Protocol for Drop Copy Service

Capital Markets Segment

Version 3.0

February 2025

National Stock Exchange of India Ltd
Exchange Plaza, Plot No. C/1, G Block,
Bandra-Kurla Complex, Bandra (E)
Mumbai - 400 051.

Notice

Drop Copy Service - Capital Market Segment Revision History		
Version	Page No	Description
3.0	6-51	Document for the new Trade Only and Order & Trade Drop Copy API, including details on Optimized message Structure, connection mechanism and multiple partition, it also include details about encryption and compression. The document should be referred in its entirety and not in parts.

CONTENTS

Chapter 1 Introduction

The NSE Drop Copy (DC) service provides dedicated Trade Only and Order & Trade data. It disseminates information about members / users order and trades on a real time basis. The data is sent to users on a TCP/IP communication protocol connection. At the time of initial login, all members need to connect to the Drop Copy Gateway Router, which will assign a Drop Copy Gateway. Order Trade Drop Copy & Trade Drop Copy are two different services and can be accessed through two different gateway router connections. Members will initiate the connection to the assigned DC Gateway using the existing login credentials being used for login to the Trading System. A Corporate Manager user will get member firm level Order and trade data. However, branch manager and dealer users will get respective user order and trade data. Any changes to the login credentials during the day on the Trading System will be effective on drop copy gateway on the same day.

The order and trades data structures are now revised for the Drop Copy service.

Chapter 2 General Guidelines

Introduction

This chapter provides general guidelines for the designers and programmers who develop Drop Copy consumers. It also provides information on data types and their size which can help in understanding various structures.

Message Structure Details

The message structure consists of two parts namely message header and message data. The message header consists of the fields of the header which is prefaced with all the structures. The message data consists of the actual data that is sent across to the drop copy system (i.e., host) or received from the drop copy system (i.e., host).

Transaction code, an important field of the message header, is a unique numeric identifier which is sent to or received from the system. This is used to identify the transaction or activity type.

Guidelines for Programmers

1. All time fields are time values with base as midnight January 1, 1980.
2. If your system uses a little-endian order, the data types such as INT, SHORT, LONG and DOUBLE contained in a packet, which occupy more than one byte should be twiddled (byte reversed). Twiddling involves reversing a given number of bytes such that the byte in 'n' position comes to the first position; the byte in (n-1) position comes to the second position and so on. For example, if the value to be sent is 1A2B (hexadecimal), reverse the bytes to 2B1A. The same applies while receiving messages. So, if the value received is 02BC, the actual value is BC02.

   Note: Twiddling is required because of the variety in endian order—big and little. A big-endian representation has a multibyte integer written with its most significant byte on the left. A little-endian representation, on the other hand, places the most significant byte on the right. **The system host end uses little-endian order**.

3. All alphabetical data must be converted to the upper case except password before sending to the host. A combination of the alphabet, numbers and special characters are allowed in the password. More details on password are explained in later chapters in this document. No NULL terminated strings should be sent to the host end. Instead, fill it with blanks before sending. The strings received from the host end are padded with blanks and are not NULL terminated.
4. All the structures should be defined in the following manner:
   - Items of type char or unsigned char, or arrays containing items of these types, are byte aligned.
   - All structures are pragma pack 2. Structures of odd size should be padded to an even number of bytes.
   - All other types of structure members are word aligned.
5. All numeric data must be set to zero (0) before sending to the host unless a value is assigned to it.
6. All reserved fields mentioned should be mapped to CHAR buffer and initialized to blank.

   Note:

   - The values of all the constants and transaction codes given in the document are listed in the Appendix.
   - The suffix IN in the transaction codes implies that the request is sent from the user system to the service host end whereas OUT implies that the message is sent from the service host end to user system.

Data Types Used

Table 2.1 DATA TYPES

Data Type	Size of Bytes	Signed / Unsigned
CHAR	1	Signed
INT	4	Signed
SHORT	2	Signed /Unsigned
LONG	8	Signed
DOUBLE	8	Signed and Floating Point
BIT	1 bit	NA

Note: 64 Bit data type format is considered in the above table

Request Message Header

Each incoming request is prefaced with a REQUEST_MESSAGE_HEADER which is an interactive header. Some data in the header are fixed whereas some data are variable and set differently for each transaction code. The structure of the Request Message Header is as follows:

Table 2.2 REQUEST MESSAGE HEADER

Structure Name	REQUEST_MESSAGE_HEADER		
Packet Length	24 bytes		
Field Name	**Data Type**	**Size in Byte**	**Offset**
TransactionCode	SHORT	2	0
TraderId	INT	4	2
SequenceNumber	LONG	8	6
PartitionID	CHAR	6	14
ConcurrentLoginID	SHORT	2	20
Reserve	CHAR	2	22

The fields of Message Header are described below.

Field Name	Brief Description
TransactionCode	Transaction message number. This describes the type of message received or sent.
TraderId	This field contains the user ID.
SequenceNumber	Sequence number for the messages being sent by the User.
Partition ID	This field contains the partition ID (Stream) for which the packet is being sent by the User. Partition ID will be identified as MXXPXX; where M is market indicator followed by 2-digit market number and P is the partition indicator followed by 2-digit partition number. Eg – For partition 1 of mkt stream 2; partition ID will be M02P01
ConcurrentLoginID	This field contains Concurrent login number of the User for which User has logged in. Expected values shall be numeric value between 1 to the max user connection allowed by exchange.

Response Message Header

Overall Response structure is prefaced with a Response_Message_Header (In case of packing multiple messages in one packet it will be appear one time). The structure of the Response Message Header is as follows:

Table 2.3 RESPONSE MESSAGE HEADER

Structure Name	RESPONSE_MESSAGE_HEADER		
Packet Length	2 bytes		
Field Name	**Data Type**	**Size in Byte**	**Offset**
Environment Type	CHAR	1	0
Compression Indicator	CHAR	1	1

Field Name	Brief Description
EnvironmentType	Following are the possible values for Environment Type • '1' for Production Environment • '2' for Prod Parallel (Mock) Environment • '3' for Testing Environment
Compression Indicator	Following are the possible values for Compression Indicator • '0' for No compression done

Field Name	Brief Description
	• '1' for Data is compressed.

Message Header

Each response message is prefaced with a MESSAGE_HEADER. The structure of the Message Header is as follows:

Table 2.4 MESSAGE HEADER

Structure Name	MESSAGE_HEADER		
Packet Length	14 bytes		
Field Name	**Data Type**	**Size in Byte**	**Offset**
TransactionCode	SHORT	2	0
ErrorCode	SHORT	2	2
SequenceNumber	LONG	8	4
Length	SHORT	2	12

Field Name	Brief Description
TransactionCode	Transaction message number. This describes the type of message received or sent.
ErrorCode	This field describes the type of error. Refer to List of Error Codes in Appendix.
SequenceNumber	Sequence number for the messages being sent by the Drop Copy Service system.
Length	Length of the data.

Order Flags

Table 2.5 ST_ORDER_FLAGS

For Big Endian Machines:

Structure Name	ST_ORDER_FLAGS		
Packet Length	2 bytes		
Field Name	**Data Type**	**Size in Bit**	**Offset**
MF	BIT	1	0

Structure Name	ST_ORDER_FLAGS		
Packet Length	2 bytes		
Field Name	Data Type	Size in Bit	Offset
AON	BIT	1	0
IOC	BIT	1	0
GTC	BIT	1	0
Day	BIT	1	0
OnStop	BIT	1	0
Mkt	BIT	1	0
ATO	BIT	1	0
Reserved	BIT	1	1
STPC	BIT	1	1
Reserved	BIT	1	1
Preopen	BIT	1	1
Frozen	BIT	1	1
Modified	BIT	1	1
Traded	BIT	1	1
MatchedInd	BIT	1	1

For Small Endian Machines:

Structure Name	ST_ORDER_FLAGS		
Packet Length	2 bytes		
Field Name	Data Type	Size in Bit	Offset
ATO	BIT	1	0
Mkt	BIT	1	0
OnStop	BIT	1	0
Day	BIT	1	0
GTC	BIT	1	0
IOC	BIT	1	0
AON	BIT	1	0
MF	BIT	1	0
MatchedInd	BIT	1	1

Structure Name	ST_ORDER_FLAGS		
Packet Length	2 bytes		
Field Name	Data Type	Size in Bit	Offset
Traded	BIT	1	1
Modified	BIT	1	1
Frozen	BIT	1	1
Preopen	BIT	1	1
Reserved	BIT	1	1
STPC	BIT	1	1
Reserved	BIT	1	1

Error Response

When the Error Code in the Message Header is having nonzero value, ERROR RESPONSE is sent. The Error Message will describe the error received. The structure is as follows:

Table 2.7 ERROR_RESPONSE

Structure Name	ERROR RESPONSE		
Packet Length	142 bytes		
Field Name	Data Type	Size in Byte	Offset
MESSAGE_HEADER (Refer Table 2.4)	STRUCT	14	0
Error Message [128]	CHAR	128	14

Field Name	Brief Description
ErrorMessage	Stores the error message. Refer to List of Error Codes in Appendix.

