Network Working Group
Request for Comments: 2351
Category: Informational

A. Robert
SITA

May 1998

Mapping of Airline Reservation, Ticketing, and Messaging Traffic over IP

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Security Disclaimer:

This document fails to adequately address security concerns. The protocol itself does not include any security mechanisms. The document notes that traffic can be authenticated based on external mechanisms that use static identifiers or what are apparently clear-text passwords, neither of which provide sound security. The document notes in general terms that traffic can be secured using IPSEC, but leaves this form of sound security strictly optional.

Abstract

This memo specifies a protocol for the encapsulation of the airline specific protocol over IP.

Table of Conents

1. Introduction

The airline community has been using a worldwide data network for over 40 years, with two main types of traffic:

Transactional traffic

This is used typically for communication between an airline office or travel agency and a central computer system for seat reservations and ticket issuing. A dumb terminal or a PC accesses the central system (IBM or UNISYS) through a data network.

This traffic is also called TYPE A and is based on real-time query/response with limited protection, high priority and can be discarded. The user can access only one predetermined central computer system. In case of no response (data loss), the user can duplicate the request.

Messaging

This is an e-mail application where real-time is not needed. However a high level of protection is required. The addressing scheme uses an international format defined by IATA and contains the city and airline codes.

This traffic is also called TYPE B and is transmitted with a high level of protection, multi-addressing and 4 levels of priority.

The detailed formats for TYPE A and TYPE B messages are defined in the IATA standards.

At the bottom level, synchronous protocols have been built since 1960’s and well before the OSI and SNA standards.

At present, there is a big number of legacy equipment installed in thousands of airline offices around the world. Many airlines do not have immediate plans to replace their terminals with more modern equipment using open standards. They are in search of more economical ways for connecting these terminals to the present reservation system.

Most airlines are willing to migrate from airline specific protocols to standardized protocols in order to benefit from the lower cost of new technologies, but the migration has been slow done to the following factors:

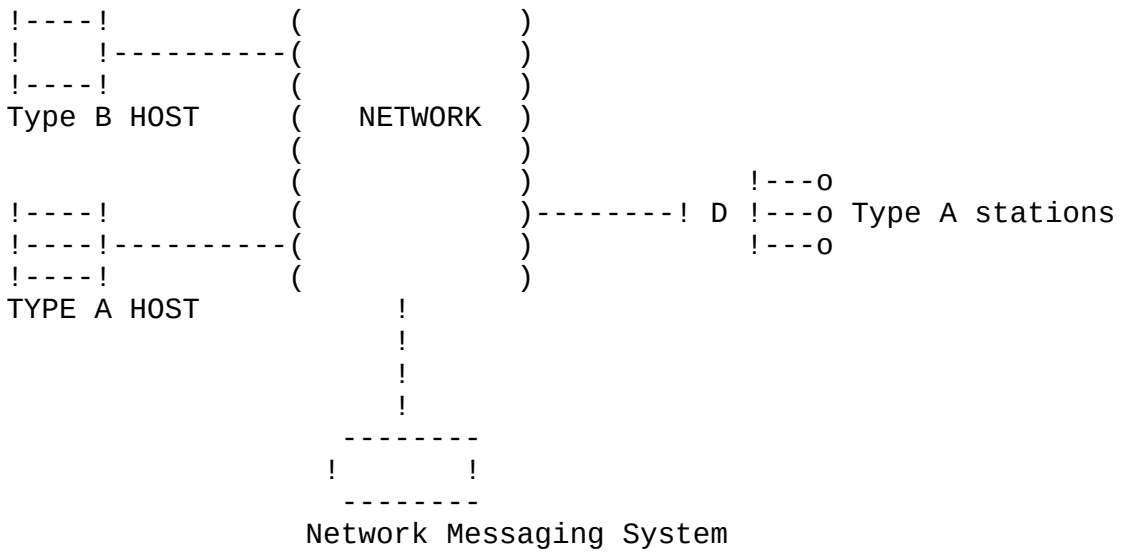
- Applications have not been migrated.
- Dumb terminals using airline protocols P1024B (IBM ALC) or P1024C (UNISYS UTS) are still numerous.

There are currently many different proprietary solutions based on gateways available to take advantage of low cast networking, but they are not scalable and cannot interact.

In the future, TCP/IP will be more commonly used as a common transport means for traffic types because:

- TCP/IP is the standard protocol of UNIX based applications
- TCP/IP stacks are inexpensive
- TCP/IP is used on intranets.

The purpose of this RFC is to define the mapping of the airline traffic types over TCP/IP. The airlines implementing it in their systems should have a TCP/IP stack to enable the traffic exchange below:



(D) : Gateway TYPE A router

The different airline traffic flows concerned by this RFC are:

- TYPE A Host / Terminal
- TYPE A Host / TYPE A host
- TYPE B Host / Network messaging System

In the case of dumb terminals, a conversion is required on the terminal side in order to have an IP connection between the host and the router. However, the IP connection is directly between the central airline host and the intelligent workstation if the latter has a direct connection to the network, a TCP/IP stack and a terminal emulation

2. Terminology & Acronyms

ALC
Airline Line Control: IBM airline specific protocol (see P1024B)

ASCII
American Standard Code for Information Interchange

ASCU
Agent Set Control Unit: Cluster at the user side.

AX.25
Airline X.25: Airline application of the X.25 OSI model (published by IATA)

BAUDOT
Alphabet defined in ITU-T Number 5. BAUDOT uses 5 bits. Padded BAUDOT uses 7 bits with the Most significant bit (bit 7) for the parity and the bit 6 equal to 1.

