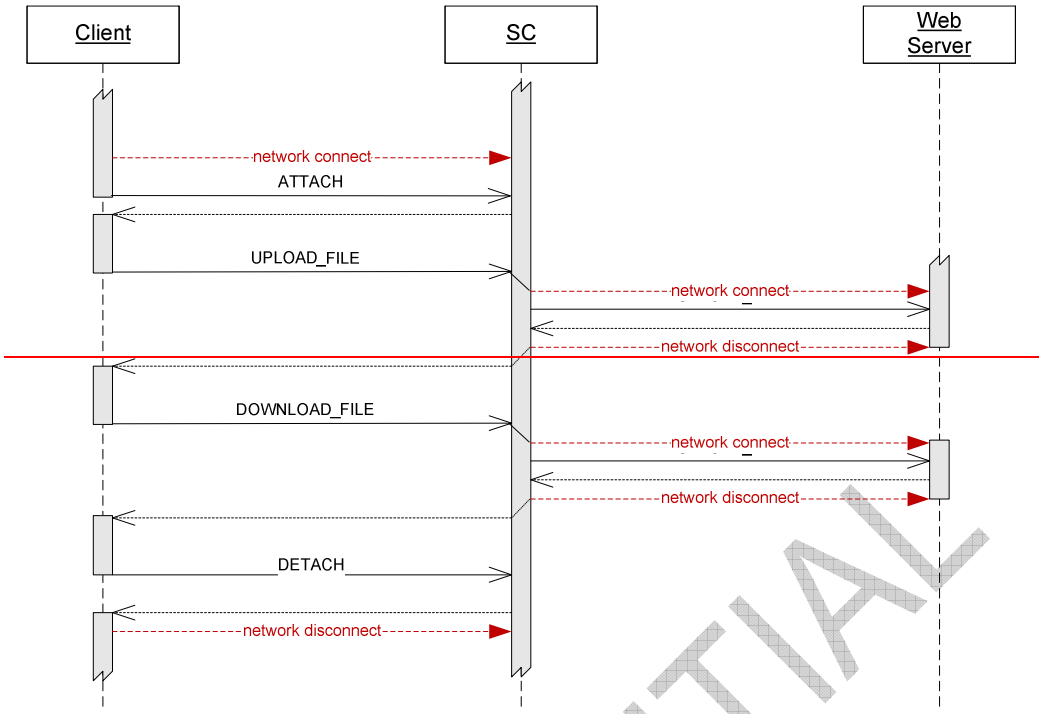
5.3 File Service

This SC service provides API for these file operations:

- Download file from the web server to the client.
- Upload file from the client to the web server.
- List files in a file repository on the web server.

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG



~~**Figure 16 File upload and download.**~~

~~The client initiates the upload or download of the file. No session is required for the transfer.~~ The SC configuration maps a service name to a directory on ~~virtual host defined in~~ the web server (virtual host). The client initiates the upload or download of the file for a service. Session context is not required for the file transfer. ~~–~~In this way the client may upload or download file in different server locations. Directory structures (tree) are not supported.

List of files is provided as *tbd.*

The Web Server is not registered to the service. It is configured to allow file upload, download and directory browsing for the specific directories (virtual hosts).

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

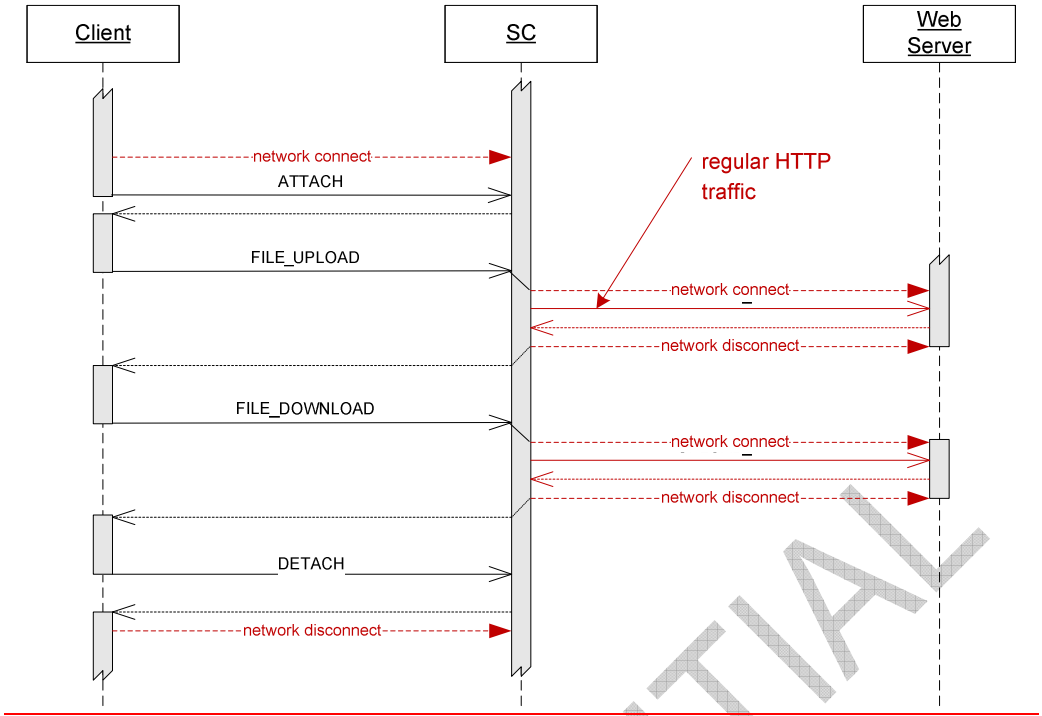


Figure 18 File upload and download.

The network connections are dynamically created form SC to the server when they are needed. Multiple HTTP requests can be pending at the same time, each one using one network connection. The limitation of 64kB for SCMP messages does not apply for traffic to and from the Web Server. Cascaded SCs on the path to the web server are transparent for the client.

5.4 HTTP Proxy~~Redirection~~ Service

~~Redirection of~~ HTTP traffic through the SC is possible without a service and session context. SC receives the http requests on a dedicated port~~previous messaging though the SC. SC works like a HTTP proxy~~ and passes all HTTP traffic to the configured server. It acts like a HTTP proxy. The requested url must be resolved (dns) by the underlying network infrastructure. SC does not provide any name resolution.