Book Types

Table 2.8 BOOK_TYPES

Book Type	Book ID	Market Type
Regular Lot Order	1	Normal Market
Special Terms Order	2	Normal Market
Stop Loss Order	3	Normal Market

Book Type	Book ID	Market Type
Negotiated Order	4	Normal Market
Odd Lot Order	5	Odd Lot Market
Spot Order	6	Spot Market
Auction Order	7	Auction Market
Call Auction1	11	Call auction1 market
Call Auction2	12	Call auction2 market

Heartbeat Exchange

Member systems must exchange heartbeat signals with drop copy service system during periods of inactivity. Service Host will consider the member system as inactive after missing two heartbeats in succession and disconnect the socket connection. Heartbeats will carry request message header only. Heartbeat is to be sent only if there is inactivity for 30 seconds. The format is MESSAGE_HEADER with following detail.

Table 2.9 HEARTBEAT

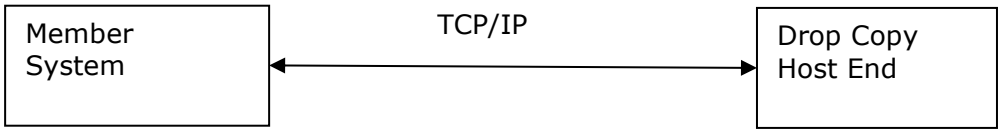
Structure Name	HEARTBEAT		
Packet Length	**24 bytes**		
Field Name	**Data Type**	**Size in Byte**	**Offset**
REQUEST_MESSAGE_HEADER (Refer Table No 2.2)	STRUCT	24	0

Field Name	Brief Description
TransactionCode	The transaction code is HEARTBEAT (23506)

Chapter 3 Drop Copy Communication

Introduction

TCP/IP communication protocol shall be used between Member System and Drop Copy Host end as per the Network setup.



Packet Format

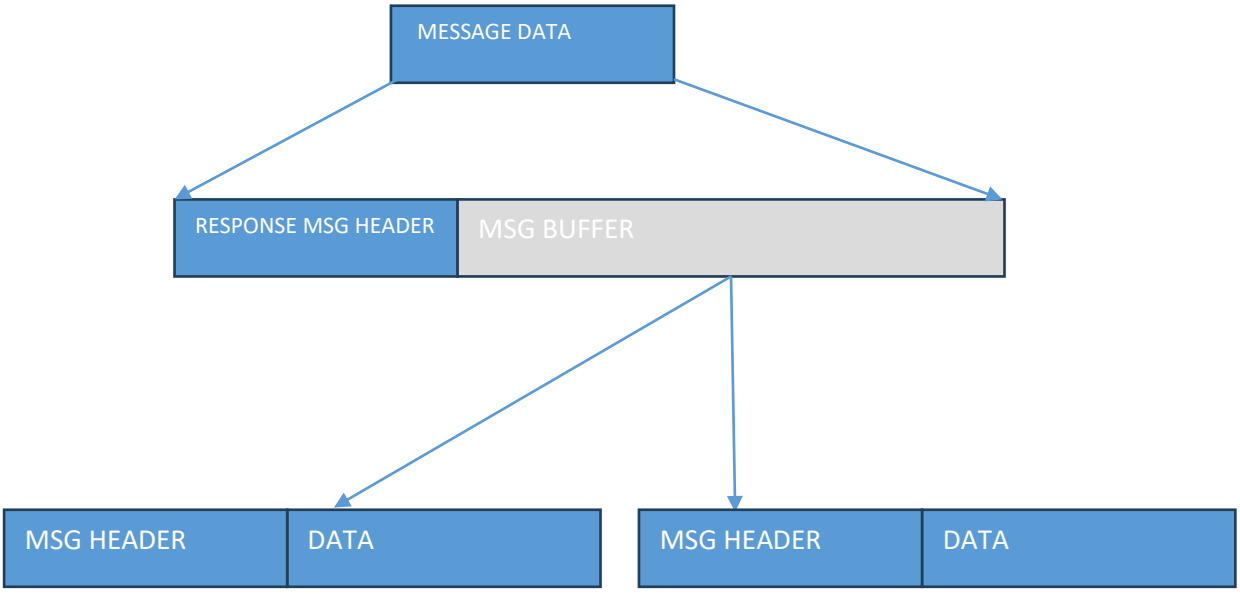
Packet structure for communication between Member System and Host End

This structure is applicable to all messages that flow between Client and Drop Copy Host

Length (2 bytes)	Sequence number (4 bytes)	Checksum (MD5) for Message data (16 bytes)	Message Data (Variable length)

- Max length will be the predefined value of 1400 bytes.
  Length = size of length field (2 bytes) +
  size of sequence number field (4 bytes) +
  size of the checksum field (16 bytes) +
  size of Message data (variable number of bytes as per the transcode).
- Maximum length of message data can be 1378
- Sequence number will start from 1 and will be incremented for every packet.
- The checksum algorithm used will be MD5. Checksum is applied only on the Message data field and not on the entire packet.
- For more details on MD5 refer: **RFC** 1321 (rfc1321) - The **MD5** Message-Digest Algorithm (http://www.faqs.org/rfcs/rfc1321.html)

- Message data will be of variable length and comprises of 24 bytes of request message header + variable sized data buffer as per transcode being sent in case of requests sent by Member system.
- Structure of Message Data sent by Host End is as follows



- First two bytes of message data will be response message header. Response message header will indicate the message buffer is compressed or not
- In case message buffer is not compressed, length of message buffer will be equal to message data length – 2 bytes (Response Message header)
- In case message buffer is compressed, actual length of message will be equal to length of message buffer after decompression (Please refer Compression and Decompression section).
- Maximum length of the message buffer after decompression can be 4096 bytes
- Message buffer may have multiple data packets, each data packet will be having message header and data part. Each data packet reads to be read one by one and length of the message buffer should be reduced by the length of data packet.

Packet Validation

Validation will be done for all requests flowing between Member System and Host End. Validation will be done through the combination of Checksum, Sequence Number, and length field.

Processing by Host

Before sending the request to Host, Member System will have to generate a sequence number and checksum value. All the requests being sent from Front-End will be sent in the format described above. If validation of sequence number, checksum value & length fails at Host End then the disconnection of the socket connection between Member System and Host End will happen.

Processing By Member System

On receiving the response from Host, Member software is expected to validate sequence number, checksum value & length field. Also it has to decompress the data if compression indicator is set.

Sequence number must be in sequential order. For any fresh connection the number should start from 1. Checksum field and the checksum recalculated on the data field must match. Length field must be less than or equal to 1400.

If any one of these validations fails, the Member System needs to drop the connection and reestablish a fresh connection**.**

Encryption/Decryption

Exchange proposes a combination of TLS 1.3 security protocol and AES-256 bits-based symmetric encryption approach. The following is an overview.

1st Step: Member applications will connect initially to Exchange Gateway Router server using TCP with TLS 1.3 security protocol and will receive unique session key from the Exchange through the secured connection.

Gateway router will be different for Order-Trade and Trade only subscription.

2nd Step: Member applications will then connect to allocated Exchange Gateway server through TCP, and each and every message will be encrypted/decrypted using the same session key (symmetric cryptography AES 256 bits GCM mode) at both member end and Exchange end.

Below are the details of the methodology

(i) Exchange will generate self-signed CA certificates on periodic basis. CA certificate will remain common for all members and shall be distributed as and when generated via extranet.