BATAP
Type B Application to Application Protocol. Protocol to secure the TYPE B traffic. It was specified by SITA and is now published by IATA (SCR Vol. 3)

EBCDIC
Extended Binary Coded Decimal Interchange Code

Flow ID Traffic
Flow identifier used in host to host traffic to differentiate traffic flow types.

HLD
High Level Designator: Indicates the entry or exit point of a block in the network.

IA
Interchange Address: ASCU identifier in P1024B protocol.

IATA
International Air Transport Association

IP
Internet Protocol

IPARS
International Program Airline Reservation System: IPARS code is used in ALC

HTH
Host to Host (traffic).

LSB
Least Significant Bit

MATIP
Mapping of Airline Traffic over Internet Protocol

MSB
Most Significant Bit

OC
Open Confirm (MATIP command)

OSI
Open Standard Interface

P1024B
SITA implementation of the ALC, the IBM airlines specific protocol. It uses 6-bit padded characters (IPARS) and IA/ TA for physical addressing.

P1024C
SITA implementation of the UTS, the UNISYS terminal protocol. It uses 7-bit (ASCII) characters and RID/ SID for physical addressing.

RFU
Reserved for Future Use

RID
Remote Identifier: ASCU identifier in P1024C protocol.

SC
Session Close (MATIP command)

SCR
System and Communication Reference. (IATA document)

SID
Station Identifier: Terminal identifier in P1024C protocol.

SITA
Societe International de Telecommunications Aeronautiques

SO
Session Open (MATIP command)

TA
Terminal Address: Terminal identifier in P1024B protocol.

TCP
Transport Control Protocol

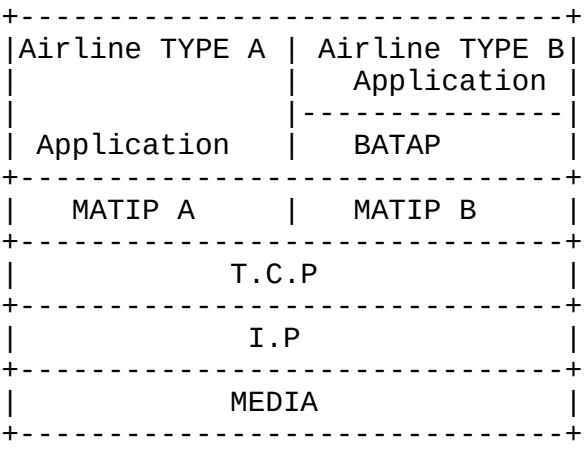
TYPE A Traffic
Interactive traffic or host to host

TYPE B Traffic
Messaging traffic in IATA compliant format with high level of reliability

UTS
Universal Terminal System by Unisys: (see P1024C)

3. LAYERING

MATIP is an end to end protocol. Its purpose is to have a mapping standard between the TCP layer and the airline application without any routing element.



4. TRAFFIC IDENTIFICATION

In TYPE A conversational traffic, the airline host application recognizes the ASCU due to 4 bytes (H1, H2, A1, A2). These bytes are assigned by the host and are unique per ASCU. Thus, a host can dynamically recognize the ASCU independent of IP address.

H1 H2 A1 A2 bytes follow one of the three cases below:

- A1,A2 only are used and H1H2 is set to 0000.
- H1,H2 identify the session and A1A2 the ASCU inside the session.
- H1,H2,A1,A2 identify the ASCU.

The first two cases are fully compatible with the AX.25 mapping where H1H2 may be equivalent to the HLD of the concentrator, i.e., 2 bytes hexadecimal. The third rule allows more flexibility but is not compatible with AX.25.

In TYPE A host to host traffic the identification field is also present and is equal to 3 bytes H1 H2 Flow ID (optional). H1H2 are reserved for remote host identification (independently of the IP address) and must be allocated bilaterally.

In Type B traffic, identification of End Systems may be carried out by the use of HLDs, or directly by the pair of IP addresses.

5. TCP PORT ALLOCATION

IANA (Internet Assigned Numbers Authority) has allocated the following ports for MATIP TYPE A and TYPE B traffic:

MATIP Type A TCP port = 350
MATIP Type B TCP port = 351

Therefore the traffic type A or B is selected according to the TCP port.

6. MATIP SESSION ESTABLISHMENT

Prior to any exchange between two applications, a single MATIP session is established above the TCP connection in order to identify the traffic characteristic such as:

- Subtype of traffic for TYPE A (Type A host to host or Type A conversational)
- Multiplexing used (for Type A)
- Data header
- Character set

A separate session and TCP connection must be established for each set of parameters (e.g., P1024B, P1024C traffic between two points needs two separate sessions).

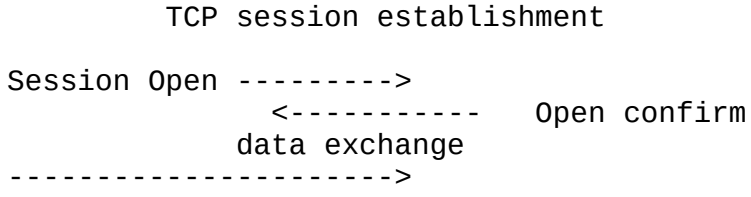
The establishment of a MATIP session can be initiated by either side. No keep-alive mechanism is defined at MATIP level. Session time out relies on the TCP time-out parameters.

