Frame Relay Operations, Administration, and Maintenance Implementation Agreement

FRF.19

Frame Relay Forum Technical Committee
March 2001

This page is intentionally left blank.

Note: The user's attention is called to the possibility that implementation of the frame relay implementation agreement contained herein may require the use of inventions covered by patent rights held by third parties. By publication of this frame relay implementation agreement, the Frame Relay Forum makes no representation that the implementation of the specification will not infringe on any third party rights. The Frame Relay Forum takes no position with respect to any claim that has been or may be asserted by any third party, the validity of any patent rights related to any such claims, or the extent to which a license to use any such rights may not be available.

Editor:

Timothy Mangan
Sync Research
26 Angela Street
Canton, MA 02021 USA
Phone: +1 781 492-0403
Email: tmangan@softricity.com

For more information contact:

The Frame Relay Forum
Suite 307
39355 California Street
Fremont, CA 94538 USA

Phone: +1 (510) 608-5920
FAX: +1 (510) 608-5917
E-Mail: frf@frforum.com

This page is intentionally left blank.

Table of Contents

List of Tables

List of Figures

Revision History

Version	Change	Date
FRF.OA&M	Document Approved	March, 2001

1 Introduction

1.1 Purpose

This document is an Operations, Administration, and Maintenance (OA&M) Protocol and Procedures Implementation Agreement for a Frame Relay Service. The agreements herein were reached in the Frame Relay Forum, and are based on, and enhance, the relevant frame relay standards referenced in section 1.4. This Implementation Agreement (IA) documents agreements reached among vendors and suppliers of frame relay products and services.

This IA provides a means to Test, Diagnose, and Measure the quality of, Frame Relay Services. This OA&M protocol and procedures document is designed to either supplement, or replace, I.620 [5]. Interoperability with I.610 [4] is beyond the scope of this IA.

Interoperability with other OA&M protocols is beyond the scope of this IA. Specifically, interoperation with ATM equipment in the case of Service Interworking is left for further study.

1.1.1 Overview

This document is divided into the following sections:

- Section 2. A reference model for measurement.
- Section 3. A protocol (message formats) for managing Virtual Circuits, in whole or in sections.
- Section 4. Procedures for using this protocol, especially in application to FRF.13 [14].
- Several Annexes. Informative text to aid interoperability.

The protocol and procedures may be used for Public and Private Frame Relay Networks by Service Providers and/or End-users. It is applicable to PVCs, as well as to the data transfer phase of SVCs.

1.2 Definitions

The following terms, when used in this document and highlighted in **bold**, are used as defined in this section:

- **Must**, **Shall**, or **Mandatory** - the item is an absolute requirement of this implementation agreement.
- **Should** - the item is highly desirable.
- **May** or **Optional** - the item is not compulsory, and may be followed or ignored according to the needs of the implementation.
- **Not Applicable** - the item is outside the scope of this implementation agreement.

1.3 Acronym List

AESA	ATM End System Address
ATM	Asynchronous Transfer Mode
BECN	Backward Explicit Congestion Notification
CIR	Committed Information Rate
DCE	Data Circuit-terminating Equipment
DDR	Data Delivery Ratio
DE	Discard Eligibility
DLCI	Data Link Connection Identifier
DTE	Data Terminal Equipment
FDR	Frame Delivery Ratio
FECN	Forward Explicit Congestion Notification
FR	Frame Relay
FROMP	Frame Relay OA&M Maintenance Point
FTD	Frame Transfer Delay
IA	Implementation Agreement
IEEE	Institute of Electrical and Electronics Engineers
I.F.	Information Field
IPv4	Internet Protocol Version 4
ITU	International Telecommunication Union
MTU	Maximum Transmission Unit
NLPID	Network Layer Protocol Identification
NNI	Network to Network Interface
OA&M	Operations, Administration, and Maintenance
OUI	Organizationally Unique Identifier
PHY	Physical Interface
PVC	Permanent Virtual Circuit
SLA	Service Level Agreement
SVC	Switched Virtual Circuit
UNI	User to Network Interface
VC	Virtual Circuit
xDR	Frame or Data Delivery Ratio (as appropriate)

1.4 Terminology

The following terms, when used in this IA, are used as defined in FRF.13:

- Frame Transfer Delay
- Frame Delivery Ratio
- Data Delivery Ratio
- Frames_offered
- Frames_received
- Data_offered
- Data_received
- Availability

1.5 Relevant Standards

The following is a list of standards on which these implementation agreements are based:

[1] E.164 ITU-T. *Recommendation E.164/I.331 (1997), The international public telecommunication numbering plan.*

[2] I.370 ITU-T. *Recommendation I.370 (1991), Congestion management for the ISDN frame relaying bearer service.*

[3] I.555 ITU-T. *Recommendation I.555 (1997), Frame Relaying Bearer Service interworking.*

[4] I.610 ITU-T. *Recommendation I.610 (1999) B-ISDN operation and maintenance principles and functions.*

[5] I.620 ITU-T. *Recommendation I.620 (1996) Frame relay operation and maintenance principles and functions.*

[6] X.36 ITU-T. *Recommendation X.36 (2000), Interface between Data Terminal Equipment (DTE) and Data circuit-terminating Equipment for public data networks providing frame relay data transmission service by dedicated circuit.*

[7] X.76 ITU-T. *Recommendation X.76 (2000), Network-to-network interface between public data networks providing the frame relay data transmission service.*

[8] X.121 ITU-T. *Recommendation X.121 (1996), International numbering plan for public data networks.*

[9] Q.922 ITU-T. *Recommendation Q.922 (1992), ISDN Data Link Layer Specification for Frame Mode Bearer Services.*

[10] Q.933 ITU-T. *Recommendation Q.933 (1995), ISDN Digital Signaling Specification no. 1 (DSS 1) signalling specifications for Frame Mode Switched and Permanent Virtual Connection Control and Status Monitoring.*

[11] FRF.3.2 Frame Relay Forum. *Multiprotocol Encapsulation Implementation Agreement*, April 2000.

[12] FRF 8.1 Frame Relay Forum. *Frame Relay / ATM PVC Service Interworking Implementation Agreement*, February 2000.

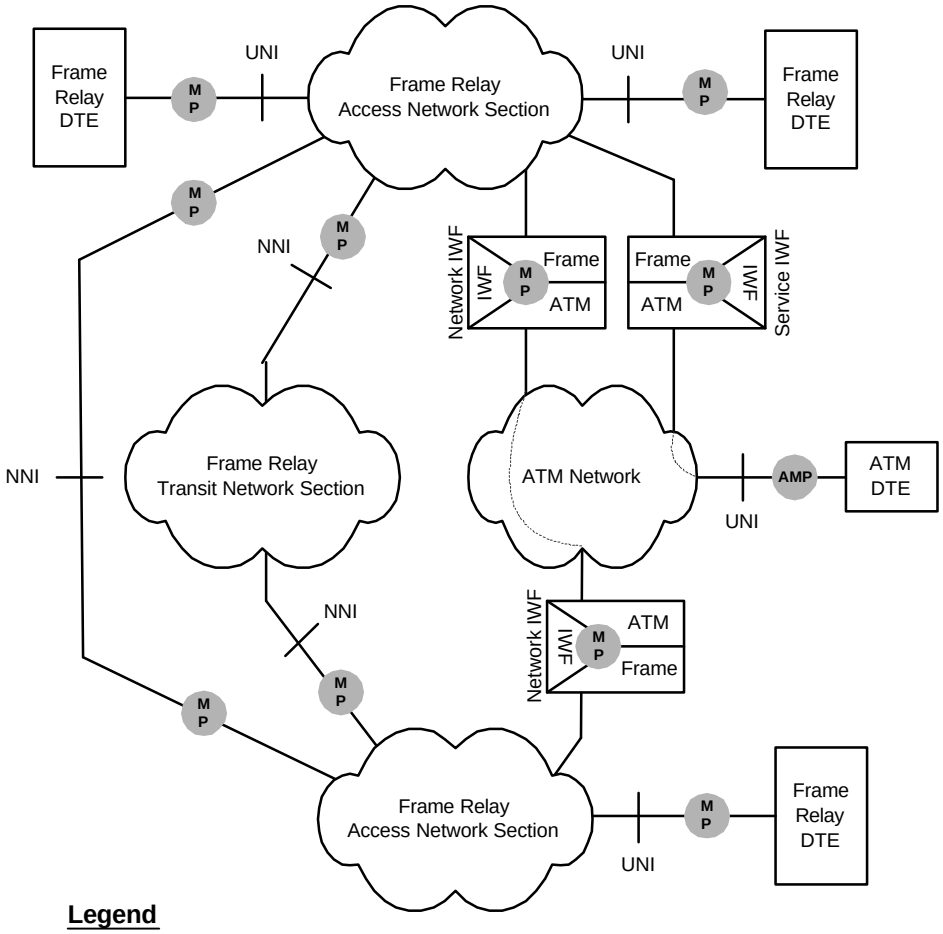
[13] FRF.11 Frame Relay Forum. *Voice Over Frame Relay Implementation Agreement*, May, 1997.