(ii) On a daily basis when member applications need to connect to trading platform for Drop Copy they will need to do the following

a. Member applications will connect to Exchange Gateway Router server on TCP using TLS 1.3 security protocol. As part of TLS 1.3 security protocol, it is recommended that member applications verify Gateway Router server authenticity using the CA certificate provided by the Exchange.

b. GR request and GR response messages will be sent and received by member applications using TLS 1.3 security protocol.

c. A unique 32-byte session key will be provided to member applications as part of GR response message.

(iii) Post successful communication with Gateway router server, member applications will establish a new TCP connection with the allocated gateway server of Exchange. The first message after connecting through TCP will be a non-encrypted special registration message (GR_SECURE_USER_REGISTRATION_REQUEST) to indicate that member application is using encryption. All the messages, after the first message, that are exchanged on this connection from both sides (member applications and Exchange) will be encrypted and decrypted using the 32-byte session key that was provided from Exchange at the time of Gateway Router handshake. GCM mode of symmetric cryptography AES 256 bits will be used by member applications and Exchange.

(iv) In case of new login or disconnection from one or more partition and then re login, the above-mentioned steps will be repeated

Sample function calls which could be considered for encryption-decryption for the above proposed approaches are provided in annexure for Encryption/Decryption.

Disconnection on MD5 Checksum failure

If member is connected on encrypted channel and MD5 checksum fails then a user sign off message with error code (19031) will be sent to member before disconnection.

Compression and Decompression

This section describes the Compression and Decompression algorithm is to be used for dropcopy related messages.

Compression of the Data

User can connect to Drop Copy system and seek data from the start of the day. This could result in large volume of data being served to the User depending on messages present in the system. To accommodate the increased network traffic in such cases, the exchange has come up with a compression algorithm to compress data being downloaded.

LZO compression algorithm is used to compress the specified broadcasts transaction codes. The details of the LZO compression algorithm are described later. The LZO stands for Lempel Ziv Oberhaumer. This algorithm is freely available on the internet (URL: http://www.oberhumer.com/opensource/lzo). It is made available by free software foundation. The algorithm is tested on various operating systems like UNIX and red hat Linux.

Sequential Packing

To improve the effective data transfer, the idea of sequential packing of messages along with the LZO compression algorithm has been incorporated. At the host end, sequential packing algorithm packs the messages which are meant for download. Data packets are packed in FIFO order. Post packing, compression of entire data will be done. Compression indicator field will be set to "1" in response message header to convey that message body (buffer) that follows is compressed.

For example,

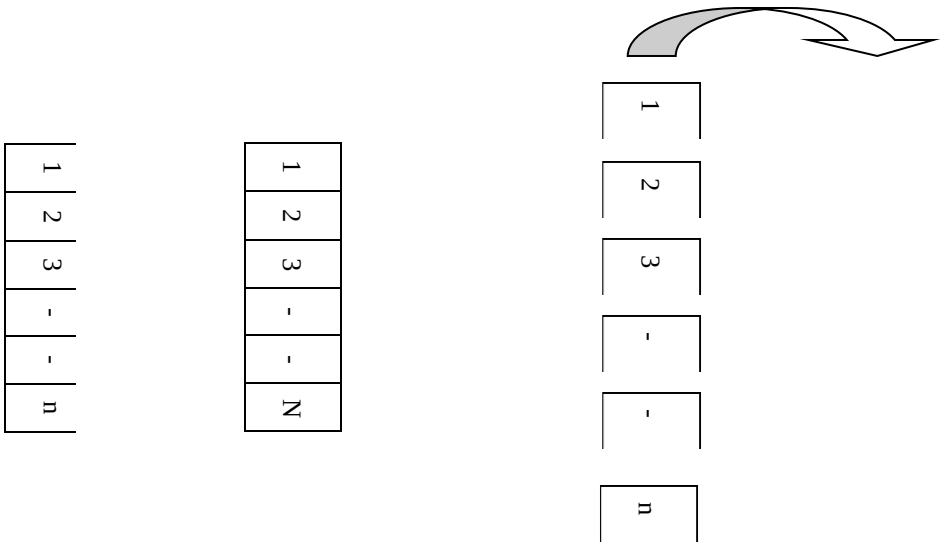
If 'n' packets are packed in a buffer, they are arranged in the following order:

1st packet will be stored at the first place in the buffer, 2nd packet will be stored at the second place, and so on.

At the front end while unpacking the buffer, the packets are to be segregated in the same order, that is, isolate each packet and process each packet as per the sequence viz- first packet first and last packet at the end.

Host End Sends Front End Receives Front end Unpacking

Process packets



Chapter 4 Logon Process

Introduction

This section describes how a user logs on to the drop copy service system for Order & Trade (O+T) or Trade(T) only feed. It covers the log-on request and the system responses. As mentioned earlier, Order-Trade and Trade only services will have separate gateway routers. User need to connect to respective gateway router for getting the required data.

The client system, after issuing a sign-on request, waits for the system response. The response could be a successful logon or an error message

User will need to connect to multiple partitions to receive data across all Market streams. Number of partitions to connect will be dynamically provided as part of Response to Logon request

User will be allowed to login concurrently multiple times (upto max value defined by Exchange) using the same User ID.

E.g An user connecting to Drop Copy system will provide User ID and ConcurrentLogin ID to login.

Drop Copy system supports multiple logins using the same User ID. To distinguish these logins, user need to specify ConcurrentLoginID along with User ID. ConcurrentLoginID will have values like 1, 2, 3 For first login, user will specify value as 1, for next value as 2 and so on to all these Partitions. Each partition ID will have specific server IP and Port. Say GR Response sent following 5 partition ID details.

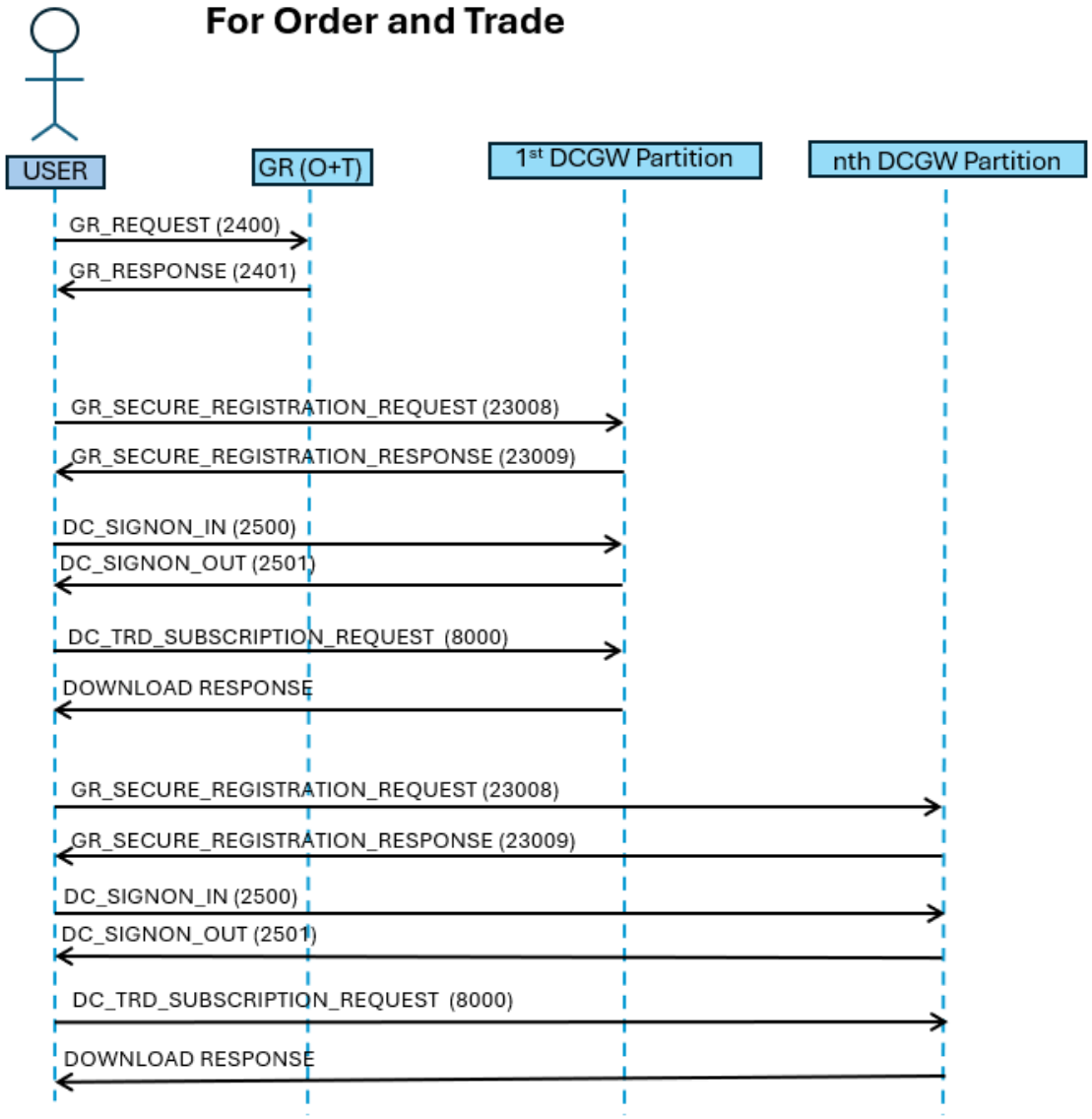
Partition ID	IP	Port
M01P01	IP1	P1
M02P03	IP2	P2
M03P05	IP3	P3
M04P04	IP4	P4
M05P01	IP5	P5