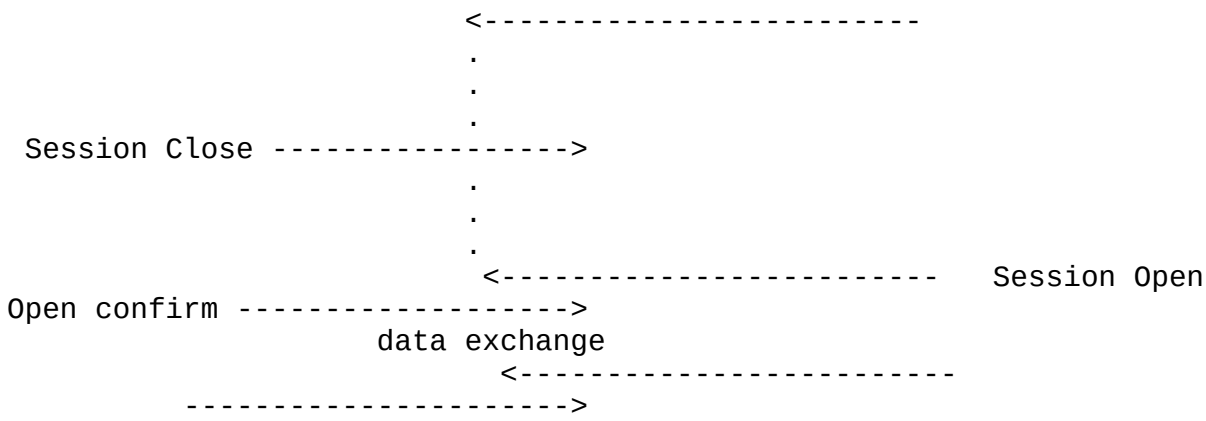
There are three commands defined to manage the MATIP session:

- Session Open (SO) to open a session.
- Open Confirm (OC) to confirm the SO command.
- Session close (SC) to close the current session.

A MATIP session can be up only if the associated TCP connection is up. However it is not mandatory to close the TCP connection when closing the associated MATIP session.

Typical exchange is:





The Session Open command may contain configuration elements. An Session Open command received on a session already opened (i.e., same IP address and port number) will automatically clear the associated configuration and a new configuration will be set up according to the information contained in the new open session command.

As illustrated above, the open and close commands are symmetrical.

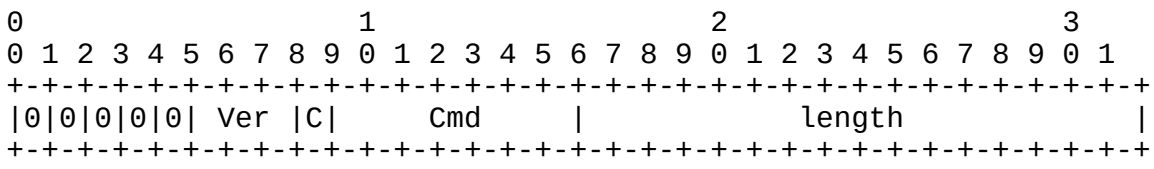
For type A conversational traffic, the SO and OC commands contain information for the identification of the ASCUs and the session. ASCUs are identified within a session by two or 4 bytes. A flag is set to indicate if the ASCU is identified by 4 bytes (H1H2A1A2) or by 2 bytes (A1A2). In the latter case, H1H2 is reserved for session identification.

The SO command is sent to open the MATIP session. In Type A conversational it may contains the list of ASCUs configured in this session.

The OC command confirms the SO command. It can refuse or accept it, totally or conditionally. In Type A, it contains the list of the ASCUs either rejected or configured in the session.

7. OVERALL PACKET FORMAT FOR TYPE A & TYPE B

The first 4 bytes of the MATIP header follow the following rules.



Ver
The ‘Ver’ (Version) field represents the version of the MATIP. It must contain the value 001 otherwise the packet is considered as invalid.

C
Identifies a CONTROL packet.
When set to 1, the packet is a Control packet
When set to 0, the packet is a Data packet

Cmd
This field identifies the control command if the flag C is set to 1.

Length
This field indicates the number of bytes of the whole packet, header included.

Notes : Fields identified as optional (Opt) are not transmitted if not used.

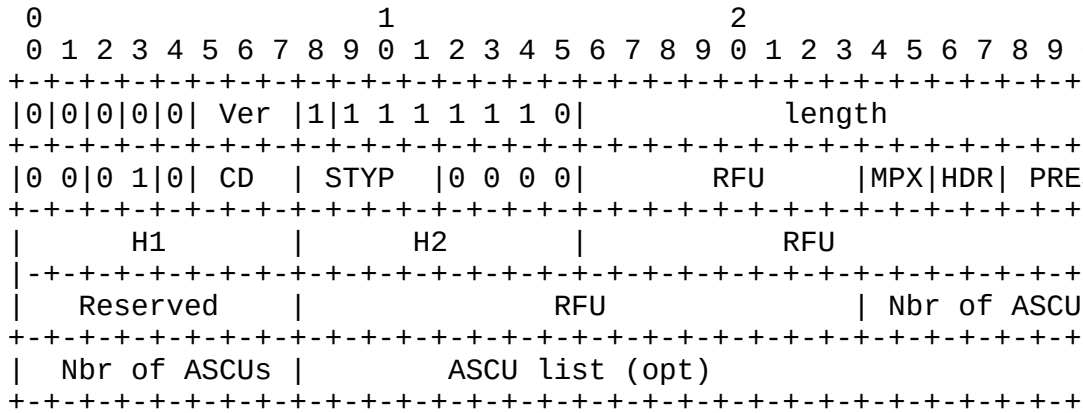
8. MATIP FORMAT FOR TYPE A CONVERSATIONAL TRAFFIC

8. 1 Control Packet Format

There are 3 control packets to open or close the session at the MATIP level.