[14] FRF.13 Frame Relay Forum. *Service Level Definitions Implementation Agreement*, November 1998.

2 Reference Model

Figure 1 illustrates a reference Frame Relay Network that is interworking with an ATM network. A number of example monitoring points are indicated. In this reference network, the following examples of circuit connections may be indicated:

- A VC that spans a single FR Access Network Section.
- A VC that spans two FR Access Network Sections connected by an NNI.
- A VC that spans two FR Access Network Sections connected by a FR Transit Network.
- A VC that spans two FR Access Network Sections connected by an ATM Transit Network Section using Network Interworking.
- A FR Circuit that spans a single FR Access Network Section but is terminated as an ATM Circuit using Service Interworking.



Legend

MP Example Monitor Point for optional Frame Relay OA&M maintenance device (FROMP).

AMP Example Monitor Point for optional ATM OA&M device.

Note: Monitoring points may be external probes or embedded in DTE or DCE equipment.
Note: AMP shown for reference to ATM OA&M function. Coexistence with this function is not precluded by this IA. Interoperability with this function is beyond the scope of this IA and is shown for reference only.

Figure 1 – Network Reference Model

FRF.13 provides a reference model for an individual Virtual Circuit. Figure 2 below overlays Frame Relay OA&M Maintenance Points (FROMPS) for verification of various types of Service Level Agreements.

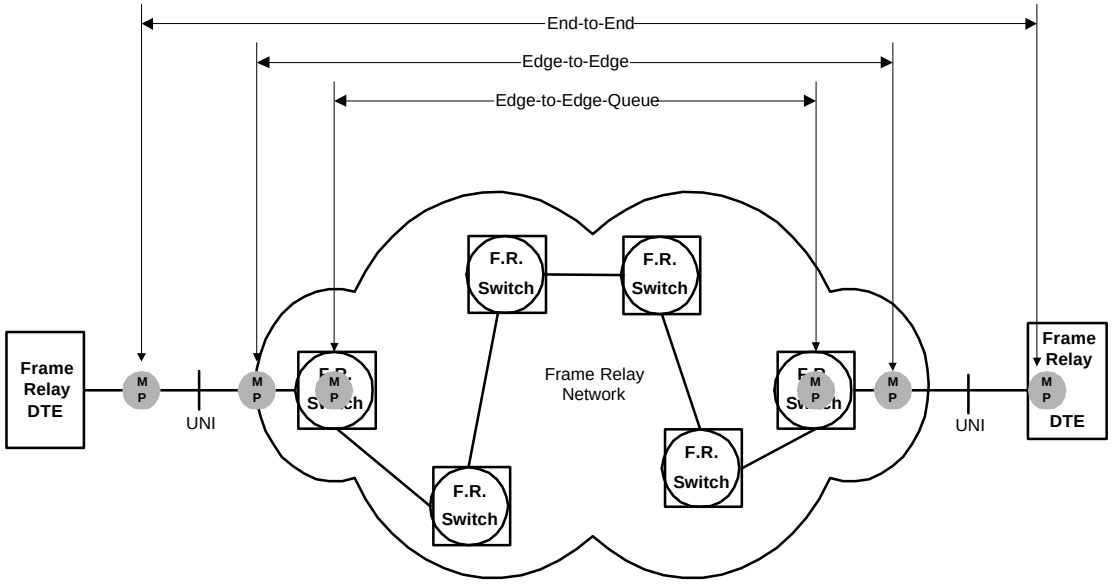


Figure 2 - Relationship with FRF.13

A VC may consist of several sections and components administered by multiple organizations. The portions of a VC that are administered by the same organization(s) create an *Administrative Domain*. Figure 3 presents the Administrative Domain Reference Model.

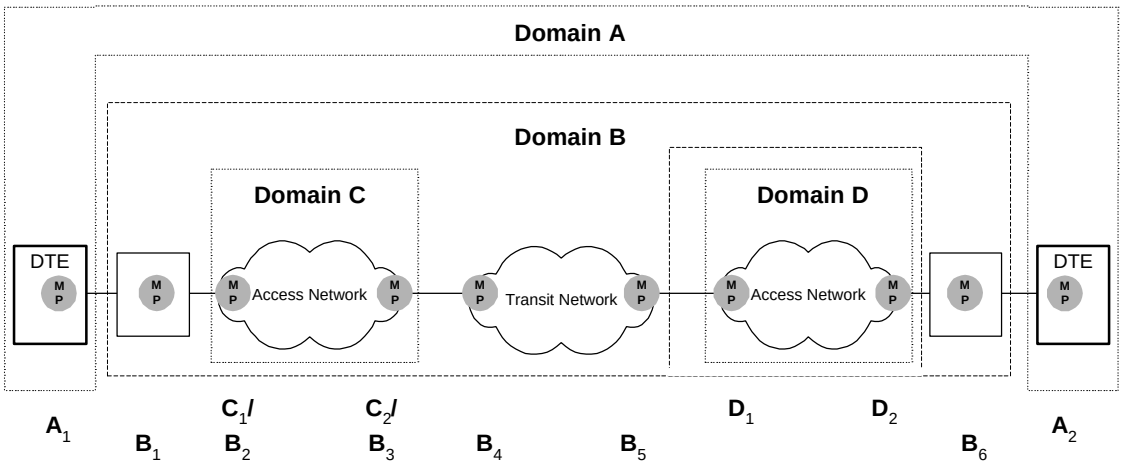


Figure 3 – Administrative Domain Reference Model

Four different and overlapping types of administrative domains are illustrated in this model. An Administrative Domain may consist of any arbitrary collection of locations on the Virtual Circuit.

Domain A – Set of interfaces and devices administered by the end-user (locations A1 and A2).

Domain B – Set of interfaces and devices administered by a global service provider working with local partners in each region (locations B1, B2, B3, B4, B5, and B6).

Domain C – Set of interfaces and devices administered by a local partner of the global service provider (locations C1 and C2). A network partner has granted the global service provider permission to interrogate OA&M devices operated by the local partner. This permission is reflected in multiple domain memberships (C1/B2 and C2/B3).

Domain D – Set of interfaces and devices controlled by a local partner of the global service provider (locations D1 and D2). The partner has refused to grant the global service provider permission to interrogate OA&M devices operated by the local partner.

Administrative Domains provide well-defined zones for OA&M messaging. At the outermost points of an administrative domain on a given VC (see Figure 3 points B1 and B6 for domain B), an *Administrative Boundary* exists to delineate the domain. All OA&M messages include a *Domain Identification*, which is used to identify the intended administrative domain.

A FROMP at a domain boundary of a VC's administrative domain prevents messages intended for the domain from being forwarded beyond the domain boundary. As an example, location D2 does not send an OA&M message with a domain identification for domain D towards B6.

Further, these boundary devices detect and discard counterfeit messages originating outside the administrative domain. Thus, if a rogue application at location B5 creates a message claiming to have domain identification D and sends the message to D1, D1 will discard the message to prevent an illegal OA&M request from entering the domain.

Messages for other domains **must** be passed through the domain boundary in either direction without interpretation or discard. As an example, location A1 transmits a message towards location A2. Location B1, a boundary device for Domain B, checks the administrative domain identification and verifies that the message does not claim to originate from within Domain B. The message is then forwarded onward to locations C1 and D1 where the same boundary checks are made. The message is then forwarded onward to location A2, the target of the message.