User will need to make 5 connections using IP-Port as IP1-P1, IP2-P2, IP3-P3, IP4-P4, IP5-P5 respectively. And User will need to specify values as M01P01, M02P03, M03P05 M04P04 and M05P01 for PartitionID in request header for the respective connections

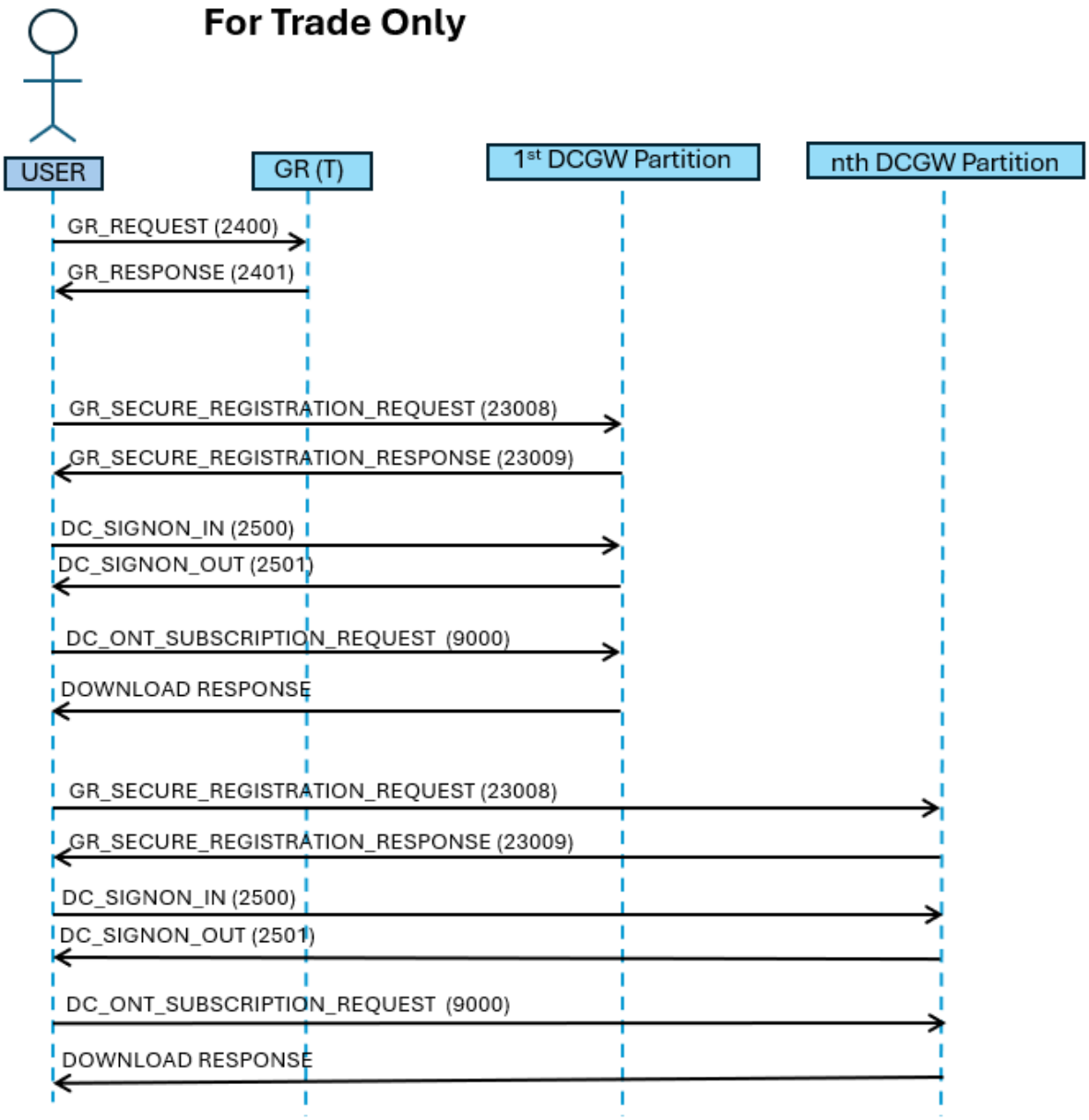
Order of Events to be followed during Logon for Drop Copy Service

The following sequence explains the order in which transaction codes are sent and received during the log-on process. The same can be seen in the diagram below.

Order of Events for Order and Trade Drop Copy



Order of Events for Trade Only Drop Copy



Note: Send the subscription request for the Order & Trade Drop Copy to the Gateway Servers specified in the GR Response received for the GR Request sent to the Order & Trade Gateway Router service. Similarly, Send the subscription request for the Trade Drop Copy to the Gateway servers specified in the GR Response received for the GR Request sent to the Trade Gateway Router service.

Seq No	Transaction Code	Sent By	Received By
1	GR_REQUEST (2400)	Client	Gateway Router (GR)
2	GR_RESPONSE (2401)	GR	Client
3	GR_SECURE_USER_REGISTRATION_REQUEST (23008)	Client	HostEnd
4	GR_SECURE_USER_REGISTRATION_RESPONSE (23009)	HostEnd	Client
5	DC_SIGNON_IN (2500)	Client	Host End
6	DC_SIGNON_OUT (2501)	Host End	Client
7	DC_TRD_SUBSCRIPTION_REQUEST (8000) / DC_ONT_SUBSCRIPTION_REQUEST (9000)	Client	Host End
8	DOWNLOAD RESPONSE (TRADE_CONFIRMATION / ORDER_RESPONSE)	Host End	Client

Logon Request & Response

1. Member to connect (TCP/IP, SSL connection) to the IP and port provided by the exchange and send the GR_REQUEST to respective GR service using OpenSSL (Version 1.1.1) library calls with TLS versions 1.3 (TLS1_3_VERSION). Refer annexure for Encryption/Decryption. Partition ID will be sent as "0" in this request
2. Exchange will send the GR_RESPONSE to the member containing array of multiple IP address and Port along with the Session key, Cryptographic key & Cryptographic IV (Initialization Vector) on SSL connection. GR will send list of IP & Ports for total number of partitions to which Member needs to subscribe to get Order / Trade data across all Market Streams. If there is any error, then ErrorCode field in MESSAGE_HEADER will be populated with relevant error code in the GR_RESPONSE.
3. Member applications will then make a new TCP connection with the allocated Gateway server (IP and port provided in the GR_RESPONSE) for each of partitions and send GR_SECURE_USER_REGISTRATION_REQUEST for each partition. Partition ID

(received in GR_RESPONSE) along with User ID and ConcurrentLoginID (sent in GR_REQUEST) is to be populated in GR_SECURE_USER_REGISTRATION_REQUEST

4. Exchange will send the GR_SECURE_USER_REGISTRATION_RESPONSE. If there is any error, then ErrorCode field in MESSAGE_HEADER will be populated with relevant error code in the GR_SECURE_USER_REGISTRATION_RESPONSE and the User connection will be terminated.
5. If there is no error in GR_SECURE_USER_REGISTRATION_RESPONSE, member should do encryption and decryption initialization to create encryption and decryption contexts (Please refer annexure). This initialization should be done only once. Once initialized, all further messages between member application and allocated Gateway server will be encrypted and decrypted using same encryption and decryption contexts respectively. Further member should send the DC_SIGNON_IN (2500). UserID and Session key (received in GR_RESPONSE) is to be populated in DC_SIGNON_IN. MD5 Algorithm to be performed on plain messages. That means, while sending the messages to Trading system, MD5 is to be performed first and then encryption. Encrypted message length + 22 (sizeof(Header)) will have to be written in first 2 bytes of header, Sequence Number in next 4 bytes and MD5 value (of plain message) will be written in last 16 bytes of Header and the header will have to be prepended to the encrypted message. This message will be sent out to Trading System. While receiving the messages from Trading System, decryption should be done first and then MD5 is to be applied on decrypted buffer. Decryption should be done on message excluding first 22 bytes of header.
6. Exchange will send the DC_SIGNON_OUT. If there is any error, then ErrorCode field in MESSAGE_HEADER will be populated with relevant error code in the DC_SIGNON_OUT and the User connection will be terminated.