8.1.1 Session Open format (SO)

To be able to identify the session and before sending any data packets, a Session Open command is sent. It can be initiated by either side. In case of collision, the open session from the side having the lower IP address is ignored.



RFU
Reserved for future use. Must be set to zero.

CD
This field specifies the Coding
- 000 : 5 bits (padded baudot)
- 010 : 6 bits (IPARS)
- 100 : 7 bits (ASCII)
- 110 : 8 bits (EBCDIC)
- xx1 : R.F.U

STYP
This is the traffic subtype (type being TYPE A).
- 0001 : TYPE A Conversational

MPX
This flag specifies the multiplexing used within the TCP session.
Possible values are:
- 00 : Group of ASCU with 4 bytes identification per ASCU (H1H2A1A2)
- 01 : Group of ASCUs with 2 bytes identification per ASCU (A1A2)
- 10 : single ASCU inside the TCP session.

HDR
This field specifies which part of the airline’s specific address is placed ahead of the message texts transmitted over the session.
Possible values are:
- 00 : ASCU header = H1+H2+A1+A2
- 01 : ASCU Header = A1+A2
- 10 : No Header
- 11 : Not used

The MPX and HDR must be coherent. When ASCUs are multiplexed, the data must contain the ASCU identification. The table below summarizes the allowed combinations:

MPX / HDR	00	01	10
00	Y	Y	Y
01	N	Y	Y
10	N	N	Y

PRES
This field indicates the presentation format
0001 : P1024B presentation
0010 : P1024C presentation
0011 : 3270 presentation

H1 H2
These fields can logically identify the session if MPX is not equal to 00. When this field is not used, it must be set to 0. If used in session (MPX <> 0) with HDR=00, H1H2 in data packet must have the same value as set in SO command.

Nbr of ASCUs
Nbr_of_ASCUs field is mandatory and gives the number of ASCUs per session. A 0 (zero) value means unknown. In this case the ASCU list is not present in the ‘Open Session’ command and must be sent by the other end in the ‘Open Confirm’ command.

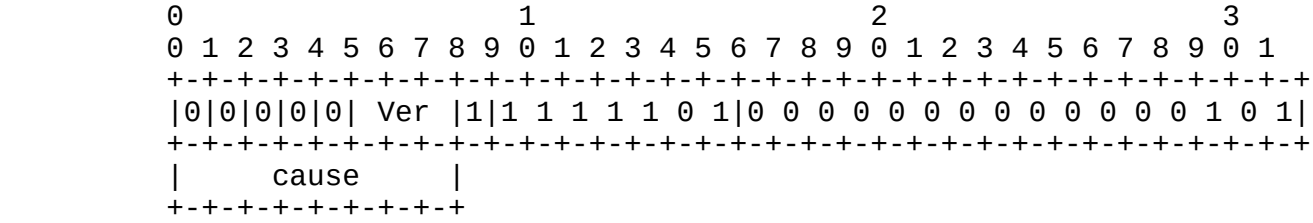
ASCU LIST
Contains the list of identifier for each ASCU. If MPX=00 it has a length of four bytes (H1H2A1A2) for each ASCU, otherwise it is two bytes (A1A2).

8.1.2 Open Confirm format (OC)

The OC (Open Confirm) command is a response to an SO (Session Open) command and is used to either refuse the session or accept it conditionally upon checking hte configuration of each ASCU.

In case of acceptance, the OC indicates the number and the address of the rejected ASCUs, if any. Alternatively, it indicates the list of ASCUs configured for that MATIP session if the list provided by the SO command was correct or the number of ASCUs configured in the session was unknown (n. of ASCU equals 0).

8.1.2.1 Refuse the connection



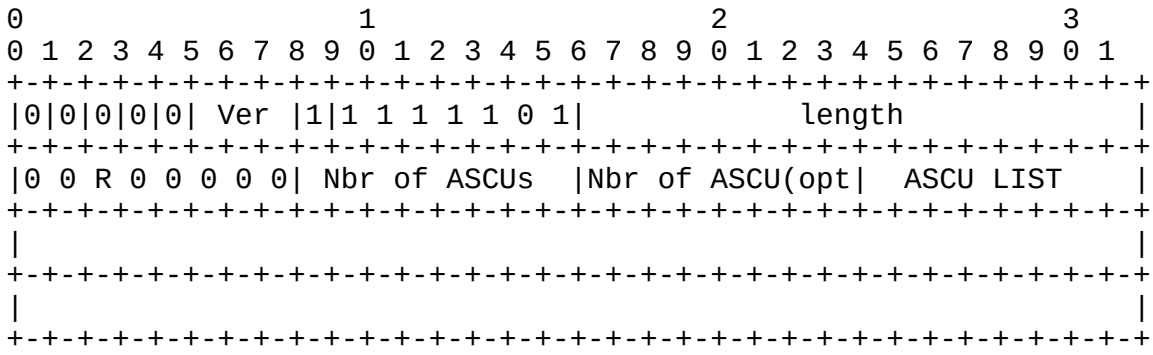
Cause
This field indicates the reason for the MATIP session refusal:

```
0 0 0 0 0 0 0 1 : No Traffic Type matching between Sender &
    Recipient
0 0 0 0 0 0 1 0 : Information in SO header incoherent

1 0 0 0 0 1 0 0
    up to       : Application dependent
1 1 1 1 1 1 1 1

Other values reserved.
```

8.1.2.2 Accept the connection



R
Flag indicating an error in the ASCU configuration provided in the SO command.