Messages received from within a domain are trusted. As an example, location B1 in Domain B trusts messages from direction C1 with the domain identification for domain B because they share a common administrative domain.

3 OA&M Protocol Formats

Frame Relay OA&M messages are carried in standard Frame Relay frames. Two encapsulation formats for the data portion of these Frame Relay frames are defined to allow for interoperability with other traffic. The messages consist of a header portion, and one or more information fields.

The remainder of this section describes the format of Frame Relay OA&M Protocol messages, and consists of three portions:

- An encapsulation format (section 3.1)
- An OA&M message (section 3.2) containing one or more
- OA&M Information Fields (section 3.3)

Note: See section 4.1 for rules on encoding and decoding these formats. Figures throughout this IA illustrate 2-octet DLCI encoding. Both 2- and 4-octet addresses are supported in all cases.

3.1 Encapsulation Formats

The Frame Relay OA&M Protocol supports two encapsulation formats. These formats allow for implementation in a variety of network elements and for compatibility with U-plane traffic formats.

Implementations **must** support the Multiprotocol Encapsulation format to be compliant with this IA. Implementations **may** optionally support the Non-UI encapsulations.

3.1.1 Multiprotocol Encapsulation

The Multiprotocol encapsulation format is compatible with Frame Relay equipment and applications. The format uses a NLPID (0xB2) to distinguish OA&M traffic from U-plane traffic conforming to FRF.3.2 [11], FRF.11 [13], and FRF 8.1 traffic. Figure 4 depicts the multiprotocol encapsulation format when a Q.922 Annex A [9] 2-octet header is used.

Bits								
8	7	6	5	4	3	2	1	Octet
x	x	x	x	x	x	0	0	1
DLCI (msb)						C/R	EA	
x	x	x	x	x	x	x	1	2
DLCI (lsb)				FECN	BECN	DE	EA	
0	0	0	0	0	0	1	1	3
Control								(Note 1)
1	0	1	1	0	0	1	0	4
NLPID								
FR_OAM Message								5

Note 1: Control is at octet 5 when 4-octet addressing of Q.922 Annex A is used**.**

Figure 4 - Multiprotocol Encapsulation Format

3.1.2 Non-UI Encapsulation

The non-UI encapsulation format is designed for use with Frame Relay traffic that is not distinguishable from the OA&M multiprotocol encapsulation format. The prime example of this is I.555 [3] section 5 (X.25 encapsulated) traffic. Figure 5 depicts the non-UI encapsulation format when a Q.922 Annex A 2-octet header is used.

Bits								
8	7	6	5	4	3	2	1	Octet
x	x	x	x	x	x	0	0	1
DLCI (msb)						C/R	EA	
x	x	x	x	x	x	x	1	2
DLCI (lsb)				FECN	BECN	DE	EA	
0	0	0	0	0	0	1	0	3 (Note 1)
Control								
1	0	1	1	0	0	1	0	4
NLPID								
FR_OAM Message								5

Note 1: Control is at octet 5 when 4-octet addressing of Q.922 Annex A is used.

Figure 5 - Non-UI Encapsulation Format

3.2 OA&M Message Format

Figure 6 depicts the format of OA&M messages.

Bits								
8	7	6	5	4	3	2	1	Octet
Message Type (Ref: 3.2.1)								N+1 (Note 1)
Domain Identification (Ref: 3.2.2)								N+2
Source Location Identifier (Ref 3.2.3)								N+7
Destination Location Identifier (Ref 3.2.4)								N+11
Information Field 1 (Ref 3.2.5)								N+15
Information Field x								N+m (Note 2)

Note 1: Offset N is 4, 6, or 10, depending upon encapsulation and address size used.

Note 2: Information fields are populated as needed.

Figure 6 - OA&M Message Format

3.2.1 Message Type Field

The purpose of the Message Type field is to identify the message being sent. Values for this field are shown in Table 1 below:

Message Type Value	Usage
0x1	Hello (see section 4.3 for usage)
0x2	Service Verification (see section 4.4 for usage)
0x3	Non-Latching Loopback (see section 4.5)
0x4	Latching Loopback (see section 4.6)
0x5	Diagnostic Indication (see section 4.7)

Table 1 - OA&M Message Type Values

3.2.2 Domain Identification

The purpose of the Domain Identification field is to uniquely identify the Administrative Domain to which this message belongs. This field consists of two parts, a 1-octet descriptor for the type of plan, shown in Table 2 below, followed by a 4-octet domain identifier.

Domain Identification Plan Value	Usage
0x00	Reserved for future use
0x01	User Defined Identifier
0x02	OUI Identifier
0x03	IPv4 Network Identifier
0x31	X.121 [8] Identifier
0x33	E.164 [1] Identifier
0xFF	Private Domain Identifier

Notes:

- User Defined Identifiers are for use by End-User administered equipment.
- OUI, IPv4, X.121, and E.164 Identifiers are for use by Service Providers.
- Private Domain Identifiers are for use via multi-lateral agreement.

Table 2 - Domain Identification Plan

The Domain Identification field (the combined values of the type of plan and domain identifier) **must** be unique for each administration along the path of a VC.

The format of the 4-octet domain identifier is dependent upon the value of the Domain Identification plan.

3.2.2.1 Domain Identifier Format for “User Defined “ Plan

The "User Defined" Plan is intended for use by Customer Administered equipment. When the Domain Identification Plan indicates usage of the User Defined Identifier, the format of the remaining 4 octets is not subject to standardization. A value of zero **may** be used as the default value to indicate the last OA&M capable device on the VC.

3.2.2.2 Domain Identifier Format for "OUI" Plan

The "OUI" Plan is one of several plans intended for use by Service Providers. When the Domain Identification Plan indicates usage of the OUI Identifier, the format of the remaining 4 octets is created by using a zero byte followed by a 3-octet OUI. OUI Identifiers are assigned and administered by the IEEE.

3.2.2.3 Domain Identifier for "IPv4 Network" Plan

The "IPv4" Plan is also intended for use by Service Providers. When the Domain Identification Plan indicates usage of the IPv4 Identifier, the format of the remaining 4 octets is the network portion of a public IPv4 address block owned by the service provider. Public IPv4 addresses are administered by the IETF.

3.2.2.4 Domain Identifier format for “X.121” Plan

The "X.121" Plan is also intended for use by Service Providers. When the Domain Identification Plan indicates usage of the X.121 Identifier, the value of the remaining 4 octets are created as follows:

- Take X.121 DNIC, as defined in X.76 [7].
- Pad on the left with zeros, as necessary, to 8 octets.
- BCD encode the result into 4 octets.

3.2.2.5 Domain Identifier Format for “E.164” Plan

The "E.164" Plan is also intended for use by Service Providers. When the Domain Identification Plan indicates usage of the E.164 Identifier, the value of the remaining 4 octets are created as follows:

- Take E.164 Network Identification Field of the Transit Network ID, as defined in X.76.
- Pad on the left with zeros, if necessary, to 8 octets.
- BCD encode the result into 4 octets.

3.2.2.6 Domain Identifier Format for "Private" Plan

When the Domain Identification Plan indicates usage of the Private Domain Identifier, the format of the remaining 4 octets is not subject to standardization.

3.2.3 Source Location Identifier Field

The purpose of the Source Location Identifier Field is to uniquely identify the source of an OA&M message with the indicated Administrative Domain.

The values used in the Source Location Identifier field **must** be unique for each administration along the path of a VC. The value of all ones is reserved and **may not** be used as a Source Location Identifier.

The format of this 4-octet field is not subject to standardization.

3.2.4 Destination Location Identifier Field

The purpose of the Destination Location Identifier Field is to uniquely identify the destination of an OA&M message with the indicated Administrative Domain, or to indicate a Broadcast Destination.

The values used in the Destination Location Identifier field **must** be unique for each administration along the path of a VC. The value of all ones is used to indicate the global (all destinations) broadcast for the identified administration.

The format of this 4-octet field is not subject to standardization.

3.2.5 OA&M Information Field Format

OA&M information fields are self identifying type-length-data entities. Figure 7 depicts the general format of an information field. Each type of information field will be defined in subsequent sections.