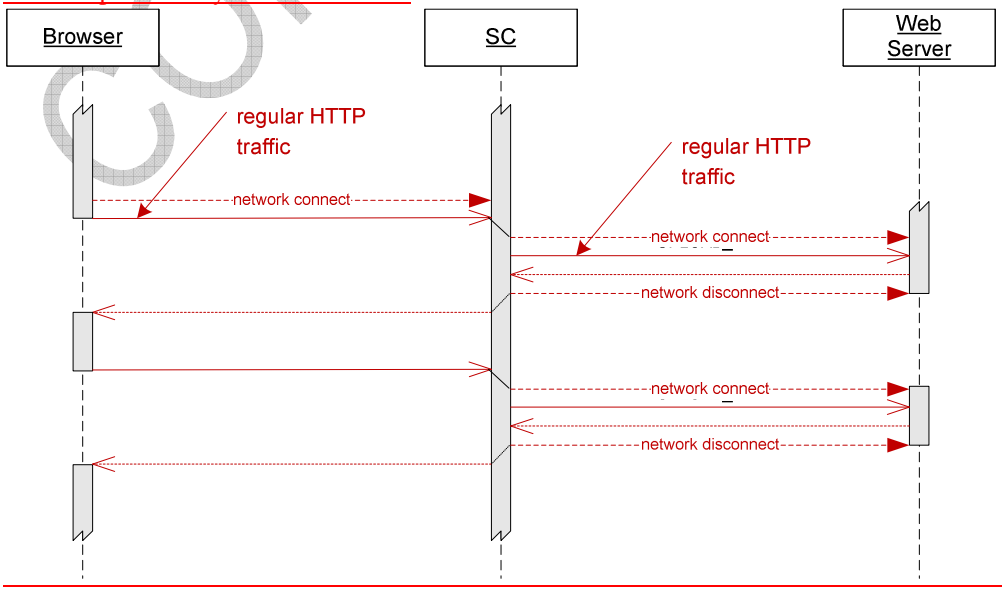


Figure 19 HTTP proxy

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

The Web Server is~~does~~ not registered to any service. The~~Instead~~ SC ~~has service~~ configuration has one destination (node + port) for~~that allows~~ redirection of the plain HTTP traffic. ~~to the configured node and port.~~ The network connections are dynamically created form SC to the server when they are needed. Multiple HTTP requests can be pending at the same time, each one using one network connection.

The limitation of 64kB for SCMP messages does not apply for traffic to and from Web Server.

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

6 SCMP Messages

Server may play the role of a client and consume other services. In such configuration message which belong to the client and to the server must have different types. For this reason messages initiated by the client have CLN_ prefix and messages sent to the server the SRV_ prefix.

6.1 Keepalive

Keepalive messages are sent in regular intervals on all idle connections initiated by a network peer. The only purpose of keepalive messages is to preserve the connection state in the firewall placed between the communicating peers and resets its internal timeout. See also Chapter 3.2

Using of keepalive messages can be disabled with the *keepaliveInterval (kpi)* attribute. The message has only a headline and no attributes and no body. The format is:

KRQ 0000000 00000 1.3

for request and

KRS 0000000 00000 1.3

~~6.1~~6.2 for response.ATTACH (ATT)

This message is sent from the client to SC in order to initiate the communication. The message has no body and contains these attributes:

mty=ATT
~~mid=974834~~
ver=1.0-023
ldt=1997-07-16T19:20:30.064+0100
kpi=360~~rct=10~~
~~snt=60~~

SC receives the message~~, starts monitoring the connection based on keep alive values~~ and sends back the response:

mty=ATT
~~mid=974834~~
ldt=1997-07-16T19:20:34.044+0200

When an SC error occurs the response message contains the attributes:

mty=ATT
~~mid=974834~~
ldt=1997-07-16T19:20:30.453+0100
sec=3000
set=SCMP version mismatch (Received=1.0-23, Required 1.1.-34)

~~6.2~~6.3 DETACH (DET)

This message is sent from the client to SC in order to terminate the communication. The message has no body and contains these attributes:

mty=DET
~~mid=974834~~

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

SC receives the message, stops monitoring of connection based on keep alive values and sends back the response:

mty=DET
~~mid=974834~~

~~6.3 KEEPALIVE (KPL)~~

~~This message is sent from the client to SC or from server to SC in order to verify the communication. The message has no body and contains these attributes:~~

~~mty=KPL~~
~~mid=974834~~

~~The sender of the keep alive message starts a timer that monitors the arrival of the response message. In case the timeout expires the connection must be aborted and cleaned up. The receiver of the keep alive message monitors the interval in which these messages arrive. In case the message does not arrive in the pre defined interval, the connection must be aborted and cleaned up.~~

~~SC receives the message, and sends back the response:~~

~~mty=KPL~~
~~mid=974834~~

6.4 INSPECT (INS)

This message is sent from the client to SC in order to get internal information from the SC. The message has body of type *text* and contains these attributes:

mty=INS
bty=txt
~~mid=974834~~

The body content and its processing will be described at later project stage.

The message returned by SC has a body of type *text* and contains these attributes:

mty=INS
bty=txt
~~mid=974834~~

6.5 MANAGE (MGT)

This message is sent from the client to SC in order to change the SC behaviour. The message has body of type *text* and contains these attributes:

mty=MGT
bty=txt
~~mid=974834~~

The body content and its processing will be described at later project stage.
This message will be used to enable or disable client access to services.

The message returned by SC has a body of type *text* and contains these attributes:

mty=MGT
bty=txt
~~mid=974834~~

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

6.6 CLN_CREATE_SESSION (CCS)

This message is sent from the client to SC in order to create~~start~~ a new session for a service. The message has no body and contains these attributes:

mty=CCS
mid=974834
nam=P01_RTXS_RPRWS1
ipl=10.0.4.32/10.0.4.32/10.2.54.12~~/10.2.54.12~~
sin=SNBZHP - TradingClientGUI 10.2.7
eci=300
ect=10

SC receives the message and does these actions:

1. Generates a unique session id
2. Chooses a free server instance from the list of available servers serving the requested service.
3. Allocates the server instance to this session
4. Sends the message SRV_CREATE_SESSION to the allocated server and awaits the server response.
5. If the response message does not contain the attribute rejectFlag, the SC keeps the session and sends back to client the message with the following attributes:

   mty=CCS
   mid=974834
   nam=P01_RTXS_RPRWS1
   sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d

6. If the response message contains the attribute rejectFlag, the SC deletes the session, de-allocates the server and sends back to client the message with the following attributes:

   mty=CCS
   mid=974834
   nam=P01_RTXS_RPRWS1
   rej
   aec=4334591
   aet=%RTXS-E-NOPARTICIPANT, Authorization error – Unknown participant

When an SC error occurs the response message contains the attributes:

mty=CCS
mid=974834
sec=3000
set=Unkown service: P01_RTXS_RPRWS3

If SC cannot allocate a free server instance for the session it will respond with the error set=No free server available for service: P01_RTXS_RPRWS3

6.7 SRV_CREATE_SESSION (SCS)

This message is sent from the SC to the server when a~~the~~ server instance has been be allocated to a session. The message has no body and contains these attributes:

mty=SCS
mid=974834
nam=P01_RTXS_RPRWS1
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
sin=SNBZHP - TradingClientGUI 10.2.7
ipl=10.0.4.32/10.0.4.32/10.2.54.12~~/10.2.54.12~~
eci=300
ect=10

The server receives the message and must decide to accept or reject this request. If it accepts, then it must return a message with the following attributes:

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

mty=SCS
mid=974834
nam=P01_RTXS_RPRWS1
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d

If it rejects the session, then it must return a message with the following attributes:

mty=SCS
mid=974834
nam=P01_RTXS_RPRWS1
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
rej
aec=4334591
aet=%RTXS-E-NOPARTICIPANT, Authorization error – Unknown participant

6.8 The *aec* / *aet* attributes should contain readable information describing the rejection reason.CLN_DELETE_SESSION (CDS)

This message CLN_DELETE_SESSION is sent from the client to SC in order to terminate~~close~~ an existing session. The message has no body and contains these attributes:

mty=CDS
mid=974834
nam=P01_RTXS_RPRWS1
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d

SC receives the message and does these actions:

1. Finds the server allocated to this session
2. Sends the message SRV_DELETE_SESSION to the allocated sever and awaits its response.
3. De-allocates the server instance from this session
4. Sends back the message CLN_DELETE_SESSION with the following attributes:

   mty=CSD
   mid=974834
   nam=P01_RTXS_RPRWS1
   sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d

Due to timing issues the client may send a delete session request to a non existing session or to session that has no allocated server. The SC must handle such situation and do all appropriate clean-up actions.