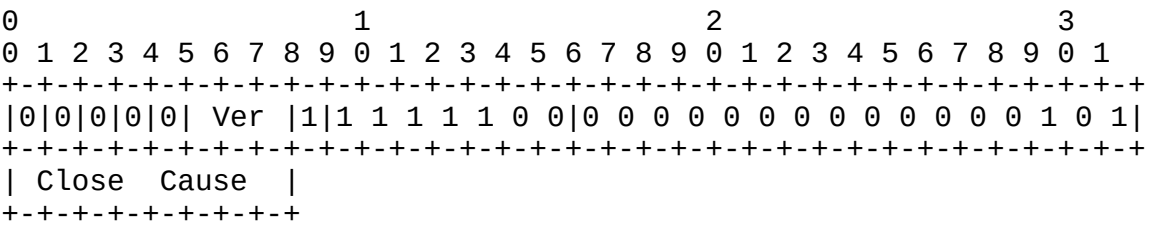
NBR of ASCUs
If the MPX value is equal to 00 in the SO command, this field is two bytes long. Otherwise, it is one byte.
If the R flag is set, the Nbr_of_ASCUs field represents the number of ASCUs in error. Otherwise, it indicates the number of ASCUs configured for that MATIP session.

Notes: The length of this field is either one or two bytes. In the SO command, the length is always two bytes. This discrepancy comes from backward compatibility with AX25 (see chapter 4). In the SO command, it is possible to use a free byte defined in the AX25 call user data. Unfortunately, there is no such free byte in the AX25 clear user data.

ASCU LIST
Depending on the R flag, this field indicates the list of ASCUs (A1A2 or H1H2A1A2) either in error or within the session.

8.1.3 Session Close (SC)

The SC (Session Close) command is used to close an existing MATIP session.



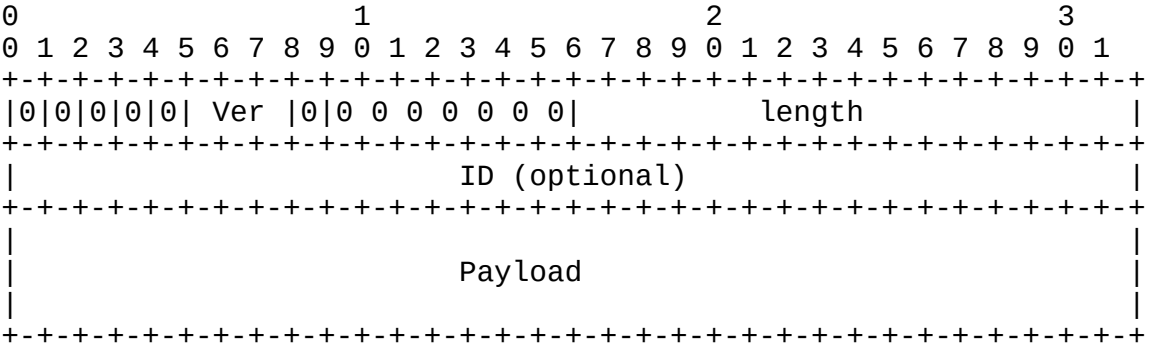
Close Cause
Indicates the reason for the session closure:

0 0 0 0 0 0 0 0 : Normal Close

1 0 0 0 0 1 0 0
up to : Application dependent
1 1 1 1 1 1 1 1

Other values reserved.

8.2 Data Packet Format



ID
This field is optional and has a different length and format according to the value of HDR, PRES indicated during the session establishment.

HDR	PRES = P1024B and 3270	PRES = P1024C
00	ID = 4 bytes H1-H2-A1-A2	ID = 5 bytes H1-H2-A1-0x01-A2
01	ID = 2 bytes A1-A2	ID = 3 bytes A1-0x01-A2
10	ID = 0 bytes	ID = 0 bytes

H1, H2 value must match the value given in the SO command if MPX is different from 0.

Payload
payload begins with the terminal identification:
- One byte Terminal identifier (TA) in P1024B
- Two bytes SID/DID Terminal identifier in P1024C.

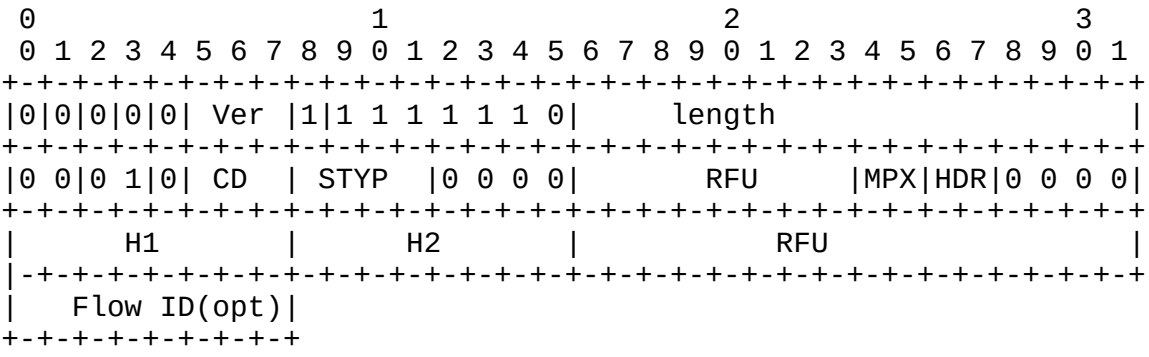
9. MATIP FORMAT FOR TYPE A HOST-TO-HOST TRAFFIC

9. 1 Control Packet Format

There are 3 control packets to open or close the session at the MATIP level.