Bits								
8	7	6	5	4	3	2	1	Octet
I.F. Type (Note 1)								1
Length (Note 2)								2
Data								3

Note 1: Information Field Type values are defined in section 3.2.5.1.
Note 2: Length includes Type, Length, and Data sub-fields.

Figure 7 - OA&M Information Field Format

3.2.5.1 I.F. Type Field Values

The values for the I.F. Type field of the OA&M Information Field are defined in Table 3 below:

Information Field Type Value	Usage	Reference Section
0x01	Capabilities	Section 3.3.1.1
0x02	Frame Transfer Delay	Section 3.3.1.2
0x03	Frame Transfer Delay Results	Section 3.3.1.3
0x04	Frame Delivery Ratio Sync	Section 3.3.1.4
0x05	Frame Delivery Ratio Results	Section 3.3.1.5
0x06	Data Delivery Ratio Sync	Section 3.3.1.6
0x07	Data Delivery Ratio Results	Section 3.3.1.7
0x08	Non-Latching Loopback	Section 3.3.1.8
0x09	Latching Loopback	Section 3.3.1.9
0x0A	Diagnostic Indication	Section 3.3.1.10
0xB	Full Source Address	Section 3.3.1.11
0xFE	Opaque	Section 3.3.1.12
0xFF	Pad	Section 3.3.1.13

Table 3 - Information Field Type Values

3.2.5.2 Information Field Length

The Length field of an Information Field includes the Type, Length, and Data Fields. The value of this field **must** be in the range of 2 through 255 inclusive.

3.3 OA&M Information Fields

An OA&M message includes one or more information field.

3.3.1 Per Type Formats of Information Fields

The formats and values of the Data field of the OA&M Information Field are dependent upon the Information Field Type.

3.3.1.1 Capabilities Information Field

The capabilities information field is used to advertise a willingness to participate in OA&M functions to other OA&M devices within the administrative domain. The format of this field is shown in Figure 8 below:

Bits								
8	7	6	5	4	3	2	1	Octet
0	0	0	0	0	0	0	1	1
Type								
x	x	x	x	x	x	x	x	2
Length								
Capability #1 (Note 1, Note 2)								3
Capability #N								3+N

Note 1: Capability field values are multi-octet with the high-order bit used to indicate extension of this capability (high order bit=1 indicates another octet follows for this capability), and are defined in Table 4.

Note 2: The Capabilities I.F. must include the Hello Message capability. All other capabilities are optional.

Figure 8 - Capabilities Information Field Format

Capability Field Value	Length	Usage
0x01 (see Figure 9)	5-octet	Hello Message (Note 1)
0x02	1-octet	Supports Frame Transfer Delay
0x03(see Figure 9)	5-octet	Supports Frame Delivery Ratio
0x04 (see Figure 9)	5-octet	Supports Data Delivery Ratio
0x05	1-octet	Supports Latching Loopback
0x06	1-octet	Supports Non-latching Loopback

Table 4 - Capability Information Field Type Values

The single octet capabilities are formatted using an 8-bit value of the capability from Table 4.

The Hello, Frame Delivery Ratio, and Data Delivery Ratio capabilities use a multi octet format, which provides a maximum-time capability value. The format for these is shown in Figure 9.

Bits

8	7	6	5	4	3	2	1	Octet
1	X	X	X	X	X	X	X	1
EA	Capability Type							
1	X	X	X	X	X	X	X	2
EA	Capability Value (high order bits)							
1	X	X	X	X	X	X	X	3
EA	Capability Value (mid-h order bits)							
1	X	X	X	X	X	X	X	4
EA	Capability Value (mid-l order bits)							
0	X	X	X	X	X	X	X	5
EA	Capability Value (low order bits)							

Figure 9 - Multi-octet Capability Format

3.3.1.1.1 Hello Message Capability

The Hello Capability uses a 5-octet extended format supporting a 28-bit value. This value indicates the time (in milliseconds) that the transmitting FROMP advertises as the recommended expiration value of the TIMER_HELLO_RX timer.

3.3.1.1.2 Supports FDR Capability

The Supports FDR Capability uses a 5-octet extended format capability supporting a 28-bit value. This value, in milliseconds, represents the maximum amount of time that may expire before any of the transmitting FROMP FDR counters (either its Tx and Rx counters) can cycle.

3.3.1.1.3 Supports DDR Capability

The Supports DDR Capability uses a 5-octet extended format capability supporting a 28-bit value. This value, in milliseconds, represents the maximum amount of time that may expire before any of the transmitting FROMP DDR counters (either its Tx and Rx counters) can cycle.

3.3.1.2 Frame Transfer Delay Information Field

The frame transfer delay information field is used to measure Frame Transfer Delay (FTD). The format for this information field is shown in Figure 10 below:

Bits								
8	7	6	5	4	3	2	1	Octet
0	0	0	0	0	0	1	0	1
Type								
0	0	0	0	x	1	1	0	2
Length								
Initiator TX Time-stamp (Note 1)								3
Receiver RX Time-stamp (Note 2)								7
Receiver TX Time-stamp (Note 2)								11

Note 1: Time-stamp fields shall be 4 octets in length and represent milliseconds. The value is assumed to be of local significance only.

Note 2: These fields are only present in response to an FTD message.
The length of the information field (1110 or 0110) is used to determine if this is the request or response.

Figure 10 - Frame Transfer Delay Information Field Format

3.3.1.3 Frame Transfer Delay Results Information Field

The frame transfer delay results information field is used to return the result of a FTD round-trip measurement. The format for this information field is shown in Figure 11 below:

Bits								
8	7	6	5	4	3	2	1	Octet
0	0	0	0	0	0	1	1	1
Type								
0	0	0	0	0	1	1	0	2
Length								
Calculated Result (Note 1)								3

Note 1: Calculated result is a 4-octet value in milliseconds representing the ONE-WAY FTD determined by a dividing in half the results of the round-trip test measurement initiated by the transmitter of this message.

Figure 11 - Frame Transfer Delay Results Information Field Format

3.3.1.4 Frame Delivery Ratio Sync Information Field

The frame delivery ratio sync information field is used to determine the Frame Delivery Ratio (FDR). The format for this information field is shown in Figure 12 below:

Bits								
8	7	6	5	4	3	2	1	Octet
0	0	0	0	0	1	0	0	1
Type								
0	0	0	0	1	1	1	0	2
Length								
$FramesOfferred_{Committed}$								3
$FramesOfferred_{Excess}$ (See note 1)								7
VC Time (See note 2)								11

Note 1: Does not include frames in CIR or in excess of CIR+ Excess Burst.
Note 2: 4-octet value indicating an approximate time offset (in ms) relative to the counters. This value must increase in successive polls. Set to zero by initiator to indicate a restart condition. See section 4.4.4

Figure 12 - Frame Delivery Ratio Sync Information Field Format

3.3.1.5 Frame Delivery Ratio Results Information Field

The frame delivery ratio results information field is used to return the result of a FDR measurement. The format for this information field is shown in Figure 13 below:

Bits								
8	7	6	5	4	3	2	1	Octet
0	0	0	0	0	1	0	1	1
Type								
0	0	0	1	0	0	1	0	2
Length								
FramesDelivered $_{Committed}$ (Note 1)								3
FramesDelivered $_{Excess}$ (Note 1, Note 2)								7
FramesLost $_{Committed}$ (Note 1)								11
FramesLost $_{Excess}$ (Note 1, Note 2)								15

Note 1: These fields are 4 octets each. They are be used to deliver the results of a Frame Delivery measurement in the reverse direction.

Note 2: Does not include frames within CIR or in excess of CIR+ Excess Burst.

Figure 13 - Frame Delivery Ratio Results Information Field Format

3.3.1.6 Data Delivery Ratio Sync Information Field

The data delivery ratio sync information field is used to determine the Data Delivery Ratio (DDR). The format for this information field is shown in Figure 14 below:

Bits								
8	7	6	5	4	3	2	1	Octet
0	0	0	0	0	1	1	0	1
Type								
0	0	0	0	1	1	1	0	2
Length								
$DataOffered_{Committed}$								3
$DataOffered_{Excess}$ (Note 1)								7
VC Time (Note 2)								11

Note 1: Does not include frames within CIR or in excess of CIR+ Excess Burst.