When an SC error occurs the response message contains the attributes:

mty=CDS
mid=974834
sec=3000
set=Session does not exist

6.9 SRV_DELETE_SESSION (SDS)

This message is sent from the SC to the server when the session will be deleted by the client and the server instance will no longer be bound to it. The message has no body and contains these attributes:

mty=SDS
mid=974834
nam=P01_RTXS_RPRWS1
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d

The server must return a message with the following attributes:

mty=SDS

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

mid=974834
nam=P01_RTXS_RPRWS1
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d

After this message the server will not receive any data requests until the next session is started.

6.10 SRV_ABORT_SESSION (SAS)

This message is sent from the SC to the server when the session is aborted due to errors or other unexpected event.~~events.~~ The message has no body and contains these attributes:

mty=SAS
mid=974834
nam=P01_RTXS_RPRWS1
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d

The server must return a message with the following attributes:

mty=SAS
mid=974834
nam=P01_RTXS_RPRWS1
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d

After this message the server will not receive any data requests until the next session is started.

6.11 REGISTER_SERVICE (REG)

This message is sent from the server instance to SC in order to tell the SC which service it serves. The message has no body and contains these attributes:

mty=REG
~~mid=974834~~
nam=P01_RTXS_RPRWS1
mxs=10
imc
pnr=9100
ver=1.0-023
ldt=1997-07-16T19:20:30.064+0100
kpi=360~~rct=10~~
~~snt=60~~
~~srq=10.4.20.222:563~~

SC receives the message and does these actions:

1. Registers the server for this service.
2. starts monitoring the connection based on keep alive values
3. Creates the requested number of connection to the server on port that was specified.
4. Sends back a message with the following attributes:

   mty=REG
   ~~mid=974834~~
   nam=P01_RTXS_RPRWS1
   ldt=1997-07-16T19:20:30.064+0100

When an SC error occurs the response message contains the attributes:

mty=RE
~~mid=974834~~
sec=3000
set=Service name=P01_RTXS_RPRWS5 not found

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

6.12 DEREGISTER_SERVICE (DRG)

This message is sent from the server instance to SC in order to tell the SC that the server will no longer provide the service. The message has no body and contains these attributes:

mty=DRG
~~mid=974834~~
nam=P01_RTXS_RPRWS1

SC receives the message and does these actions:

1. Finds the server and performs a cleanup by aborting and de-allocation all sessions of this server. If the server has allocated sessions the SC will first send the SRV_ABORT_SESSION to it.
2. Terminates all connections that have been established from SC to this server.
3. Sends back message with the following attributes:

   mty=DRG
   ~~mid=974834~~
   nam=P01_RTXS_RPRWS1

When an SC error occurs the response message contains the attributes:

mty=DRG
~~mid=974834~~
sec=3000
set=Server is not registered

After this message the server may close disconnect from the SC.

6.13 CLN_DATA (CDA)

This message is sent from the client to SC in order exchange information with the allocated server. The client may send this message only in scope of a session. The message has a body and contains these attributes:

mty=CDA
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
nam=P01_RTXS_RPRWS1
mid=974833
min=SECURITY_MARKET_QUERY

Optionally these attributes can also be set when the client wants to fetch the message from the SC cache:

cid=CBCD_SECURITY_MARKET
ced=1997-08-16T19:20:34.237+0200

SC receives the message and finds the server allocated to this session.
It sends the message SRV_DATA to the server it and awaits the response. Then it sends back a message with a body and the following attributes:

mty=CDA
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
nam=P01_RTXS_RPRWS1
mid=974834
min=SECURITY_MARKET_RESULT

Optionally these attributes can also be set when the server wants to store the message in the SC cache:

cid=CBCD_SECURITY_MARKET
ced=1997-08-16T17:00:00.000+0100

In case of an application error these attributes can also be set.

aec=4334591
aet=%RDB-F-NOTXT, no transaction open

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

When an SC error occurs the response message contains the attributes:

mty=CLN_DATA
sec=3000
set=Session does not exist

Large messages are supported in this context.

6.14 SRV_DATA (SDA)

This message is sent from the SC to the server allocated to this session in order to execute the request. The SC will send this message only in scope of a session. The message has a body and contains these attributes:

mty=SDA
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
nam=P01_RTXS_RPRWS1
mid=974833
min=SECURITY_MARKET_QUERY

The server receives the message extracts the body and executes the application code. It must send back a message with a body and the following attributes:

mty=SDA
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
nam=P01_RTXS_RPRWS1
mid=34834
min=SECURITY_MARKET_RESULT

Optionally these attributes can also be set when the server wants to insert the message into the SC cache:

cid=CBCD_SECURITY_MARKET
ced=1997-08-16T17:00:00.000+0100

In case of an application error these attributes can also be set.

aes=4334591
aet=%RDB-F-NOTXT, no transaction open

6.15 CLN_ECHO (CEC)

This message is sent from the client to SC and passed to the allocated server in order to verify the session consistency.~~complete message exchange through all SC components.~~ The client must~~may~~ send this message in periodic intervals~~only~~ in scope of every~~a~~ session. The message has no body ~~of any type~~ and contains these attributes:

mty=CEC
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
nam=P01_RTXS_RPRWS1
mid=974833
~~bty=text~~
crq=122.42.3.64:314

SC receives the message and finds the server allocated to this session.
It passes the message SRV_ECHO to the allocated server and awaits the response. Then it sends back a message without ~~a~~ body and the following attributes:

mty=CEC
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
nam=P01_RTXS_RPRWS1
mid=974834
~~bty=text~~
srs=10.0.3.3:31464

~~Large messages are supported in this context.~~

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

6.16 SRV_ECHO (SEC)

This message is sent from SC to the allocated server as result of the CLN_ECHO request. The message has no body ~~of any type~~ and contains these attributes:

mty=SEC
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
nam=P01_RTXS_RPRWS1
mid=974833
~~bty=txt~~
crq=10.0.3.3:3223