9.1.1 Session Open format (SO)

To be able to identify the session and before sending any data packet, a Session Open command is sent. It can be initiated by either side. In case of collision, the open session from the side having the lower IP address is ignored.



RFU
Reserved for future use. Must be set to zero.

CD
This field specifies the Coding, as defined in section 8.1.1.1.

STYP
This is the traffic subtype (type being Type A).
0010 : TYPE A IATA Host to Host
1000 : SITA Host to Host

MPX
This flag specifies the multiplexing used within the MATIP session in TYPE A SITA host to host. Possible values are:

00 : irrelevant
01 : multiple flow inside the TCP connection
10 : single flow inside the TCP connection

HDR
This field specifies which part of the airline's specific address is placed ahead of the message text transmitted over the session. Possible values are:

00 : used in TYPE A SITA Host to Host Header = H1+H2+Flow ID
01 : used in TYPE A SITA Host to Host Header = Flow ID
10 : No Header (default for IATA host to Host)
11 : Not used

The MPX and HDR must be coherent. When flow are multiplexed, the data must contain the flow identification. The table below summarizes the possible combinations:

MPX / HDR	01	10
00	Y	Y
01	Y	Y
10	N	Y

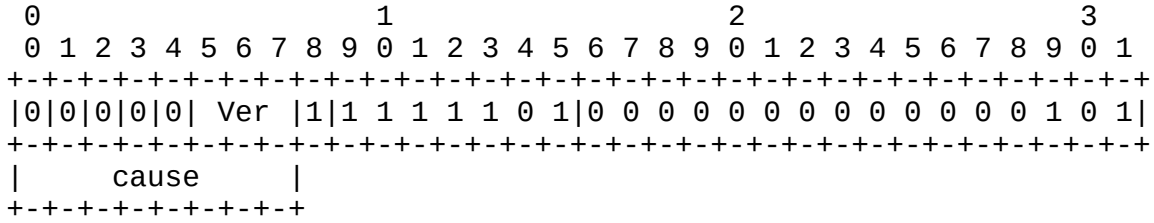
H1 H2
These fields can be used to identify the session. When this field is not used, it must be set to 0. If HDR=00, H1H2 in data packet must have the same value as set in SO command.

Flow ID
This field is optional and indicates the Flow ID (range 3F - 4F Hex).

9.1.2 Open Confirm format (OC)

The OC (Open Confirm) command is a response to an SO (Session Open) command and is used to either refuse the session or accept it.

9.1.2.1 Refuse the connection



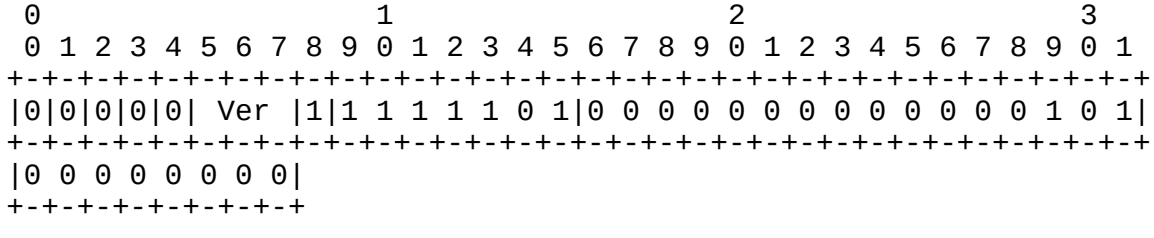
Cause
This field indicates the reason for the MATIP session refusal

0 0 0 0 0 0 0 1 : No Traffic Type matching between Sender & Recipient
0 0 0 0 0 0 1 0 : Information in SO header incoherent

1 0 0 0 0 1 0 0
up to : Application dependent
1 1 1 1 1 1 1 1

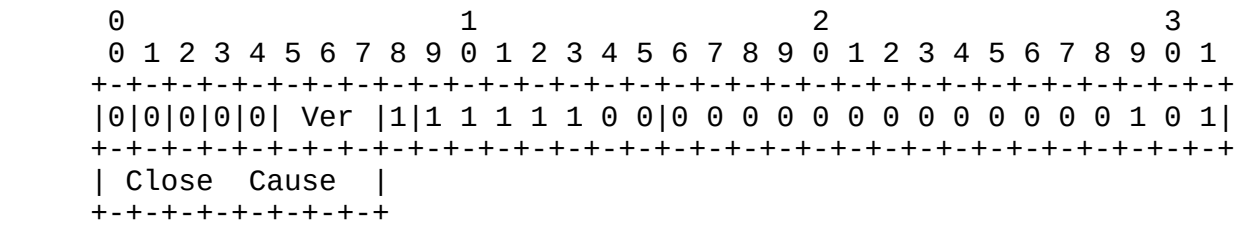
Other values reserved.

9.1.2.2 Accept the connection



9.1.3 Session Close (SC)

The SC (Session Close) command is used to close an existing MATIP session.