Note 2: 4-octet value indicating an approximate time offset (in ms) related to the counters. This value must increase in successive polls. Set to zero by initiator to indicate a restart condition. See section 4.4.5.

Figure 14 - Data Delivery Ratio Sync Information Field Format

3.3.1.7 Data Delivery Ratio Results Information Field

The data delivery ratio results information field is used to return the result of a DDR measurement. The format for this information field is shown in Figure 15 below:

Bits								
8	7	6	5	4	3	2	1	Octet
0	0	0	0	0	1	1	1	1
Type								
0	0	0	1	0	0	1	0	2
Length								
DataDelivered $_{Committed}$ (Note 1)								3
DataDelivered $_{Excess}$ (Note 1, Note 2)								7
DataLost $_{Committed}$(Note 1)								11
DataLost $_{Excess}$ (Note 1, Note 2)								15

Note 1: These fields are 4 octets each. They are used to deliver the results of a Data Delivery measurement in the reverse direction.

Note 2: Does not include frames within CIR or in excess of CIR+ Excess Burst.

Figure 15 - Data Delivery Ratio Results Information Field Format

3.3.1.8 Non-Latching Loopback Information Field

The non-latching loopback information field is used to perform minimally intrusive operational diagnostic actions. The format for this information field is shown in Figure 16 below:

Bits								
8	7	6	5	4	3	2	1	Octet
0	0	0	0	1	0	0	0	1
Type								
x	x	x	x	x	x	X	x	2
Length								
Non-Latching Loopback Code (Note 1)								3
Option Data (Note 2)								5

Note 1: Non-Latching Code Values are defined in Table 5.

Note 2: Length of this field may be determined from length of the I.F. Option Data **may** be present and content is not subject to standardization.

Figure 16 - Non-Latching Loopback Information Field Format

Command Value	**Usage**
0x01	Non-latched Loop Frame Request
0x02	Non-latched Loop Frame Response

Table 5 - Non-Latching Loopback Code Values

3.3.1.9 Latching Loopback Information Field

The latching loopback information field is used to perform service affecting operational diagnostic actions. The format for this information field is shown in Figure 17 below:

Bits								
8	7	6	5	4	3	2	1	Octet
0	0	0	0	1	0	0	1	1
Type								
0	0	0	0	0	0	1	1	2
Length								
Latching Loopback Code (Note 1)								3

Note 1: 1-octet value. Latching Loopback Code Values are defined in Table 6.

Figure 17 - Latching Loopback Information Field Format

Command Value	Usage
0x01	Latched Loop Enable Request
0x02	Latched Loop Disable Request
0xFF	Latched Loop Denied

Table 6 - Latched Loopback Code Values

3.3.1.10 Diagnostic Indication Information Field

The diagnostic indication information field is used to convey operational information to other OA&M devices. The format for this information field is shown in Figure 18 below:

Bits								
8	7	6	5	4	3	2	1	Octet
0	0	0	0	1	0	1	0	1
Type								
x	x	x	x	x	x	X	x	2
Length								
Event Type (Note 1)								3
Event Location (Note 2)								4

Note 1: See Table 7.

Note 2: Length and Content of this field is not subject to standardization.

Figure 18 - Diagnostic Indication Information Field Format

Event Type Value	Usage
0x00	VC Latching Loopback Enabled
0x01	VC Latching Loopback Disabled
0x02	Phy down
0x03	Phy up

Table 7 - Event Types for Diagnostic Indication

3.3.1.11 Full Source Address Information Field

The full source address information field **may** be used by an OA&M device to advertise a more complete identification of the device. This is for use by higher layer management. The format for this information field is shown in Figure 19 below:

Bits								
8	7	6	5	4	3	2	1	Octet
0	0	0	0	1	0	1	1	1
Type								
x	x	x	x	x	x	x	x	2
Length								
Address Type (Note 1)								3
Address information								4

Note 1: Address Type values are shown in Table 8.

Figure 19 - Full Source Address Information Field

Address Type Value	**Usage**
0x01	Clear Text (Null terminated string)
0xCC	IPv4 Address (4-octet)
0xFD	AESA Identified per X.36 [6]
0xFE	E.164 Address per X.36
0xFF	X.121 Address per X.36

Table 8 – Address Type Values

3.3.1.12 Opaque Information Field

The opaque information field allows for vendor-specific extensions to the OA&M protocol. An implementation receiving an opaque information field **may** choose to process or ignore this information field based upon the organizationally unique identifier (OUI) contained in the field. The OUI information field **may** be repeated within an OA&M message. The format for this information field is shown in Figure 20 below:

Bits								
8	7	6	5	4	3	2	1	Octet
1	1	1	1	1	1	1	0	1
Type								
x	x	x	x	x	x	x	x	2
Length								
Organizationally Unique Identifier (OUI) (Note 1)								3
SubCode (Note 2)								6
Vendor-Specific Data (Note 3)								7

Note 1: OUIs are assigned by IEEE. Bit-8 is the most significant bit.

Note 2: Content of SubCode field is not subject to standardization.

Note 3: Length and contents of Vendor-Specific Data field are not subject to standardization.

Figure 20 - Opaque Information Field Format

3.3.1.13 Pad Information Field

The pad information field **may** be used to create an OA&M message with a specific length. The pad information field **may** be repeated within an OA&M message as needed. The format for this information field is shown in Figure 21 below:

Bits								
8	7	6	5	4	3	2	1	Octet
1	1	1	1	1	1	1	1	1
Type								
x	x	x	x	x	x	x	x	2
Length (Note 1)								
Padding (Note 2)								3

Note 1: Length may be from 2-255.

Note 2: Contents of the Padding field is not subject to standardization.

Figure 21 - Pad Information Field Format

4 OA&M Procedures

This section describes a set of rules for processing OA&M messages that use the formats described in section 3.

- Section 4.1 describes rules for the encoding and decoding of messages.
- Section 4.2 provides the general rules for the processing of OA&M messages.
- Procedures to discover peer FROMPs, and advertise capabilities, via the Hello message are covered in section 4.3.
- Service Level Measurement procedures using the Service Verification message are detailed in section 4.4.
- Procedures for the Non-Latching and Latching Loopback messages are in of section 4.5 and 4.6.
- Procedures for the Diagnostic Indications message are covered in section 4.7.

4.1 Message Encoding/Decoding Rules

Implementations of this IA **should** process the decoding of messages described in section 3 using the following general rules:

- Improprieties in the message header, such as an ill-formed address or unknown message type, **should** cause the entire message to be discarded.
- An improperly formed Information Field **should** be ignored along with the remainder of the message, and the remainder of the message processed. One example would be any information field with a length of zero or one.
- A properly formed, but unknown, Information Field **should** be ignored and the remainder of the message processed.
- A properly formed Information field with an unexpected length **should** be ignored and the remainder of the message processed.
- If the last information field is not complete, this field should be ignored, however the remainder of the message **may** be processed.

OA&M messages passing through a FROMP are not subject to Information Field decoding and **should** be forwarded intact.

4.1.1 Order of transmission

- Throughout this Implementation Agreement, multi-octet values **shall** be transmitted most significant byte to least significant byte (MSB) order.
- When bits are depicted in the formats, Bit-8 is the Most Significant Bit.

4.1.2 Order of Information Fields

Information fields within an OA&M message **must** be presented in ascending order of information field type values. For example, the capabilities information field, when present, **must** be the first information field present in the message. Similarly, the pad information field **must** be the last element when present. Only the Opaque and Pad information fields are allowed to be repeated within an OA&M message.

4.1.3 Usage of Information Fields

Each OA&M message **must** include at least one information field. The maximum number of information fields is limited by MTU size.

Information fields are included in an OA&M message dependent upon the message type indicated in the OA&M header. Table 9 defines information fields that **may** be included for each message type. Fields marked N/A may not be used in a message of the indicated message type. A message containing an Information Field that of an unknown

Information Field Type, or containing an information field that is not allowed for the indicated message type will be ignored without affecting the processing of subsequent information fields.