The server receives the message and sends back a message with no~~the same~~ body and the following attributes:

mty=SRV_ECHO
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
nam=P01_RTXS_RPRWS1
mid=554834
~~bty=txt~~
srs=143.12.3.6:884

~~Large messages are supported in this context.~~

6.17 CLN_SUBSCRIBE (CSU)

This message is sent from the client to SC in order to subscribe for a publishing service. The message has no body and contains these attributes:

mty=CSU
mid=53834
nam=P01_BCST_CH_RPRWS2
msk=000012100012832102FADF----------
ipl=10.0.4.32/10.0.4.32/10.2.54.12~~/10.2.54.12~~
sin=SNBZHP - TradingClientGUI 10.2.7
asi= cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d

SC receives the message and does these actions:

1. Generates a unique session id
2. Sends the message SRV_SUBSCRIBE to the server registered for this service and awaits the server response.
3. If the server response message does not contain the attribute rejectFlag, the SC remembers the subscription mask of the client for this service and sends back to client the message with the following attributes:
   mty=CSU
   mid=974834
   nam=P01_BCST_CH_RPRWS2
   sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
4. If the server response message contains the attribute rejectFlag, the SC deletes the session, and sends back to client the message with the following attributes:
   mty=CSU
   mid=974834
   nam=P01_BCST_CH_RPRWS2
   rej
   aec=4334591
   aet=%RTXS-E-NOPARTICIPANT, Authorization error – Unknown participant

When an SC error occurs the response message contains the attributes:

mty=CSU
mid=53834
sec=3000
set=Unkown service: P01_BCST_CH_RPRWS2

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

The subscription is synchronous operation. The client gets control when all SC components on the path to the publishing server are aware of the subscription.
If SC cannot find server registered for this service it will respond with the error set=No server available for service: P01_BCST_CH_RPRWS2.

6.18 SRV_SUBSCRIBE (SSU)

This message is sent from the SC to the server in order to process the client subscription (e.g. perform authentication). The message has no body and contains these attributes:

mty=SSU
mid=53834
nam=P01_BCST_CH_RPRWS2
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
msk=000012100012832102FADF----------
ipl=10.0.4.32/10.0.4.32/10.2.54.12~~/10.2.54.12~~
sin=SNBZHP - TradingClientGUI 10.2.7
asi= cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d

The server receives the message and must decide to accept or reject this request. If it accepts, then it must return a message with the following attributes:

mty=SSU
mid=974834
nam=P01_BCST_CH_RPRWS2
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d

If it rejects the session, then it must return a message with the following attributes:

mty=SSU
mid=974834
nam=P01_BCST_CH_RPRWS2
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
rej
aec=4334591
aet=%RTXS-E-NOPARTICIPANT, Authorization error – Unknown participant

6.19 CLN_CHANGE_SUBSCRIPTION (CHS)

This message is sent from the client to SC in order to change the subscription for a publishing service. The message has no body and contains these attributes:

mty=CHS
mid=53834
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
nam=P01_BCST_CH_RPRWS2
msk=000012100012832102FADF----------

SC receives the message and does these actions:

1. Sends the message SRV_CHANGE_SUBSCRIPTION to the server registered for this service and awaits the server response.
2. If the server response message does not contain the attribute rejectFlag, the SC changes the subscription mask of the client for this service and sends back to client the message with the following attributes:

   mty=CHS
   mid=974834
   nam=P01_BCST_CH_RPRWS2
   sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d

3. If the server response message contains the attribute rejectFlag, the SC keeps the previous subscription and sends back to client the message with the following attributes:

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

mty=CHS
mid=974834
nam=P01_BCST_CH_RPRWS2
rej
aec=4334591
aet=%RTXS-E-NOPARTICIPANT, Authorization error – Unknown participant

When an SC error occurs the response message contains the attributes:

mty=CHS
mid=53834
sec=3000
set=Client is not subscribed

The change of the subscription is synchronous operation. The client gets control when all SC components on the path to the publishing server are aware of the new subscription. If SC cannot find server registered for this service it will respond with the error set=No server available for service: P01_BCST_CH_RPRWS2.

6.20 SRV_CHANGE_SUBSCRIPTION (SHS)

This message is sent from SC to the server in order to delete the client subscription. The message has no body and contains these attributes:

mty=SHS
mid=53834
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
nam=P01_BCST_CH_RPRWS2

SC receives the message and does these actions:

1. Changes the subscription mask of the client for the service
2. Sends back a message with the following attributes:

   mty=SHS
   mid=53834
   nam=P01_RTXS_RPRWS1

When an SC error occurs the response message contains the attributes:

mty=SHS
mid=53834
sec=3000
set=Client is not subscribed

The change of the subscription is synchronous operation. The client gets control when all SC components on the path to the publishing server are aware of the new subscription.

6.21 CLN_UNSUBSCRIBE (CUN)

This message is sent from the client to SC in order to delete the subscription for a publishing service. The message has no body and contains these attributes:

mty=CUN
mid=53834
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
nam=P01_BCST_CH_RPRWS2

SC receives the message and does these actions:

1. Deletes the client subscription for the services and deletes all pending messages for this client.
2. Sends back a message with the following attributes:

   mty=CUN

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

mid=53834
nam=P01_RTXS_RPRWS1

When an SC error occurs the response message contains the attributes:

mty=CUN
mid=53834
sec=3000
set=Client is not subscribed

This operation is synchronous. The client gets control when all SC components on the path to the publishing server have deleted the subscription. If SC cannot find server registered for this service it will respond with the error set=No server registered for service: P01_BCST_CH_RPRWS2.

6.22 SRV_UNSUBSCRIBE (SUN)

This message is sent from the client to SC in order to delete the subscription for a publishing service. The message has no body and contains these attributes:

mty=SUN
mid=53834
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
nam=P01_BCST_CH_RPRWS2

The server must return a message with the following attributes:

mty=SUN
mid=974834
nam=P01_BCST_CH_RPRWS2
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d

This operation is synchronous. The client gets control when all SC components on the path to the publishing server have deleted the subscription.

6.23 RECEIVE_PUBLICATION (CRP)

This message is sent from the client to SC in order to get data published by a server. The client may send this message only in scope of a subscription session. The message has no body and contains these attributes:

mty=CRP
sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
nam=P01_BCST_CH_RPRWS2
mid=974833
noi=300

SC receives the message and does these actions:

1. Finds the client subscription
2. Creates a timer monitoring the response delivery
3. Waits until one of these two events occurs:
   a. A message that matches the client subscription arrives. Then it sends back a message with the body and the following attributes:
      mty=CRP
      sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
      nam=P01_BCST_CH_RPRWS2
      mid=974834
      moi=533min=CH_AUCTION
      msk=%%%%%%%%%%%%%%%%%%%%%%%%%%X%%%%%%%%%%%%%%%%%%%%%
   b. The *noDataInterval (noi)* timeout expires. Then it sends back a message with the no body and the following attributes:
      mty=CRP

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d
nam=P01_BCST_CH_RPRWS2
mid=974834
nod

When an SC error occurs the response message contains the attributes:

mty=CRP
mid=53834
sec=3000
set=Client is not subscribed to service: P01_BCST_CH_RPRWS2

6.24 PUBLISH (SPU)

This message is sent from the publishing server to SC in order to send this message to the subscribed clients. The message has a body and contains these attributes:

mty=SPU
nam=P01_BCST_CH_RPRWS2
mid=65411
min=CH_AUCTION_IOI
msk=%%%%%%%%%%%%%%%%%%%%%%%%%%X%%%%%%%%%%%%%%%%%%%%

SC receives the message and does the following steps:

1. It inserts the message on top of the message queue for this service
2. Sends back to the server a message with the following attributes:
   mty=SPU
   nam=P01_BCST_CH_RPRWS2
   mid=65412
3. Starts distribution of the message to the subscribed clients based on their subscription mask and the mask of the message.