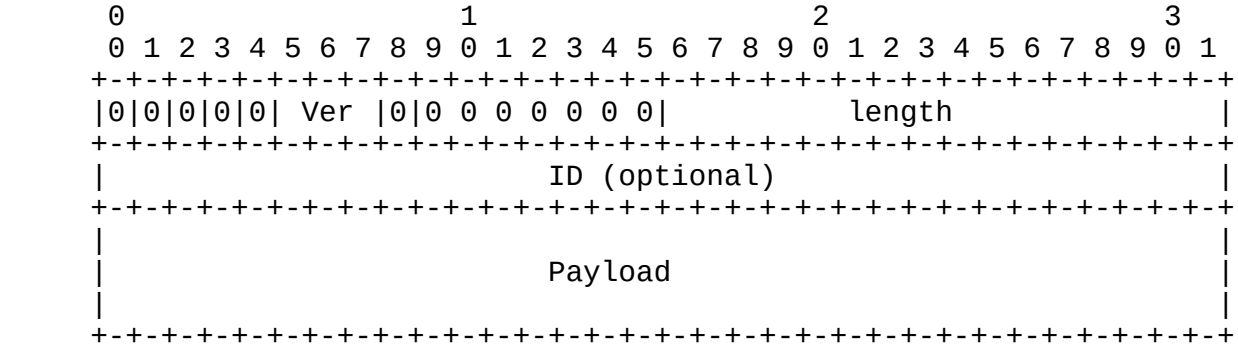
Close Cause
Indicates the reason for the session closure:

0 0 0 0 0 0 0 0 : Normal Close

1 0 0 0 0 1 0 0
up to : Application dependent
1 1 1 1 1 1 1 1

Other values reserved

9.2 Data Packet Format



ID
This field is optional and has a different length and format according to the value of HDR indicated during the session establishment.

HDR	I.D.
00	ID = 3 bytes H1-H2 FLOW ID
01	ID = FLOW ID
10	ID nor present

Payload packet
The payload format is relevant to the MATIP layer. It is formatted according to the IATA host to host specifications and agreed bilaterally by the sender and the receiver.

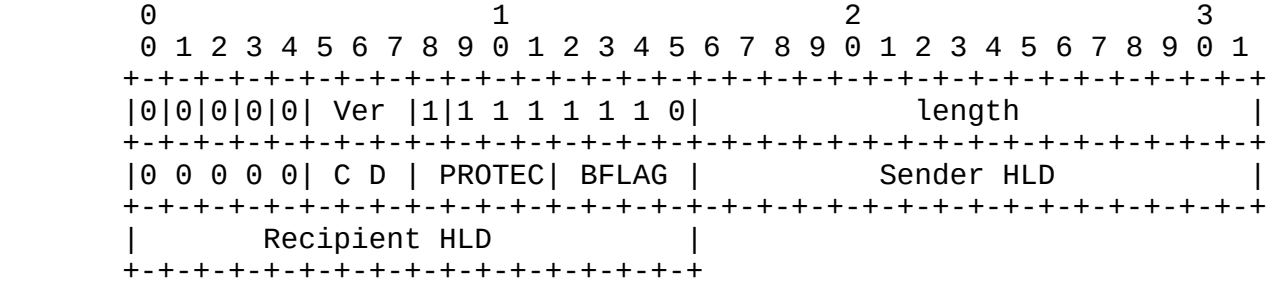
10. MATIP FORMAT FOR TYPE B TRAFFIC

10.1 Control packet format

There are 3 control packets used to open or close the session at the MATIP level for exchanging Type B data

10.1.1 Session Open format (SO)

Before sending any data packets, it is recommended to let the systems establishing a session check that they are indeed able to communicate (i.e., Both systems agree on the characteristics of the traffic that will cross the connection). For this purpose, a two way handshake, using the Session commands defined hereafter, is performed immediately after the establishment of the TCP level connection. Either side can initiate this procedure. In case of collision, the open session from the side having the lower IP address is ignored.



Length
This field indicates the number of bytes of the whole command, header included. The only possible values are equal to 6 bytes or 10 bytes.

CD
This field specifies the Coding, as defined in section 8.1.1.1.

PROTEC
Identifies the end to end Messaging Responsibility Transfer protocol used.
0010: BATAP
All other values available.

BFLAG (X means ‘do not care’

X X 0 0 means that the fields ‘Sender HLD, Recipient HLD’ do not exist in this packet. In this case, the exact length of the packet is 6 Bytes.

X X 1 0 means that the ‘Sender HLD, Recipient HLD’ are carried respectively in bytes 9,10 and 11,12 of this packet. In this case, the exact length of the packet is 10 Bytes.

0 0 X X means that the connection request has been transmitted from a host (Mainframe system)

0 1 X X means that the connection request has been transmitted from a gateway)

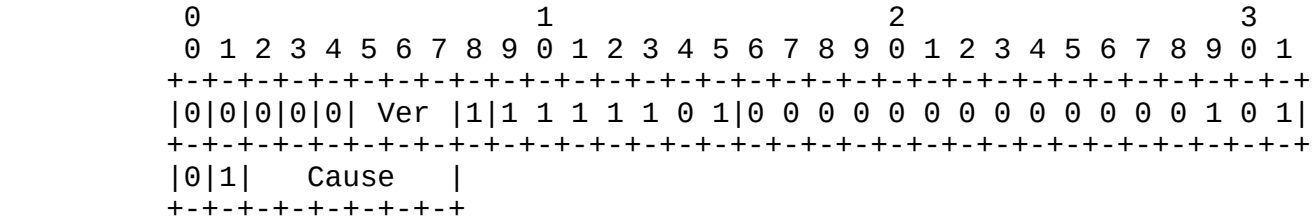
Sender HLD
HLD of the Type B System sending the Session Open.