Note :

1. Login of member will be for a given User ID and ConcurrentLoginID
2. List of Partition will be published to user in response (GR Response) to Logon Request (GR_Request).
3. Member can specify upto maximum three concurrent logins for same User ID (max value will be defined by Exchange from time to time).

Table 4.1 GR_REQUEST

Structure Name	GR_REQUEST		
Packet Length	24 bytes		
Transaction Code	GR_REQUEST (2400)		
Field Name	Data Type	Size in Byte	Offset
REQUEST_MESSAGE_HEADER (Refer Table No 2.2)	STRUCT	24	0

Table 4.2 IP_DETAILS_PARTION_WISE

Structure Name	IP_DETAILS_PARTITION_WISE		
Packet Length	26 bytes		
Field Name	Data Type	Size in Byte	Offset
IPAddress [16]	CHAR	16	0
Port	INT	4	16
PartitionID	CHAR	6	20

Field Name	Brief Description
IPAddress	This field contains IP address of DC Gateway.
Port	This field contains Port of DC Gateway.
PartitionID	This field contains Partition ID for which Data is being received.

Table 4.3 GR_RESPONSE

Structure Name	GR_RESPONSE		
Packet Length	1114 bytes		
Transaction Code	GR_RESPONSE (2401)		
Field Name	Data Type	Size in Byte	Offset
MESSAGE_HEADER (Refer Table No 2.4)	STRUCT	14	0
MessageIndicator	SHORT	2	14
PartitionCount	SHORT	2	16

Structure Name	GR_RESPONSE		
Packet Length	1114 bytes		
Transaction Code	GR_RESPONSE (2401)		
Field Name	**Data Type**	**Size in Byte**	**Offset**
IP_DETAILS_PARTITION_WISE [40] (Refer Table No 4.2)	CHAR	1040	18
SessionKey [8]	CHAR	8	1058
CryptographicKey [32]	CHAR	32	1066
CryptographicIV (Initialization Vector) [16]	CHAR	16	1098

Field Name	Brief Description
MessageIndicator	This field will indicate whether there is more than one response expected for the request. If number of partitions exceed 40 then there will be additional response sent for next 40 partitions. The value set in this field will be following: ⇨ 0, Interim message – Meaning there is next response following this message ⇨ 1, Last Message – This is last response to the Logon Request
PartitionCount	This field will contain count of partition details that are present in this message.
IP_DETAILS_PARTITION_WISE	This will be array of IPs and Ports for number of partitions to connect. Max 40 partition details will be specified in one message. If there are more partitions, then incremental details will be sent in subsequent response
SessionKey	This field contains Session Key for the validated session.
Cryptographic Key	Cryptographic key for both the encryption and decryption of all messages between member application and allocated Gateway Server.

Field Name	Brief Description
Cryptographic IV (Initialization Vector)	Cryptographic IV (Initialization Vector) for both the encryption and decryption of all messages between member application and allocated Gateway Server.

Secure User Registration Request

Table 4.4 GR_SECURE_USER_REGISTRATION_REQUEST

Structure Name	MS_ SECURE_USER_REGISTRATION_REQUEST_IN		
Packet Length	24 bytes		
Transaction Code	GR_SECURE_USER_REGISTRATION_REQUEST_IN (23008)		
Field Name	Data Type	Size in Byte	Offset
REQUEST MESSAGE HEADER (Refer Table 2.2 structure)	STRUCT	24	0

Field Name	Brief Description
Transcode	This field is the part of Message Header. The transaction code is 23008

Secure User Registration Response

Table 4.5 GR_SECURE_USER_REGISTRATION_RESPONSE

Structure Name	MS_ SECURE_USER_REGISTRATION_RESPONSE_OUT		
Packet Length	14 bytes		
Transaction Code	GR_SECURE_USER_REGISTRATION_RESPONSE_OUT (23009)		
Field Name	Data Type	Size in Byte	Offset
MESSAGE_HEADER (Refer Table No 2.4)	STRUCT	14	0

Field Name	Brief Description
Transcode	This field is the part of Message Header. The transaction code is 23009
ErrorCode	This field is the part of Message Header. Error Code will be set if the query is unsuccessful. *Refer to List of Error Codes in Appendix*

Table 4.6 DC_SIGNON_IN

Structure Name	DC_SIGNON IN		
Packet Length	40 bytes		
Transaction Code	DC_SIGNON_IN (2500)		
Field Name	**Data Type**	**Size in Byte**	**Offset**
REQUEST_MESSAGE_HEADER (Refer Table No 2.2)	STRUCT	24	0
Password [8]	CHAR	8	24
SessionKey [8]	CHAR	8	32

Field Name	Brief Description
TransactionCode	The transaction code is DC_SIGNON IN (2500)
Password	This field should contain the password entered by the user. A combination of alphabet, numbers and special characters are allowed in the password. The user should enter the valid password for a successful Logon. If password is less than 8-character length, the password should be padded by blank.
SessionKey	Session Key as was received in GR_RESPONSE.

Table 4.6 DC_SIGNON_OUT

Structure Name	DC_SIGNON_OUT		
Packet Length	26 bytes		
Transaction Code	DC_SIGNON_OUT (2501)		
Field Name	**Data Type**	**Size in Byte**	**Offset**
MESSAGE_HEADER (Refer Table No 2.4)	STRUCT	14	0
UserId	INT	4	14
PartitionID	CHAR	6	18
ConcurrentLoginId	SHORT	2	24

Field Name	Brief Description
TransactionCode	The transaction code is DC_SIGNON_OUT (2501) in login response
UserId	This field contains User ID of user.
Partition ID	For messages coming from the host, this field contains the partition ID(Stream) from which the packet is being sent
ConcurrentLoginID	This field contains Concurrent login number of the User for which User has logged in.

Logon Error

In case of any error, the structure returned is:

ERROR RESPONSE (Refer to Error Response in Chapter 2)

Field Name	Brief Description
TransactionCode	The transaction code is DC_SIGNON_OUT (2501).
ErrorCode	This contains the error number. Refer to List of Error Codes in Appendix.

Chapter 5 Drop Copy Message Subscription

Introduction

NSE Drop Copy Service sends the user, intended Order & Trade (O&T) or Trade only messages. For receiving these messages, the user must send the respective subscription request on the different drop copy gateway partitions. In response to this request, the Trade only or Order & Trade messages are sent to the user.

The users must send separate subscription request for each Partition. The number of partitions and their details is sent in Logon Response from host during logon sequence.

In case of any disconnection during market hours, it is recommended to make use of the incremental download facility by sending the last received sequence number in the subsequent subscription request. It is advisable to not to initiate full download again.

In case of receipt of duplicate message sequence number the message may be dropped at user end. In case of gap in sequence number, request for Drop Copy subscription to be done by the User with last received sequence number.

In case of partition level TCP disconnection or complete disconnection across partitions, user will need to initiate from Logon Request

Drop Copy Message Subscription Request

Table 5.1 DROP COPY MESSAGE SUBSCRIPTION

Structure Name	DC_SUBSCRIPTION_REQUEST		
Packet Length	32 bytes		
Transaction Code	DC_TRD_SUBSCRIPTION_REQUEST (8000) DC_ONT_SUBSCRIPTION_REQUEST (9000)		
Field Name	**Data Type**	**Size in Byte**	**Offset**
REQUEST_MESSAGE_HEADER (Refer to Table 2.2)	STRUCT	24	0
SequenceNumber	LONG LONG	8	24

Field Name	Brief Description
TransactionCode	The transaction code is DC_TRD_SUBSCRIPTION_REQUEST (8000) for Trades only subscription and DC_ONT_SUBSCRIPTION_REQUEST (9000) for Order & Trade subscription and will be part of header
SequenceNumber	This contains the last sequence number as received by the user. To retrieve the messages from the beginning of the trading day, this field should be set to '0'.