When an SC error occurs the response message contains the attributes:

mty=SPU
mid=53834
sec=3000
set=Service P01_BCST_CH_RPRWS2 does not exist

6.25 FILE_DOWNLOAD (FDO)~~HTTP (HTT)~~

This message is used to download file from~~transport HTTP protocol over SCMP. This is section necessary when~~ a web server.~~SC network segment is configured to use plain TCP/IP.~~
The message has no~~a regular~~ body and contains these attributes:

mty=FDO
nam=P01_LOGGING
rfn=LSC TradingClientGUI_20100115_07h28m59s.log

The SC takes the message and initiates a download from the web server configured for this service. The requesting URL is constructed according to the configuration and the given remote file name. The response message has a body containing the file and has these attributes:

mty=FDO
bty=http
nam=P01_LOGGING
rfn=LSC TradingClientGUI_20100115_07h28m59s.log

The maximal message length may exceed the 64kB limit.

On Error the SC may return message a response message contains the attributes:

mty=FDO

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

nam=P01_LOGGING
rfn=LSC TradingClientGUI_20100115_07h28m59s.log
sec=4000
set=404 Not found
See http://www.w3.org/Protocols/rfc2616/rfc2616-sec6.html#sec6.1.1 for possible status codes and reasons.

6.26 FILE_UPLOAD (FUP)

This message is used to upload file to a web server. The message has a body containing the file and has these attributes:

mty=FUP
bty=http
nam=P01_CONFIGURATION
rfn=SCconfig-P01-V3.3-433.properties

The SC takes the message and initiates an upload to the web server configured for this service. The requesting URL is constructed according to the configuration and the given remote file name. The response message has no body and has these attributes:

mty=FUP
nam=P01_LOGGING
rfn=SCconfig-P01-V3.3-433.properties

The maximal message length may exceed the 64kB limit. On Error the SC may return message a response message contains the attributes:

mty=FUP
nam=P01_LOGGING
rfn=SCconfig-P01-V3.3-433.properties
sec=4000
set=406 Not Acceptable

See http://www.w3.org/Protocols/rfc2616/rfc2616-sec6.html#sec6.1.1 for possible status codes and reasons.

6.27 FILE_LIST (FLI)

This message is used to get list of files on web server. The Web Server must allow the directory browsing. The message has a no and has these attributes:

mty=FLI
nam=P01_CONFIGURATION

The SC takes the message and creates an URL to explore the location on the web server corresponding to the service. The response message has body and has these attributes:

mty=FLI
bty=http
nam=P01_CONFIGURATION

The maximal message length may exceed the 64kB limit. On Error the SC may return message a response message contains the attributes:

mty=FLI
nam=P01_CONFIGURATION
sec=4000
set=403 Forbidden

See http://www.w3.org/Protocols/rfc2616/rfc2616-sec6.html#sec6.1.1 for possible status codes and reasons.~~mty=HTT~~
~~mid=53834~~
~~bty=http~~

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

~~SC passes this message to the next node as defined in its configuration.~~

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

7 SCMP Header Attributes

The following is a list of all possible attributes in a SC message header in alphabetical order. All attributes and their values are ASCII, encoded as ISO 8859-1 (Latin-1).

You can find the matrix describing which attribute is used in which message at the end of this document.

7.1 appErrorCode (aec)

Name	appErrorCode
Code	aec
Description	Numeric value passed between server and the client used to implement error protocol on the application level.
Validation	Numeric value ≥ 0
Comment	This can be used by the client to check a specific server error.
Example	aec=4334591

7.2 appErrorText (aet)

Name	appErrorText
Code	aet
Description	Textual value passed between server and the client used to implement error protocol on the application level. It can be the textual interpretation of the *appErrorCode*.
Validation	Any printable character, length > 0 and < 256Byte
Comment	This can be used by the client to display or log an error that occurred on the server and so get the user better understanding what happened.
Example	aet=%RDB-F-NOTXT, no transaction open

7.3 authSessionId (asi)

Name	authSessionId
Code	asi
Description	Authenticated session ID.
Validation	none
Comment	This attribute is optionally sent by the client for a subscription. It is passed to the publishing server in order to allow look-up for authenticated session on the server.
Example	asi= cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d

~~7.3~~7.4 bodyType (bty)

Name	bodyType
Code	bty
Description	Type of the message body.
Validation	Enumeration: • txt – message body is ISO-8859-1 (Latin 1) encoded text • bin – binary data (default) • http – message is part of HTTP over SCMP transport

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

	• xml – XML data (not implemented yet)
Comment	When http transport is used, the content-type header is set according to this attribute.
Example	bty=txt

~~7.4~~7.5 cacheExpirationDateTime (ced)

Name	cacheExpirationDateTime
Code	ced
Description	When sent by the server then it represents the absolute expiration date and time of the message in cache. When sent by the client then it represents the latest date and time of the message in cache the client will accept. It must be set together with *cacheId* attribute.
Validation	YYYY-MM-DDThh:mm:ss.fff+hhmm It is local date time plus zone information. The fff are seconds fractions and time zone offset is at the end.
Comment	The client uses *cacheExpirationDateTime* to tell how old the message could be. The server uses *cacheExpirationDateTime* to define how long the message is valid. The client will get a cached message when: 1. the *cacheId* matches a message in the cache and 2. *cacheExpirationDateTime* requested by the client is timely before the *cacheExpirationDateTime* of the cached message. Client sending ced=9999-12-31T23:59:59.999+0000 will never get the message from the cache.
Example	ced=1997-08-16T19:20:34.237+0200

~~7.5~~7.6 cacheId (cid)

Name	cacheId
Code	cid
Description	Identification agreed by the communicating applications to uniquely identify the cached content. When *cacheID* is used the attribute *cacheExpirationDateTime* must also be present.
Validation	Any printable character, length > 0 and < 256Byte
Comment	The client uses *cacheId* to identify which message should be retrieved from the cache. The server uses *cacheId* to designate message that should be cached. The client will get a cached message when: 1. the *cacheId* matches a message in the cache and 2. *cacheExpirationDateTime* requested by the client is timely before the *cacheExpirationDateTime* of the cached message.
Example	cid=CBCD_SECURITY_MARKET

~~7.6~~7.7 clnRequesterId (crq)