Recipient HLD
HLD of the Type B system to which session opening is destined.

10.1.2 Open confirm format (OC)

The OC (Open Confirm) command is a response to an SO (Session Open) command and is used to either refuse the session or accept it.

10.1.2.1 Refuse the connection

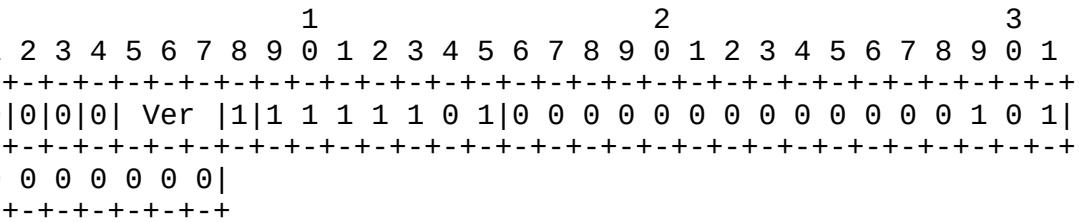


Length of this packet is 5 Bytes.

Cause
Indicates the cause of the rejection

0 0 0 0 0 1 : No Traffic Type matching between Sender & Recipient
0 0 0 0 1 0 : Information in SO header incoherent
0 0 0 0 1 1 : Type of Protection mechanism are different
0 0 0 1 0 0 up to 1 1 1 1 1 1 : R.F.U

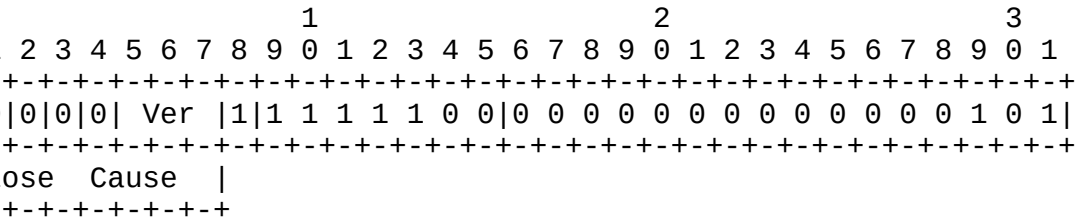
10.1.2.2 Accept the connection



Length of this packet is 5 Bytes.

10.1.3 Session Close (SC)

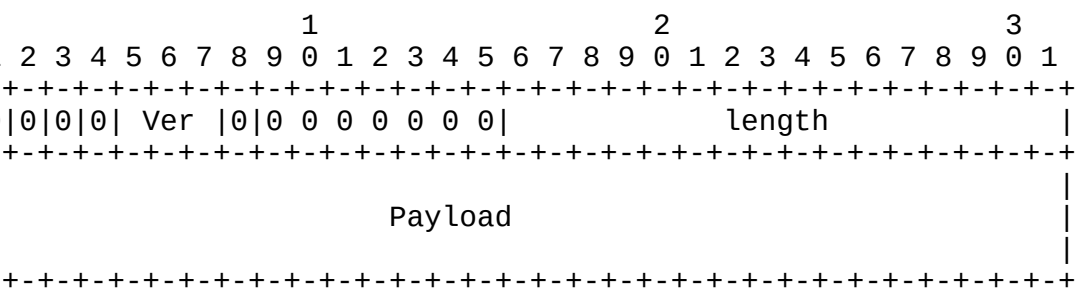
The SC (Session Close) command is used to close an existing MATIP session.



Close Cause
Indicates the reason for the session closure:
0 0 0 0 0 0 0 0 : Normal Close
1 0 0 0 0 1 0 0 up to 1 1 1 1 1 1 1 1 : Application dependent

Other values reserved

10.2 Data packet format



Length
This field indicates the number of bytes of the whole packet, header included.

Payload
Type B message formatted according to the IATA standard and conforming to the rules of the accessed TYPE B service

11. Security Considerations

The security is a very sensitive point for airline industry. Security for the MATIP users can take place at different levels:

The ASCU must be defined to enable the session with the host application. The control can be achieved in two ways: either the ASCU address (H1 H2 A1 A2) is defined at the application level by the means of a static configuration, or the ASCU is identified by a User ID / password. In most cases, the User ID and Password are verified by a dedicated software running in the central host. But they can also be checked by the application itself.

The MATIP sessions being transported over TCP/IP, It can go through a firewall. Depending on the firewall level, the control can be performed at network (IP addresses) or TCP application layer.

For higher level of security all compliant implementations MAY implement IPSEC ESP for securing control packets. Replay protection, the compulsory cipher suite for IPSEC ESP, and NULL encryption MAY be implemented. Optionally, IPSEC AH MAY also be supported. All compliant implementations MAY also implement IPSEC ESP for protection of data packets. Replay prevention and integrity protection using IPSEC ESP mandated cipher suit MAY be implemented. NULL encryption also MAY be supported. Other IPSEC ESP required ciphers MAY also be supported.

12. Author’s Address

Alain Robert
S.I.T.A.
18, rue Paul Lafargue
92904 PARIS LA DEFENSE 10
FRANCE

Phone: 33 1 46411491
Fax: 33 1 46411277
EMail: arobert@par1.par.sita.int

13. Full Copyright Statement