I.F. Type Value	Usage	Hello Message	Service Verification Message	Latching Loopback Message	Non-Latching Loopback Message	Diagnostic Indication Message
0x01	Capabilities	Mandatory	N/A	N/A	N/A	N/A
0x02	Frame Transfer Delay	N/A	Optional	N/A	N/A	N/A
0x03	Frame Transfer Delay Results	N/A	Optional	N/A	N/A	N/A
0x04	Frame Delivery Ratio Sync	N/A	Optional	N/A	N/A	N/A
0x05	Frame Delivery Ratio Results	N/A	Optional	N/A	N/A	N/A
0x06	Data Delivery Ratio Sync	N/A	Optional	N/A	N/A	N/A
0x07	Data Delivery Ratio Results	N/A	Optional	N/A	N/A	N/A
0x08	Non-Latching Loopback	N/A	N/A	N/A	Mandatory	N/A
0x09	Latching Loopback	N/A	N/A	Mandatory	N/A	N/A
0x0A	Diagnostic Indication	N/A	N/A	N/A	N/A	Mandatory
0x0B	Full Source Address	Optional	N/A	N/A	N/A	N/A
0xFE	Opaque	Optional	Optional	Optional	Optional	Optional
0xFF	Pad	Optional	Optional	Optional	Optional	Optional

Table 9 - Information Fields by Message Type

4.1.4 Counters and Counter Wrap

These procedures support the use of various fixed length counters that will wrap (roll over to zero). Implementations of these procedures **must** support normal counter-wrapping to occur. Computations using these counters take into consideration the maximum value, and upon receiving a lower value in a subsequent message assume the counter has wrapped once.

4.2 General Message Processing

General rules for the transmission, reception, and forwarding of OA&M messages are described in this section.

4.2.1 Transmission of Messages

A FROMP generating an OA&M message **shall** always provide valid domain identification, source location identifier, and destination location identifier data in the OA&M message header.

The domain identification **shall** uniquely identify all administrations on the virtual circuit. Service Providers **should** use their X.121 or E.164 Network Identifiers. The domain identification **must** be one of the domains for which the transmitting OA&M device is a member. OA&M messages **must not** use the "all domain broadcast" domain identification plan.

The source location identifier **must** be unique within this domain on this VC. The source location identifier used by a FROMP **should** be the same on a given VC for all domains.

The destination location identifier can either be the global destination identifier (see section 3.2.4), or it can be the source location identifier received in a Hello message from another device (see section 4.3). The global destination address is used only for the Hello message type.

4.2.2 Reception and Forwarding of Messages

OA&M messages arriving at an interface of a FROMP may be discarded, processed, and/or forwarded according to the rules in this section. Figure A - 1 provides an example flow chart depicting the decision-making logic that can be used.

A FROMP **must** distinguish between arriving messages with domain identification matching a domain of which the FROMP is a member, and those that are not. These messages will be referred to as being "in the same domain" and "from a foreign domain" respectively.

4.2.2.1 Arriving OA&M Message From a Foreign Domain

A FROMP **must** forward (local conditions permitting) any messages that do not match its domain identification.

4.2.2.2 Arriving OA&M Messages From Same Domain

Messages arriving at an interface of a FROMP that match its domain identification are processed according to the rules of this section. In some cases, the messages are treated differently depending upon whether this FROMP terminates the administrative domain associated with this message.

4.2.2.2.1 Duplicate Location Identifier Detection

At any FROMP, a message that contains a Domain Identification and Source Location Identifier that match those of the receiving entity **shall** be discarded. A FROMP detecting this condition **should** send an indication of the conflict to the network management layer.

4.2.2.2.2 Arriving at a Non-Boundary Device

A FROMP that does not terminate a domain boundary **must**:

- Receive for further processing, and not forward, messages with the same domain identification and a matching destination location identifier.
- Receive for further processing, and forward (subject to congestion), messages with the same domain identification and the broadcast destination identifier.
- Forward (subject to congestion), without receiving for further processing, messages with the same domain identification and a destination location identifier that is neither matching nor the broadcast identifier.

4.2.2.2.3 Arriving at a Boundary Device

A FROMP that does terminate a domain boundary **must**:

- Discard without processing, or forwarding, all messages with the same domain identification that arrive on an interface that is outside the domain boundary. For example, in Figure 3, for a device at location B1, messages arriving from the direction of location A1 are discarded if domain B is identified. The FROMP **may** send an indication of the conflict to the device's network management layer.
- Receive for further processing, and not forward, messages with the same domain and a matching destination location identifier or broadcast location identifier arriving on an interface that is inside the domain boundary.

Discard without processing, or forwarding, all messages with the same domain identification and a destination identifier that is neither matching nor the broadcast identifier arriving on an interface that is inside the domain boundary.

4.2.3 Timers

A number of timers are defined in these procedures. These timers are used per Domain/Interface in some cases, and Domain/Interface/Peer in others. Table 10 summarizes these timers, their ranges and defaults.

Name	Purpose	Range	Default
TIMER_HELLO_TX	Send Hello Message (Discovery)	15-3600 seconds	900 Seconds
TIMER_HELLO_RX	Detect Lost Peer (Discovery)	60-14400 seconds	3200 Seconds
TIMER_SLV	Initiate SLV Measurement(s)	15-3600 seconds	900 Seconds

Table 10 - OA&M Timers

4.3 Hello Message Processing (Device Discovery)

Peer FROMPs are discovered when a Hello message is received on the frame relay connection from another OA&M device in the same administrative domain. The Hello message contains information about the peer FROMP's capabilities and are transmitted periodically based upon the TIMER_HELLO_TX timer.

If a FROMP is in the middle of an administrative domain (not a boundary device), two Hello messages are transmitted; one message towards each VC endpoint. If a FROMP is at the administrative boundary, the Hello messages will only be transmitted on the interface within the domain. Each Hello message applies to a single domain as encoded in the Domain Identification field of the message header. If a FROMP supports multiple domains (*e.g.*, Figure 22 C1/F1) a separate message **must** be generated for each domain. A device **may** advertise a different capability set for each domain.

The following functions are provided by the discovery procedure:

1. Association of a FROMP with one or more administrative domains,
2. Association of a FROMP with a specific location identifier for an administrative domain,
3. Advertisement of OA&M capabilities supported by the device, and
4. Support for vendor extensions via the opaque field.

Figure 22 illustrates transmission of the Hello message from a number of hypothetical FROMPs located on the path of a single virtual connection.

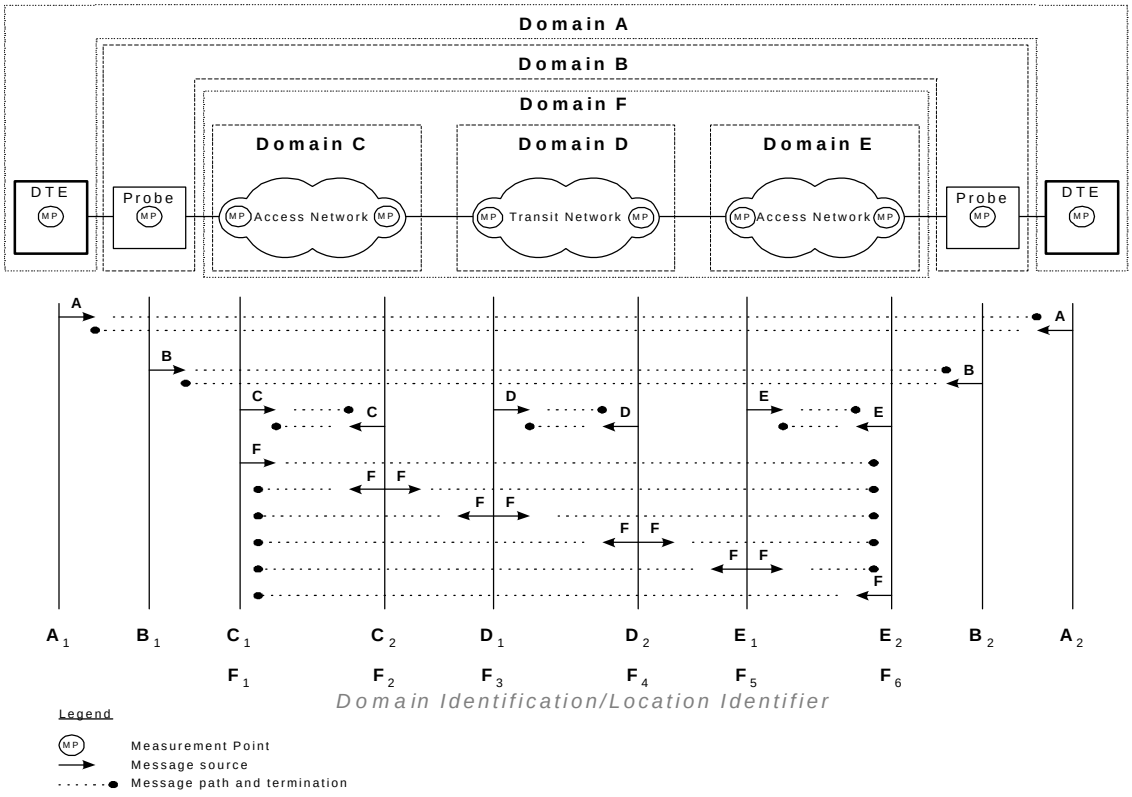


Figure 22 - Example of Hello Messages on a VC with multiple Administrative Domains

Appendix B.1 provides an example of message flows for Hello messages between two peer FROMPS in the same domain.