Name	clnRequesterId
Code	crq
Description	Identification of the client requester
Validation	Any printable character, length > 0 and < 256Byte
Comment	Concatenation of IP address and port. Used for troubleshooting.
Example	crq=128.45.3.12:1244

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

~~7.7~~7.8 compression (cmp)

Name	compression
Code	cmp
Description	Flag true or false describing if the message body is compressed or not.
Validation	True is present, false is missing
Comment	The compression can be enabled or disabled on message level.
Example	cmp

7.9 echoInterval (eci)

Name	echoInterval
Code	eci
Description	Interval in seconds between two subsequent CLN_ECHO messages are sent by the client.
Validation	Number ≥ 1 and < 3600
Comment	This is used by the SC to detect a broken session. The value should be set with respect to the throughput of the network connection and the server load. e.g. If this timeout expires the session is treated as dead and a cleanup is done.
Example	eci=300

7.10 echoTimeout (ect)

Name	echoTimeout
Code	ect
Description	Maximal response time in seconds allowed for SRV_ECHO sent to the server (measured in SC).
Validation	Number ≥ 1 and < 3600
Comment	This is used by SC to detect a broken session. When this timeout expires, the session is treated as dead and the client is informed.
Example	ect=10

~~7.8~~7.11 immediateConnect (imc)

Name	immediateConnect
Code	imc
Description	Flag true or false to tell SC when connection to the server should be created. ~~If missing the default value is true.~~
Validation	True is present, false is missing
Comment	After server registers to a service SC will create as many connections to it as defined by *maxSession*. When *immediateConnect* = true SC will create the connections immediately and keep the session until DEREGISTER_SERVICE~~deregister service~~ is done. When *immediateConnect* = false SC will create the connections before a session is allocated and close the connection when the session is deleted.
Example	imc

~~7.9~~7.12 ipAddressList (ipl)

Name	ipAddressList
Code	ipl
Description	List of IP addresses on the network path between the client and the session server. The list contains ~~pairs of~~ IP addresses in the form 999.999.999.999

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

Validation	List in format {999.999.999.999/999.999.999.999}...
Comment	The list has at least three~~four~~ entries. 1. IP of the client, 2. Incoming IP received by SC (IP of the VPN Tunnel) 3. IP of the SC 4. ~~Incoming IP received by server~~ Client connected via cascaded SC placed in a customer DMZ will have the list in the format: 1. IP of the client, 2. Incoming IP received by SC in customer DMZ. 3. IP of the SC in customer DMZ 5. Incoming IP received by SC (IP of the VPN Tunnel) 6. IP of the SC 4. ~~Incoming IP received by server~~ If any of the pairs at position1-2 or 3-4has different values, then in this network segment NAT occurs. As long as there is only one SC behind the VPN, the second~~third~~ last address is always the tunnel IP used for the authentication.
Example	ipl=10.0.4.32/10.2.54.12/192.243.43.1~~/192.243.43.1~~

7.13 keepaliveInterval (kpi)

Name	keepaliveInterval
Code	kpi
Description	Interval in seconds between two subsequent keepalive requests (KRQ). The keepalive message is used to refresh the firewall timeout on the network path. Keepalive message is only sent on a idle connection. The value = 0 means no keep alive messages will be sent.
Validation	Number ≥ 0 and < 3600
Comment	The keepaliveInterval is exchanged at the beginning of the communication. In ATTACH the *keepaliveInterval* defines how often the client will send keepalive messages to the SC. In REGISTER SERVICE the *keepaliveInterval* defines how often the server will sent keepalive messages to SC and how often will SC sent keepalive messages back to the server.
Example	kpi=360

~~7.10~~7.14 localDateTime (ldt)

Name	localDateTime
Code	ldt
Description	String value describing the actual local date and time.
Validation	YYYY-MM-DDThh:mm:ss.fff+hhmm It is local date time plus zone information. The fff are seconds fractions and time zone offset is at the end after the + sign.~~.~~
Comment	The local date time is exchanged at the beginning of the communication (ATTACH, REGISTER SERVICE).~~each connection and in the keep alive messages.~~ It is used to calculate the time difference between the communicating parties and to harmonize the log for troubleshooting purposes.
Example	ldt=1997-07-16T19:20:30.064+0100

~~7.11~~7.15 messageID (mid)

Name	messageId

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

Code	mid
Description	Identification generated by the sender of a message in order to identify and track it during a session.~~transmission.~~ The sessionId + the messageId uniquely identify the message.~~ at any point of its transmission.~~ Request and response messages are treated as independent.
Validation	Composite Id in format 9[/9] First is a message sequence number optionally followed by delimiter "/" and a part sequence number to count parts of large messages. Both numbers > 0.~~0, steadily increasing.~~
Comment	For large messages the message sequence number is extended with a part sequence number. The message sequence number is reset at begin of the session~~communication~~ and is steadily increasing, incremented by the sender. The part sequence number is reset for every regular message and steadily increasing, incremented by the sender for every message part.
Example	**REQ .. mid=3** **RES .. mid=64** ... **PRQ .. mid=4/1** PRS .. mid=65/1 PRQ .. mid=4/2 PRS .. mid=65/2 PRQ .. mid=4/3 PRS .. mid=65/3 **REQ .. mid=4/4** PRS .. mid=66/1 PRQ .. mid=5/1 PRS .. mid=66/2 PRQ .. mid=5/2 **RES .. mid=66/3** ... **REQ .. mid=6** **RES .. mid=67**

~~7.12~~7.16 messageInfo (min)

Name	messageInfo
Code	min
Description	Optional information passed together with the message body that helps to identify the message content without investigating the body.
Validation	Any printable character, length > 0 and < 256Byte
Comment	This can be set by the sender and evaluated by the receiver of the message to simplify decision how the message should be processed. It can also be used for troubleshooting to identify the message during the message transmission.
Example	min=SECURITY_MARKET_QUERY

~~7.13~~7.17 messageType (mty)

Name	messageType
Code	mty
Description	Unique message type
Validation	List of known message types
Comment	Message type that represents a certain command. The direction of the message is visible in the headline.
Example	mty=ATT

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

~~7.14~~7.18 mask (msk)

Name	mask
Code	msk
Description	The mask is used in SUBSCRIBE or CHANGE_SUBSCRIPTION to express the client interest and in PUBLISH to designate the message contents. Only printable characters are allowed.
Validation	Any printable character, length < 256Byte Client may not subscribe with mask containing "%" character.
Comment	If the message mask matches the subscription mask, the client will get this message. The matching rules: • masks of unequal length do not match • % - matches any single character at this position • All other characters must exactly match (case sensitive)
Example	Subscription mask: msk=00001210001283210 2FADF----------X---------- Matching examples of message masks: msk=00001210001283210 2FADF----------X---------- msk=0000121%%%%%%%%%%%%%%----------X---------- Not matching examples of message masks: msk=00001210001283210 2FADF---------- msk=0000121%%%%%%%%%%%%%%----------

~~7.15~~7.19 maxSessions (mxs)