Trade Subscription

In response to DC_TRD_SUBSCRIPTION_REQUEST (8000), below mentioned message packets will be sent to users. The packets having sequence number greater than the sequence number coming in DC SUBSCRIPTION_REQUEST are only downloaded

1. Trade Confirmation Response - TRADE_CONFIRMATION (2222)
2. Trade Cancellation Confirmation Response - TRADE_CANCEL_CONFIRM (2282)
3. Trade Cancellation Rejection Response - TRADE_CANCEL_REJECT (2286)
4. Trade Modification Confirmation Response - TRADE_MODIFY_CONFIRM (2287)

The structures for the messages received on Trade Subscription can be found in the section "Message Structures"

Order & Trade (O&T) Subscription

In response to DC_ONT_SUBSCRIPTION_REQUEST (9000), below mentioned message packets will be sent to users. The packets having sequence number greater than the sequence number coming in DC SUBSCRIPTION_REQUEST are only downloaded

1. Price Confirmation Response - PRICE_CONFIRMATION (2012)
2. Order Modification Reject Response - ORDER_MOD_REJECT (2042)
3. Order Cancel Reject Response - ORDER_CANCEL_REJECT (2072)
4. Order Confirmation Response - ORDER_CONFIRMATION (2073)
5. Order Modification Confirmation Response - ORDER_MOD_CONFIRMATION (2074)
6. Order Cancel Confirmation Response - ORDER_CANCEL_CONFIRMATION (2075)
7. Freeze to Control - FREEZE_TO_CONTROL (2170)
8. On Stop Notification - ON_STOP_NOTIFICATION (2212)
9. Order Error Response - ORDER_ERROR (2231)
10. Batch Order Cancel - BATCH_ORDER_CANCEL (9002)
11. All Trade Confirmations as listed for **"Trade Confirmations"**

Message structures for Order Confirmations can be found in the section "Message Structures". Order & Trade Subscription service is available at a member or user level.

Message Structures

Below are the structures for different types of confirmations:

Table 5.2 TRADE_CONFIRMATION

Structure Name	TRADE_CONFIRMATION		
Packet Length	118 bytes		
Transaction Code	TRADE_CONFIRMATION (2222) TRADE_CANCEL_CONFIRM (2282) TRADE_CANCEL_REJECT (2286) TRADE_MODIFY_CONFIRM (2287)		
Field Name	**Data Type**	**Size in Byte**	**Offset**
MESSAGE_HEADER (Refer Table No 2.4)	STRUCT	14	0
OrderNumber	DOUBLE	8	14
TraderNumber	INT	4	22
BuySell	SHORT	2	26
OriginalVolume	INT	4	28
DisclosedVolume	INT	4	32
RemainingVolume	INT	4	38
DiclosedVolRemaining	INT	4	40
Price	INT	4	54
ST_ORDER_FLAGS	STRUCT	2	48
FillNumber	INT	4	50
FillQty	INT	4	54
FillPrice	INT	4	58
Token	INT	4	62
BookType	SHORT	2	66
ProClient	SHORT	2	68
Algo ID	INT	4	70
ActivityTimeInNanos	LONG	8	74
NNFField	DOUBLE	8	82

Structure Name	TRADE_CONFIRMATION		
Packet Length	118 bytes		
Transaction Code	TRADE_CONFIRMATION (2222) TRADE_CANCEL_CONFIRM (2282) TRADE_CANCEL_REJECT (2286) TRADE_MODIFY_CONFIRM (2287)		
Field Name	**Data Type**	**Size in Byte**	**Offset**
Segment	SHORT	2	90
BrokerId [5]	CHAR	5	92
Filler	CHAR	1	97
PAN [10]	CHAR	10	98
AccountNumber [10]	CHAR	10	108

Field Name	Brief Description
TransactionCode	The transaction code for Trade Confirmation (e.g. 2222, 2282, etc).
OrderNumber	This field contains the order number of the trader's order taking part in the trade.
BrokerId	This field contains the Trading Member ID.
TraderNumber	This field contains the trader or user ID.
AccountNumber	This field contains the Account Number or Client code.
BuySell	This field contains one of the following values based on Buy or Sell. '1' for Buy '2' for Sell.
OriginalVolume	This field contains the Original traded volume.
DisclosedVolume	This field contains the quantity to be disclosed to the market.
RemainingVol	This field contains the volume remaining after trade(s).
DisclosedVolRemaining	This field contains the disclosed volume remaining after trade(s).
Price	This field contains the order price.
OrderFlags	Refer to Table No 2.5

Field Name	Brief Description
	Note: Preopen Indicator will be set as 0 for the trades happening in Normal Market session for Normal Market orders and pre-open carried forward orders Preopen indicator will be set as 1 for trades happening in the call auction 2 market. Applicable for CM Segment only.
FillNumber	This field contains the trade number.
FillQty	This field contains the traded volume.
FillPrice	This field contains the price at which order is traded.
Token	Security identifier
BookType	This field contains the book type - RL/ ST/ SL/ NT/ OL/ SP/ AU/CA/CB.
ProClient	This field is same as Pro/Client /WHS indicator having one of the following values: '1' - client's order '2' - broker's order '4' - warehousing order Applicable for CM segment only.
PAN	This field contains the PAN (Permanent Account Number)
Algo ID	This field contains the Algo ID
ActivityTimeInNanos	Activity time in nanoseconds
NNFField	This field contains a 15 digit a unique identifier for various products deployed as per Exchange circular download ref no 16519 dated December 14, 2010 and as updated from time to time
Segment	Represents the business segment. • '1' – Equity Derivatives (F&O) • '2' – Currency Derivatives • '3' – Capital Markets (Cash Equity) • '4' – SLBM Markets • '5' – Commodity Derivatives

Table 5.4 Order Response Message

Structure Name	**ORDER_RESPONSE**		
Packet Length	**114 bytes**		
Transaction Code	**PRICE_CONFIRMATION (2012)** **ORDER_MOD_REJECT (2042)** **ORDER_CANCEL_REJECT (2072)** **ORDER_CONFIRMATION (2073)** **ORDER_MOD_CONFIRMATION (2074)** **ORDER_CANCEL_CONFIRMATION (2075)** **FREEZE_TO_CONTROL (2170)** **ON_STOP_NOTIFICATION (2212)** **ORDER_ERROR (2231)** **BATCH_ORDER_CANCEL (9002)**		
Field Name	**Data Type**	**Size in Byte**	**Offset**
MESSAGE_HEADER (Refer Table No 2.4)	STRUCT	14	0
ReasonCode	SHORT	2	14
Token	INT	4	16
OrderNumber	DOUBLE	8	20
BookType	SHORT	2	28
BuySell	SHORT	2	30
DisclosedVolume	INT	4	32
DisclosedVolRemaining	INT	4	36
TotalVolRemaining	INT	4	40
Volume	INT	4	44
Price	INT	4	48
TriggerPrice	INT	4	52
ST_ORDER_FLAGS	STRUCT	2	56
TraderId	INT	4	58
NNFField	DOUBLE	8	62
AlgoID	INT	4	70
ActivityTimeInNanos	LONG	8	74

Structure Name	ORDER_RESPONSE		
Packet Length	114 bytes		
Transaction Code	PRICE_CONFIRMATION (2012) ORDER_MOD_REJECT (2042) ORDER_CANCEL_REJECT (2072) ORDER_CONFIRMATION (2073) ORDER_MOD_CONFIRMATION (2074) ORDER_CANCEL_CONFIRMATION (2075) FREEZE_TO_CONTROL (2170) ON_STOP_NOTIFICATION (2212) ORDER_ERROR (2231) BATCH_ORDER_CANCEL (9002)		
Field Name	**Data Type**	**Size in Byte**	**Offset**
CompetitorPeriod	SHORT	2	82
SolicitorPeriod	SHORT	2	84
AuctionNumber	SHORT	2	86
Suspended	CHAR	1	88
Filler	CHAR	1	89
PAN	CHAR	10	90
Segment	CHAR	1	100
ParticipantType	CHAR	1	101
AccountNumber	CHAR	10	102
ProClient	CHAR	1	112
SettlementType	CHAR	1	113

Field Name	Brief Description
TransactionCode	The transaction code for O&T Confirmation (e.g., 2042, 2072, etc)
ParticipantType	Since only exchange can initiate the auction, this field should be set to 'I' for initiator. This should be set to 'C' for competitor order and 'S' for solicitor order.