4.3.1 Sending the Hello Message

For each virtual circuit for each domain that this FROMP is participating in, the following procedures apply. Implementations are encouraged to use techniques that prevent bursts of Hello messages from being transmitted.

4.3.1.1 Connection Initialization

A FROMP **may** initiate the discovery process upon establishment of the connection. In the case of PVCs, establishment is indicated when Q.933 [10] signaling status messages report the virtual connection as "active". If the FROMP is positioned at the network-to-network interface then both networks need to report the virtual connection as "active" for the connection to be considered established. In the case of SVCs, establishment is indicated when the Q.933 CONNECT message is received.

Upon initiating the discovery process, the FROMP transmits a Hello message. The message **shall** be sent with a destination location identifier for the global destination. A FROMP at a domain boundary in a network **may not** send the Hello message on a segment of the connection that is not part of the domain. For example, location D2 in Figure 22sends a Hello message for Domain D towards location D1 but never towards location E1.

Capabilities advertised via the capabilities information field **must** remain available for the duration of the frame relay connection. Additional capabilities **may** be added in subsequent Hello messages (for example due to changes initiated by a higher layer management operation). Once added, the new capabilities **must** remain available for the duration of the frame relay connection. In the case of multi-octet time intervals advertised in the capabilities information field, the interval **may not** change in subsequent Hello messages.

4.3.1.2 Periodic Transmission Interval

All FROMPs **shall** transmit the Hello message periodically. Upon transmitting a hello message for a domain on an interface, the device **shall** set a timer, TIMER_HELLO_TX.

Transmission of the Hello message **may** be suspended when the data link connection is not operational. Examples of causes include:

1. a failure of the link integrity verification mechanism,
2. the clearing of the "active" bit,
3. the setting of the "delete" bit,
4. the absence of the data link connection information element.

Transmission of the Hello message **should** resume upon connection initialization as described in section 4.3.1.1.

4.3.2 Processing the Received Hello Message

The received Hello message shall be compared with previously recorded hello messages from this peer on this VC. The timer, TIMER_HELLO_RX, is (re)set for this peer. The Peer provides a recommended value for this timer in the Supports Hello Capability.

4.3.2.1 Discovery of a New Peer

Receiving a valid Hello message from a new peer device enables this device to send OA&M messages of message types other than Hello directed towards this new peer. The capabilities listed in this Hello message shall be maintained and honored. OA&M communication to this peer **may** be initiated immediately upon receipt of a single Hello message from the peer.

4.3.2.2 Previously Recorded Peer

Upon receiving a valid Hello message from an existing peer, the contents of the Capabilities Information Field **shall** be examined for new and/or improved capabilities.

4.3.3 TIMER_HELLO_RX Expiration

A time-out algorithm for detecting that an OA&M device is no longer advertising its presence and willingness to participate in OA&M with the Hello message is recommended. It is further suggested that such an algorithm allow for implementations that use variable logic for their TIMER_HELLO_TX value.

Upon detecting such a timeout expiration condition, procedures to initiate Service Level Verification measurements **should** be discontinued.

4.4 Service Level Verification Message Processing

Service Level verification and segment-oriented quality of service measurement is performed by use of the Service Verification message. In most cases, a measurement requires multiple messages to be exchanged between two OA&M peer devices. In some cases, these measurements measure a service parameter in one direction, and a separate independent measurement **may** be needed in the reverse direction.

There are three service measurements supported by the Service Verification message:

- Frame Transfer Delay
- Frame Delivery Ratio
- Data Delivery Ratio

The three measurements are implemented with independent information fields. These measurements are independent of each other, although in many cases they will be combined in a single message.

Appendix B.2 and Appendix B.3 provide an example of message flows for FTD and FDR/DDR.

4.4.1 Sending the Service Verification Message

The Service Verification message **must** be transmitted only using a specific (non-broadcast) destination location. A FROMP **must** receive at least one Hello message from a peer prior to transmission of a Service Verification message to this location.

4.4.1.1 Periodic Transmission Interval for Measurement Initiations

Each type of service measurement **may** use an independent timer (designated TIMER_SLV_*), or share a single timer (designated TIMER_SLV). At the expiration of any TIMER_SLV, the FROMP **may** send the Service Verification message.

The value of any TIMER_SLV is not subject to standardization. A FROMP **must** take the received maximum interval from a peer device into account in setting its TIMER_SLV. The recommended default interval for TIMER_SLV is 900 seconds.

4.4.2 Processing the Received Service Verification Message

Processing of the received message is entirely dependent upon the information fields present. The presence of these information fields indicates which function(s) are to be performed. Sections 4.4.3, 4.4.4, and 4.4.5 describe procedures based upon the function being performed.

4.4.3 Procedures for Delay Measurement

In this procedure, a round-trip delay measurement is made. This measurement is divided in half to obtain the FRF.13 one-way FTD measurement.

A Frame Transfer Delay measurement requires a two-way exchange between initiator and receiver FROMPs. The initiator begins the measurement by sending a message with the frame transfer delay information field; the receiver loops the message back after filling in additional time-stamps. Optionally, the initiator **may** then deliver a copy of the results back to the receiver using the frame transfer delay results information field.

This procedure uses the Frame Transfer Delay I.F., the Frame Transfer Results I.F., and the Pad I.F. An example of message flows between the initiator and receiver devices is shown in Figure B - 2.

4.4.3.1 Delay Initiation

On the initiation of a delay measurement, the initiator device transmits the Frame Transfer Delay I.F. using the short form (6 octets). The initiator **shall** fill in the initiator TX time-stamp with a value representing the time the opening bit of the frame will begin transmission.

4.4.3.2 Delay Turnaround

Upon receiving a Frame Transfer Delay I.F. of the short form, the receiver device responds to the initiator with the Frame Transfer Delay I.F. long form (12 octets). The responder **shall** copy the initiator Tx time-stamp, fill in the responder Rx time-stamp with a value representing the arrival time of the closing bit of the frame, and fill in the responder Tx time-stamp with a value representing the time the opening bit of the frame will begin transmission. This response **shall** be sent in an OA&M message padded to the same length as was received. The pad information field is available to be used for this purpose.

4.4.3.3 Delay Measurement

Upon receiving a Frame Transfer Delay I.F. of the long form, the initiator device **shall** record a time-stamp with a value representing the arrival time of the closing bit of the frame. Calculation of FTD is performed using the following equation:

$$FTD = ((Initiator\_Rx - Initiator\_Tx) - (Responder\_Tx - Responder\_Rx))/2$$

4.4.3.4 Delivery of Delay Results

Dependent upon provisioning, the initiator device **may** forward the calculated one-way FTD results to the receiver device using the Frame Transfer Delay Results I.F. Such forwarding **may** be done immediately, or held for inclusion in the next measurement interval.

4.4.3.5 Error Handling

A lost or damaged FTD request or response message can result in a missed measurement period. Implementations **may** optionally time-out and retransmit to recover the period.

4.4.4 Procedures for Frame Delivery Ratio Measurement

In this procedure, a one-way measurement is made of the delivery ratio from the initiator to the receiver. This measurement satisfies the requirements for FDR, FDRc, and FDRe of FRF.13.