Name	maxSessions
Code	mxs
Description	Number of sessions this server instance can serve.
Validation	Number > 0
Comment	When a session server registers to a service it must tell the SC how many sessions it can serve. This is necessary to know in order to maintain the count of free/busy servers in SC. The value 1 means single session server. Value > 1 means multi-connection server. See also *immediateConnect* flag
Example	mxs=10

~~7.16~~7.20 noData (nod)

Name	noData
Code	nod
Description	NoData flag is used in RECEIVE_PUBLICATION to tell the subscribed client, that no data for publishing exists. The client must immediately send another RECEIVE_PUBLICATION to renew the interest.
Validation	True if present, false if missing
Comment	
Example	nod

7.21 noDataInterval (noi)

Name	noDataInterval
Code	noi

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

Description	Interval in seconds the SC will wait to deliver RECEIVE_PUBLICATION response with *noData* flag set.
Validation	Number > 0 and < 3600
Comment	The receiving client monitors the interval and treats the subscription as broken when this time is exceeded.
Example	noi=60

7.22 originalMessageID (omi)

Name	Orginal message ID
Code	omi
Description	Orginal message ID used by the publishing server to send the message.
Validation	Number > 0
Comment	This is used in RECEIVE_PUBLICATION messages as cross reference to the original message. It is required for troubleshooting the message fan-out.
Example	omi=355

~~7.17~~7.23 portNr (pnr)

Name	portNr
Code	pnr
Description	Number of the TCP/IP port the session server accepts the connection(s).
Validation	Number > 0 and < 99999
Comment	When a session server registers, SC will create a connection to this server on the IP address of the server and the given port number. Multiple connections are created to the same port. The value must be > 1.
Example	pnr=9100

~~7.18 receiverTimeout (rct)~~

~~Name~~	~~receiverTimeout~~
~~Code~~	~~rct~~
~~Description~~	~~Interval in seconds between two subsequent KEEPALIVE messages received by the receiver~~ ~~The value = 0 means no keep alive messages will be used.~~
~~Validation~~	~~Number ≥ 0 and < 3600~~ ~~If *receiverTimeout* is 0 then *senderTimeout* must also be 0.~~ ~~*receiverTimeout > senderTimeout*~~
~~Comment~~	~~This is used by the receiver to detect a broken connection. The value should be set with respect to the latency of the communication e.g. *receiverTimeout = sendingInterval + (senderTimeout / 2)*~~ ~~If this timeout expires the connection is treated as dead and a cleanup is done.~~
~~Example~~	~~rct=60~~

~~7.19~~7.24 rejectSession (rej)

Name	rejectSession
Code	rej
Description	Flag in response of SRV_CREATE_SESSION message set by the server when it rejects the session. In such case the server can also set the *appErrorCode* and *appErrorText* to explain the rejection reason. Subsequent response CLN_CREATE_SESSION message to client contains the same values.

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

Validation	True if present, false if missing
Comment	
Example	rej

7.25 remoteFileName (rfn)

Name	remoteFileName
Code	rfn
Description	Name used in FILE_UPLOAD in to store the file on the web server or name used in FILE_DOWNLOAD to get the download the file.
Validation	Any printable character allowed as filename, length < 256Byte
Comment	
Example	rfn=LSC TradingClientGUI_20100115_07h28m59s.log

~~7.20~~7.26 scErrorCode (sec)

Name	scErrorCode
Code	sec
Description	Numeric error code set by SC in other to inform the communication partner about an error. List of possible error codes will be published.
Validation	Number > 1
Comment	This is used to handle the SC error. The message must have EXC key in the headline.
Example	sec=4453

~~7.21~~7.27 scErrorText (set)

Name	scErrorText
Code	set
Description	English text set by the SC in other to describe the error signalled as *scErrorCode*. Precise error description must be here.
Validation	Any printable character, length > 0 and < 256Byte
Comment	This is used to log or display the SC error. The message must have EXC key in the headline.
Example	set=Unknow service name: P01_RTXR_RPRWS4

~~7.22~~7.28 scReqesterId (crq)

Name	scReqesterId
Code	crq
Description	Unique identification of the SC requester
Validation	Any printable character, length > 0 and < 256Byte
Comment	Concatenation of IP address and port. Used for troubleshooting.
Example	crq=128.45.3.12:1244

~~7.23~~7.29 scResponderId (crs)

Name	scResponderId
Code	crs
Description	Unique identification of the SC responder
Validation	Any printable character, length > 0 and < 256Byte

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

Comment	Concatenation of IP address and port. Used for troubleshooting.
Example	crs=128.45.3.12:1244

~~7.24~~7.30 scVersion (ver)

Name	scVersion
Code	ver
Description	Software version number of the producer of this message.
Validation	String format 9.9-999
Comment	This version number is sent in ATTACH or REGISTER_SERVER and checked by the receiver against its own SC version number. This ensures that only compatible components can communicate to each other. The value is hard coded in the communication components like API or SC. The version number looks like 1.0-023: • 1 = Release number • 0 = Version number • 023 = Revision number The matching rules are: • Request: 1.0-023 + own: 1.0-023 => compatible • Request: 1.0-023 + own: 1.0-025 => compatible • Request: 1.0-025 + own: 1.0-023 => not compatible (requestor may utilize new features unknown here) • Request: 1.0-023 + own: 1.2-005 => compatible • Request: 1.2-004 + own: 1.0-023 => not compatible (requestor uses new functions unknown here) • Request: 1.0-023 + own: 2.0-007 => not compatible (possibly other incompatible interface) • Request: 2.0-001 + own: 1.0-023 => not compatible (possibly other incompatible interface)
Example	ver=1.0-023

~~7.25 senderTimeout (snt)~~

~~Name~~	~~senderTimeout~~
~~Code~~	~~snt~~
~~Description~~	~~Maximal time in seconds allowed between KEEPALIVE request and response (measures by the sender).~~ ~~The value = 0 means no keep alive messages will be sent.~~
~~Validation~~	~~Number ≥ 0 and < 3600~~ ~~If *senderTimeout* is 0 then *receiverTimeout* must also be 0.~~
~~Comment~~	~~This is used by the sender to detect a broken connection. When this timeout expires, the connection is treated as dead and a cleanup is done.~~
~~Example~~	~~snt=10~~

~~7.26~~7.31 serviceName (nam)

Name	serviceName
Code	nam
Description	Name of the service
Validation	Any printable character, length > 0 and < 256Byte
Comment	The service name is an abstract name and represents the logical address of the service. It order to allow message routing the name must be unique in scope of the entire SC network. Service names must be agreed at the application level and

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

	are stored in the SC configuration.
Example	nam=P01_RTXS_RPRWS1

~~7.27~~7.32 sessionId (sid)

Name	sessionId
Code	sid
Description	Unique identification of the session
Validation	Known session
Comment	The sessionId is allocated by SC to which the client is connected when it sends the request CLN_CREATE_SESSION. The sessionID is universally unique because multiple SC may exist in the same network. The client must set the sessionId in each message during the session. For publishing services the sessionId is allocated by SC to the client when it sends the request SUBSCRIBE message. Subscription is internally treated as a session.
Example	sid=cdc50b36-1fc4-4f9e-8430-d2e3d7284d9d