Field Name	Brief Description
CompetitorPeriod	This field should be competitor time set by exchange at the time of initiation
SolicitorPeriod	This field should be Solicitor time set by exchange at the time of initiation
ReasonCode	This field contains the reason code for a particular order request rejection or order being frozen. This has the details regarding the error along with the error code. Refer to Reason Codes in Appendix.
Token	Instrument/token identifier
AuctionNumber	Auction number is available when initiation of auction is broadcast (Auction Status Change Broadcast). For an auction order, valid auction number should be given. For other books, this field should be set to zero. Applicable for CM Segment only.
Suspended	This field specifies whether the security is suspended or not.
OrderNumber	This field contains an Order Number assigned to the order. It is a unique identification for an order. The first two digits will contain the stream number (This will be different from the stream number for Journal Download Request-Response). The next fourteen digits will contain fourteen-digit sequence number.
AccountNumber [10]	If the order is entered on behalf of a trader, the trader account number should be specified in this field. For broker's own order, this field should be set to broker code.
BookType	This field contains the type of order. BOARD_LOT_IN_TR (20000) must have BookType 1 or 11 or 12.
BuySell	This field should specify whether the order is a buy or sell. It should take one of the following values: • '1' for Buy Order • '2' for Sell Order
DisclosedVolume	This field contains the quantity that has to be disclosed to the market. It is not applicable if the order has either the All Or None or the Immediate Or Cancel attribute set. It should not be greater than the volume of the order and not less than the Minimum Fill quantity if the Minimum Fill attribute is set. In either case, it cannot be less than the Minimum Disclosed Quantity allowed. It should be a multiple of the Regular lot
DisclosedVolRemaining	This field contains the disclosed volume remaining from the original disclosed volume after trade(s).
TotalVolRemaining	This field specifies the total quantity remaining from the original quantity after trade(s). For order entry, this field should be set to Volume. Thereafter, for every response the system will return this value.
Volume	This field represents the quantity of the order placed.

Field Name	Brief Description
Price	This field contains the price at which the order is placed. For Market orders, the price will be zero.
TriggerPrice	Applicable only for a Stop Loss order, this field provides the price at which the order is to be triggered and brought to the market. For a Stop Loss buy order, the trigger price will be less than or equal to the limit price but greater than the last traded price. For a Stop Loss sell order, the trigger price will be greater than or equal to the limit price but less than the last traded price.
Order Flags	Refer to Table No 2.5 Note: Preopen Indicator will be set as 0 for the trades happening in Normal Market session for Normal Market orders and pre-open carried forward orders Preopen indicator will be set as 1 for trades happening in the call auction 2 market. Applicable for CM Only.
Trader Id	In Request packet, this field contains the ID of the user on whose behalf order is to be modified/cancelled. This field accepts only numbers
ProClient	This field contains one of the following values based on the order entering is on behalf of the broker or a trader. • 1 represents client's order. • 2 represents broker's order. • 4 represents warehousing order
SettlementType	Settlement type can be one of the following: • 0 – representing T + 0 Settlement • 1 – representing T + 1 Settlement • 2 – representing T + 2 Settlement
NNFField	This field contains a 15 digit a unique identifier for various products deployed as per Exchange circular download ref no 16519 dated December 14, 2010 and as updated from time to time
PAN	This field shall contain the PAN (Permanent Account Number / PAN_EXEMPT) - This field shall be mandatory for all orders (client / participant / PRO orders).
AlgoID	For Algo order this field shall contain the Algo ID issued by the exchange. For Non-Algo order, this field shall be Zero (0)
TimeStamp	This filed is stamped with time at the matching engine in the Trading System.
ActivityTimeInNanos	This field contains the timestamp value in nanoseconds.
Segment	Represents the business segment.

Field Name	Brief Description
	• '1' – Equity Derivatives (F&O) • '2' – Currency Derivatives • '3' – Capital Markets (Cash Equity) • '4' – SLBM Markets • '5' – Commodity Derivatives

Drop Copy Error Response

In case any error in request, the system will reject the request and send drop copy error response message to user. The reason of rejection is given in error code field in message header.

ERROR RESPONSE (Refer to Error Response in Chapter 2)

Field Name	Brief Description
TransactionCode	The transaction code is DC_ERROR_RESPONSE (8006 / 9006).
ErrorCode	This contains the error number. Refer to List of Error Codes in Appendix section.

Appendix

List of Error Codes

Error Code ID	Error Code Value	Description of Error Code
ERR_INVALID_USER_TYPE	16001	Invalid User Type
ERR_INVALID_STREAM_ID	16002	Requested download Partition ID doesn't match with logged in Partition ID.
ERR_INVALID_SIGNON	16006	Invalid sign-on, please try again.
ERR_INVALID_BROKER_OR_BRANCH	16041	Trading Member does not exist in the system.
ERR_USER_NOT_FOUND	16042	Dealer does not exist in the system.
ERR_USER_IS_DISABLED	16134	This Dealer is disabled. Please call the Exchange.
ERR_INVALID_USER_ID	16148	Invalid Dealer ID entered.
ERR_INVALID_TRADER_ID	16154	Invalid Trader ID entered.
ERR_BROKER_NOT_ACTIVE	16285	The broker is not active.
ERR_INVALID_SEQUENCE_NO	16801	Invalid sequence number in drop copy download request.
ERR_INVALID_TRANSACTION_CODE	16802	Invalid transcode in drop copy download request.

List of Transaction Codes

Transaction Code	Code	Structure
DC_SIGNON_IN	2500	DC_SIGNON_IN
DC_SIGNON_OUT	2501	DC_SIGNON_OUT

Transaction Code	Code	Structure
GR_SECURE_USER_REGISTRATION_REQUEST	23008	GR_SECURE_USER_REGISTRATION_REQUEST
GR_SECURE_USER_REGISTRATION_RESPONSE	23009	GR_SECURE_USER_REGISTRATION_RESPONSE
DC_TRD_SUBSCRIPTION_REQUEST	8000	DC_TRD_REQUEST
DC_ONT_SUBSCRIPTION_REQUEST	9000	DC_ONT_REQUEST
DC_ERROR_RESPONSE	9006	DC_ERROR_RESPONSE (ORDER)
DC_ERROR_RESPONSE	8006	DC_ERROR_RESPONSE (TRADE)
TRADE_CONFIRMATION	2222	TRADE_CONFIRMATION
TRADE_CANCEL_CONFIRM	2282	TRADE_CONFIRMATION
TRADE_CANCEL_REJECT	2286	TRADE_CONFIRMATION
TRADE_MODIFY_CONFIRM	2287	TRADE_CONFIRMATION
ORDER_CONFIRMATION	2073	ORDER_RESPONSE
ORDER_ERROR	2231	ORDER_RESPONSE
ORDER_MOD_CONFIRMATION	2074	ORDER_RESPONSE
ORDER_MOD_REJECT	2042	ORDER_RESPONSE
ORDER_CANCEL_CONFIRMATION	2075	ORDER_RESPONSE
ORDER_CANCEL_REJECT	2072	ORDER_RESPONSE
BATCH_ORDER_CANCEL	9002	ORDER_RESPONSE
ON_STOP_NOTIFICATION	2212	ORDER_RESPONSE
PRICE_CONFIRMATION	2012	ORDER_RESPONSE

Transaction Code	Code	Structure
FREEZE_TO_CONTROL	2170	ORDER_RESPONSE

Note: If any transcode is not present in NNF document , then end user needs to drop that transcode.

List of Transaction Codes Containing Timestamp in Nanoseconds

The transaction codes that will contain timestamp in nanoseconds from 01-Jan-1980 00:00:00 are listed in following table:

Transaction Code	Code
PRICE_CONFIRMATION	2012
ORDER_MOD_REJECT	2042
ORDER_CANCEL_REJECT	2072
ORDER_CONFIRMATION	2073
ORDER_MOD_CONFIRMATION	2074
ORDER_CANCEL_CONFIRMATION	2075
FREEZE_TO_CONTROL	2170
ON_STOP_NOTIFICATION	2212
ORDER_ERROR	2231
BATCH_ORDER_CANCEL	9002
TRADE_CONFIRMATION	2222
TRADE_CANCEL_CONFIRM	2282
TRADE_CANCEL_REJECT	2286
TRADE_MODIFY_CONFIRM	2287

Note: If any transcode is not present in NNF document, then end user needs to drop that transcode.

Annexure for Encryption/Decryption

Sr. No.	The following are sample function calls of OpenSSL library in Linux (for reference)
1	***Note –*** • Openssl Library version used is OpenSSL 1.1.1. • TLS protocol version has been set to 1.3 (TLS1_3_VERSION). Following are the system library calls for TLS1.3- **SSL/TLS library initialization →** 1. **SSL_library_init**() - Initialize SSL library by registering algorithms. 2. **OpenSSL_add_all_algorithms**() - Adds all algorithms to the table (digests and ciphers) 3. **SSL_load_error_strings**() - Registers the error strings for all libcrypto and libssl error strings. 4. **SSL_CTX_new**(**TLS_client_method**()) - Create a new SSL_CTX object as framework for TLS/SSL enabled functions. 5. **SSL_CTX_set_min_proto_version**(SSL_CTX *ctx, int version) - Set the minimum protocol versions to TLS1_3_VERSION. 6. **SSL_CTX_set_max_proto_version**(SSL_CTX *ctx, int version) - Set the maximum protocol versions to TLS1_3_VERSION. **Establishing the SSL/TLS connection→** 1. **socket**(PF_INET, SOCK_STREAM, 0) - Create TCP socket. 2. **connect**(int sockfd, const struct sockaddr *addr, socklen_t addrlen) - Initiate the TCP/IP connection with server. 3. **SSL_new**(SSL_CTX *ctx) - Create new SSL connection state. 4. **SSL_set_fd**(SSL *ssl, int fd) - Attach the socket descriptor. 5. **SSL_connect**(SSL *ssl) - Perform the SSL connection. **Validating the Gateway Router server certificate →** 1. **SSL_get_peer_certificate**(const SSL *ssl) - Get the server's certificate. 2. **X509_STORE_new**() - This function returns a new X509_STORE. 3. **X509_STORE_CTX_new**() - This function returns a newly initialised X509_STORE_CTX. 4. **X509_STORE_load_locations**(X509_STORE *ctx, const char *file, const char *dir) - Configure files and directories used by a certificate store. The path of CA certificate

	(gr_ca_cert1.pem) will be used in this function. The CA certificate (gr_ca_cert1.pem) will be provided by the Exchange for validation of Gateway Router certificate. 5. **X509_STORE_CTX_init**(X509_STORE_CTX *ctx, X509_STORE *trust_store, X509 *target, STACK_OF(X509) *untrusted) - This function returns a newly initialised X509_STORE_CTX structure. 6. **X509_verify_cert**(X509_STORE_CTX *ctx) - This function builds and verify X509 certificate chain. **Send and Receive messages on SSL/TLS connection →** 1. **SSL_write**(SSL *ssl, const void *buf, int num) - Send message on SSL. 2. **SSL_read**(SSL *ssl, void *buf, int num) - Receive message from SSL.

2	**For symmetric encryption/decryption methodology –**
	
	<u>Encryption:</u>
	
	Initialization→
	void encrypt_EVP_aes_256_cbc_init(EVP_CIPHER_CTX **ctx, unsigned char *key, unsigned char *iv)
	{
	if(!(*ctx = **EVP_CIPHER_CTX_new()**))
	handleErrors();
	
	if(1 != **EVP_EncryptInit_ex**(*ctx**, EVP_aes_256_gcm()**, NULL, key, iv))
	handleErrors();
	}
	
	Encryption→
	void encrypt(EVP_CIPHER_CTX *ctx, unsigned char *plaintext, int plaintext_len, unsigned char *ciphertext, int *ciphertext_len)
	{
	int len;
	
	if(1 != **EVP_EncryptUpdate**(ctx, ciphertext, &len, plaintext, plaintext_len))
	handleErrors();
	*ciphertext_len = len;
	}

Decryption:

Initialization→

```
void decrypt_EVP_aes_256_cbc_init(EVP_CIPHER_CTX **ctx, unsigned char *key,
unsigned char *iv)
{
  if(!(*ctx = EVP_CIPHER_CTX_new()))
    handleErrors();

  if(1 != EVP_DecryptInit_ex(*ctx, EVP_aes_256_gcm(), NULL, key, iv))
    handleErrors();
}
```

Decryption→

```
int decrypt(EVP_CIPHER_CTX *ctx, unsigned char *ciphertext, int ciphertext_len,
unsigned char *plaintext, int *plaintext_len)
{
  int len;

  if(1 != EVP_DecryptUpdate(ctx, plaintext, &len, ciphertext, ciphertext_len))
    handleErrors();
  *plaintext_len = len;
}
```

Note –

- The ones highlighted in bold are OpenSSL library functions.
- plaintext is the actual message buffer.
- ciphertext is the encrypted message buffer.

FAQs

Q – What do I need to do before I try connecting directly to Drop Copy Service system?

Kindly contact Member Services Team before initiating the connectivity with **Drop Copy Service or any other** Exchange provided system.

Q – Where to connect?

Exchange shall provide a list of addresses, IP address and Port number(s). to connect to the Drop Copy service.

Q – How to connect?

Member's application must initiate a TCP socket connection to the address given by the Exchange and follow the login process as mentioned in the document.

Q – How to Logoff?

Member's application must shut down the established TCP connection(s) gracefully to log-off from Exchange Drop Copy service.

Q – What User Ids / Passwords to be used for login to drop copy?

Member should use existing NNF User ID and password, as used for login to Exchange Trading system.

Q – How to reset the password through drop copy?

Through drop copy user can't reset the password but any password change/reset done via the Exchange Trading System will be reflected in Drop Copy system. New login to drop copy service, after password reset via Trading System, should be done with the new password.

Q – With the same user id can we take simultaneously login on Interactive channel for order entry and on Drop Copy channel?

Yes. Drop copy channel is independent of the Interactive channel.

Q – What information shall be provided in the drop copy?

If only trade data API is implemented as per section 1 then following information will be sent through Drop Copy system

- Trade confirmation
- Trade modification confirmation
- Trade modification reject
- Trade cancel confirmation
- Trade cancel reject

If order and trade data API is implemented as per section 2 then following information will be sent through Drop Copy system

- Trade confirmation
- Trade modification confirmation
- Trade cancel confirmation
- Trade cancel reject
- Order confirmation
- Order modification reject
- Order modification confirmation
- Order cancel reject
- Order cancel confirmation
- Price confirmation
- Freeze to Control
- On Stop Notification
- Order error
- Batch Order cancel

Q – Will clearing member also get trade data?

Yes. All the trades related to Clearing Member will be available.

Q – How shall we know that we have received all the trades (End of Day)?

No explicit message will be sent to indicate end of messages.

Q – What happens if I login late or miss receiving some trade in the drop copy channel?

During download request user needs to specify the last received sequence number from where the messages download should start.

Q – For order and trade data how will sequence number field value in Message header be provided?

Sequence number is user wise and streamwise unique value maintained at host end. For different user types i.e. Dealer, Branch manager, Corporate manager and clearing member, sequence number is uniquely maintained for each user. Also, for different streams available at host end, sequence number value is uniquely maintained. For download request, user must send sequence number value which was received in last message from drop copy service.

Q – Will trades executed in IPO Listing / Relisting, Illiquid call auction session, block trades and trades in closing session be available in the drop copy channel?

The trades executed in the following sessions shall be available in the drop copy channel

- Pre-open
- Normal market (Continuous matching)
- Special Pre-open for IPO listing / Relisting
- Auction
- Illiquid call auction session
- Block trades
- Post close session

For trades in CALL AUCTION 2 market Book type will be set as Regular Lot Order (1)

Q – Time from which login available to the system?

Details shall be clarified through a circular.

Q – Can I connect to the drop copy channel after close of market?

Details shall be clarified through a circular.

Q – Till when I can connect to the drop copy channel?

Details shall be clarified through a circular.