~~7.28~~7.33 sessionInfo (sin)

Name	sessionInfo
Code	sin
Description	Additional information passed by the client to the session server when the session starts.
Validation	Any printable character, length > 0 and < 256Byte
Comment	This is used to pass additional authentication or authorization data to the server.
Example	sin=SNBZHP - TradingClientGUI 10.2.7

~~7.29~~7.34 srvRequersterId (srq)

Name	srvReqId
Code	srq
Description	Unique identification of the server requester
Validation	Any printable character, length > 0 and < 256Byte
Comment	Concatenation of IP address and port. Used for troubleshooting.
Example	srq=128.45.3.12:1244

~~7.30~~7.35 srvResponderId (srs)

Name	srvResponderId
Code	srs
Description	Unique identification of the server responder
Validation	Any printable character, length > 0 and < 256Byte
Comment	Concatenation of IP address and port. Used for troubleshooting.
Example	srs=128.45.3.12:1244

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

8 Glossary

Client

Piece of an application consuming services and initiating actions.

Server

Piece of an application providing services to clients.

Service

Abstract unit of work provided by the server and delivered to the client in order to implement a specific functionality. SC supports session, publishing and file services.

Session

Temporary allocation of a dedicated server to a client. Session ensures information flow between a client and the allocated server. SC supports request/response sessions and subscription sessions.

Call

A call represents a pair of a request and response.

Command

A command dispatches specific actions on a server according to the incoming request.

Request

Data structure created by the Client or SC in order to initiate an information exchange. It may contain one or more messages.

Response

Data structure created by the Server or SC in order to deliver the requested information. It may contain one or more messages.

Message

Basic transport instrument to exchange information between client, SC and the server. It belongs to a request or to a response.

Message Part

Message part is a piece of a large message. Large message is splittet into parts.

Composite

Data structure prepared to hold all message parts of a large message

Registry

Common list of known objects that ensures their uniqueness, organized in a way to find them easily.

Requester

Piece of code in SC or client initiating the information exchange

Responder

Piece of code in SC or server delivering the requested information

Connection

Network communication between client and SC or SC and the server

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG

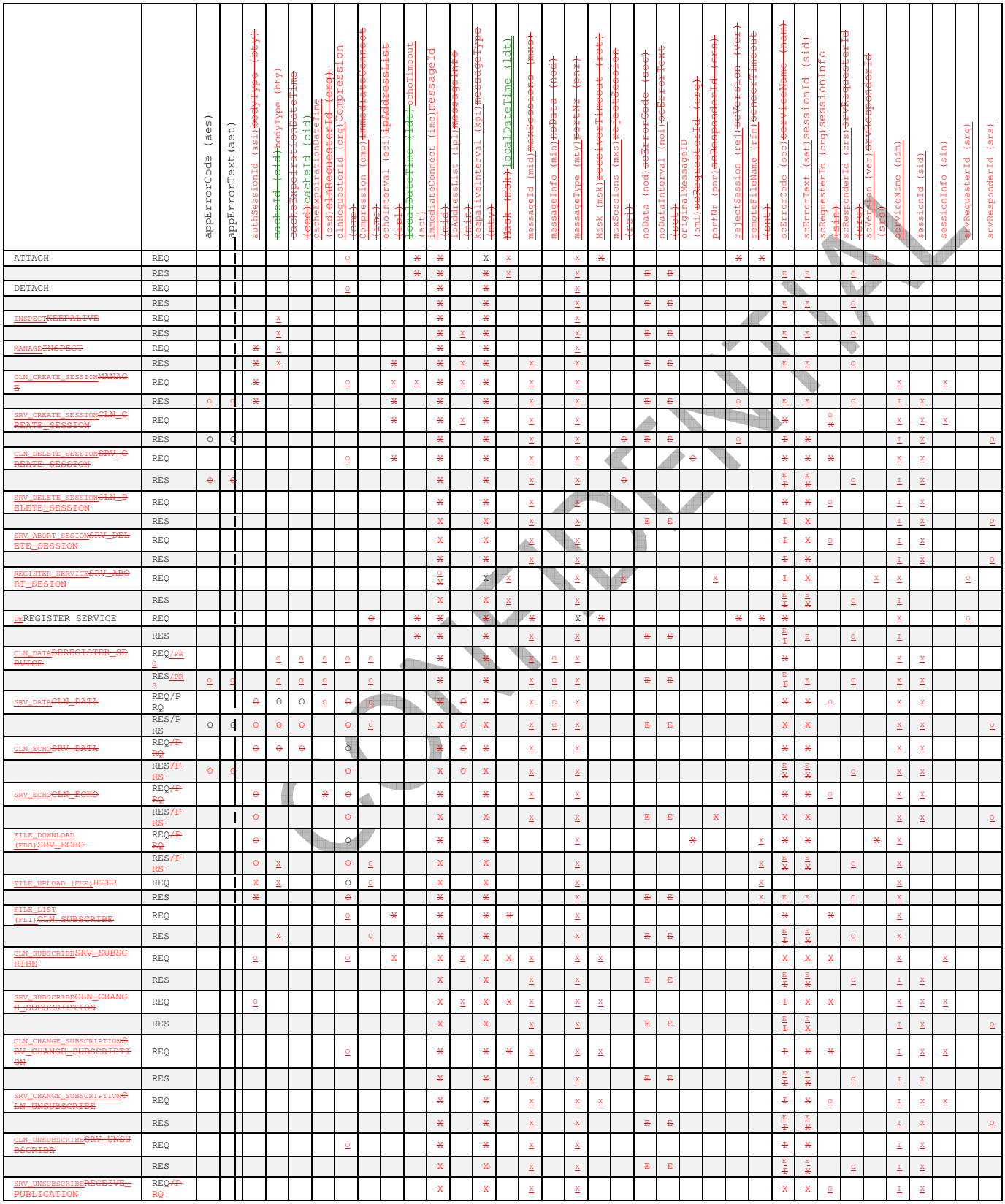
Endpoint

Network communication part on SC or server

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

Appendix A Message Header Matrix



Confidential
Copyright © 2010 by STABILIT Informatik AG

	RES/PRS			O				O				X	X	X	I	X	O	X			E	E								I	X			O
RECEIVE_PUBLICATION	REQ/PRQ			O				O				X	X	X	X	X		X									X					X	X			
	RES/PRS				O				O			X		X		X	X	X	I		O	X	X				E	E			O			I	X			
PUBLISH	REQ/PRQ				O				O							X	X	X	X													X			O	
	RES/PRS															X		X									E	E			O			I				

Legend:
X => required attribute
O => optional attribute
I => informational only
E => EXC exception message only

CONFIDENTIAL

Confidential
Copyright © 2010 by STABILIT Informatik AG

Index

No index entries found.

CONFIDENTIAL

Copyright © 2010 by STABILIT Informatik AG