A complete Frame Delivery Ratio measurement requires multiple exchanges between the initiator and receiver. The beginning of a measurement session requires the initiator to send a sync indication. Measurements **may** then be made by the initiator sending a second FDR Sync I.F. message to the receiver. This creates a one-way measurement of the parameter. The receiver **may** send a copy of the results back to the initiator by using the frame delivery results information field. An independent measurement session **may** also be established in the reverse direction.

This procedure uses the Frame Delivery Ratio Sync I.F., and the Frame Delivery Results I.F. An example of message flows between the initiator and receiver devices is shown in Figure B - 3. An example of a method to perform this measurement is shown in Appendix C.

4.4.4.1 Frame Delivery Ratio Initiation

The Frame delivery ratio sync I.F. is used to initialize (or re-initialize) an FDR measurement session.

The initiator of this message shall fill in the VC Time (in milliseconds) to ensure that the receiver interprets the message to indicate a(n) (re-)initialization. A VC Time of zero is used to indicate initiation or re-initialization.

The initiator of this message shall also fill in the current counters for this VC ($FramesOffered_{Committed}$ and $FramesOffered_{Excess}$) prior to this message being transmitted. OA&M messages **must** be included in these frame counters.

When a Frame Delivery Ratio Sync I.F. is received with the VC Time value set to zero or less than the previous received value (taking into account normal counter-wrapping), the receiver **shall** terminate any previous session and restart a new session. A FROMP receiving this information field (regardless of the VC Time indicated) **shall** record the receiver frame counts representing the counters for this VC ($FramesReceived_{Committed}$ and $FramesReceived_{Excess}$) as they were prior to the reception of this frame.

4.4.4.2 Frame Delivery Ratio Measurement

The Frame Delivery Ratio Sync I.F. is also used to complete a one-way measurement of the ratio of frames delivered to frames offered. The initiator device of this message shall fill in the current counters for this VC ($FramesOffered_{Committed}$ and $FramesOffered_{Excess}$) prior to this message being transmitted. When wrapping of the VC Time occurs, the initiator **shall** ensure that a value of zero is not sent.

A FROMP receiving the frame delivery ratio sync I.F. **shall** record the receiver frame counts representing the counters for this VC ($FramesReceived_{Committed}$ and $FramesReceived_{Excess}$) as they were prior to the reception of this frame. The value of the VC Time **shall** be inspected for indications of a restart as described in the previous section.

The receiving device **shall** determine if the recorded maximum interval has been exceeded.

- If the interval has been exceeded, the device **shall not** use the previous counters to calculate the FDR for the interval terminated by this message. The counters from this poll **shall** be stored such that the next poll in this measurement session will be valid if it is received within the allowable interval.
- If the interval has not been exceeded, the device **shall** use these counters to calculate the FDRs for the interval. FDRs for the receive direction are calculated using the following formulae:

$$FramesOffered_{Committed} = FramesOffered_{Committed}2 - FramesOffered_{Committed}1$$

$$FramesOffered_{Excess} = FramesOffered_{Excess}2 - FramesOffered_{Excess}1$$

$$FramesDelivered_{Committed} = FramesReceived_{Committed}2 - FramesReceived_{Committed}1$$

$$FramesDelivered_{Excess} = FramesReceived_{Excess}2 - FramesReceived_{Excess}1$$

$$FramesLost_{Committed} = FramesOffered_{Committed} - FramesDelivered_{Committed}$$

$$FramesLost_{Excess} = FramesOffered_{Excess} - FramesDelivered_{Excess}$$

$$FDR_C = FramesDelivered_{Committed} / FramesOffered_{Committed}$$

$$FDR_E = FramesDelivered_{Excess} / FramesOffered_{Excess}$$

$$FDR = \frac{(FramesDelivered_{Committed} + FramesDelivered_{Excess})}{(FramesOffered_{Committed} + FramesOffered_{Excess})}$$

The device **shall** record the counters for use by the next “FDR Sync” message.

4.4.4.3 Delivery of Frame Delivery Ratio Results

Dependent upon provisioning, the receiver device **may** forward the calculated one-way FDR results to the initiator device using the Frame delivery ratio results I.F. Such forwarding **may** be done immediately, or held for inclusion in the next measurement interval.

4.4.4.4 FDR Error Handling

A lost or damaged FDR Sync message **may** result in one or more missed measurement intervals. If the maximum interval for counter-wrap (advertised by the peer in the capabilities information field) does not expire prior to the next successful FDR Sync message, this next complete measurement will span the period between the two received messages. If the maximum interval for counter-wrap occurs, the next successful FDR Sync message is treated as if it were a restart. In this case, the prior interval(s) are lost and FDR Results **shall not** be sent.

4.4.5 Procedures for Data Delivery Ratio Measurement

In this procedure, a one-way measurement is made of the delivery ratio from the initiator to the receiver. This measurement satisfies the requirements for DDR, DDRc, and DDRe of FRF.13.

A complete Data Delivery Ratio measurement requires multiple exchanges between the initiator and receiver. The beginning of a measurement session requires the initiator to send a sync indication. Measurements **may** then be made by the initiator sending a second DDR Sync I.F. message to the receiver. This creates a one-way measurement of the parameter. The receiver **may** send a copy of the results back to the initiator by using the frame delivery results information field. An independent measurement session **may** also be established in the reverse direction.

This procedure uses the Data Delivery Ratio Sync I.F., and the Data Delivery Results I.F. An example of message flows between the initiator and receiver devices is shown in Figure B - 3. An example of a method to perform this measurement is shown in Appendix C.

4.4.5.1 Data Delivery Ratio Initiation

The data delivery ratio sync I.F. is used to initialize (or re-initialize) a DDR measurement session.

The initiator of this message shall fill in the VC Time (in milliseconds) to ensure that the receiver interprets the message to indicate a(n) (re-)initialization. A VC Time of zero is used to indicate initiation or re-initialization.

The initiator of this message shall also fill in the current counters for this VC ($DataOffered_{Committed}$ and $DataOffered_{Excess}$) prior to this message being transmitted. OA&M messages **must** be included in these data counters.

When a Data Delivery Ratio Sync I.F. is received with the VC Time set to zero, or a value less than the previous received value from the initiator, the receiver **shall** terminate any previous session and restart a new session. A FROMP receiving this information field (regardless of the VC Time indicated) **shall** record the receiver frame counts representing the counters for this VC ($DataReceived_{Committed}$ and $DataReceived_{Excess}$) as they were prior to the reception of this frame.

4.4.5.2 Data Delivery Ratio Measurement

The Data Delivery Ratio Sync I.F. is also used to complete a one-way measurement of the ratio of octets delivered to octets offered. The initiator device of this message shall fill in the current counters for this VC ($DataOffered_{Committed}$ and $DataOffered_{Excess}$) prior to this message being transmitted.

A FROMP receiving the data delivery ratio sync I.F. **shall** record the receiver octet counts representing the counters for this VC ($DataReceived_{Committed}$ and $DataReceived_{Excess}$) as they were prior to the reception of this frame. The value of the VC Time **shall** be inspected for indications of a restart as described in the previous section.

The receiving device **shall** determine if the recorded maximum interval has been exceeded.

- If the interval has been exceeded, the device **shall not** use the previous counters to calculate the DDR for the interval terminated by this message. The counters from this poll **shall** be stored such that the next poll in this measurement session will be valid if it is received within the allowable interval.
- If the interval has not been exceeded, the device **shall** use these counters to calculate the DDRs for the interval. DDRs for the receive direction are calculated using the following formulae:

$$\text{DataOffered}_{\text{Committed}} = \text{DataOffered}_{\text{Committed}}2 - \text{DataOffered}_{\text{Committed}}1$$

$$\text{DataOffered}_{\text{Excess}} = \text{DataOffered}_{\text{Excess}}2 - \text{DataOffered}_{\text{Excess}}1$$

$$\text{DataDelivered}_{\text{Committed}} = \text{DataReceived}_{\text{Committed}}2 - \text{DataReceived}_{\text{Committed}}1$$

$$\text{DataDelivered}_{\text{Excess}} = \text{DataReceived}_{\text{Excess}}2 - \text{DataReceived}_{\text{Excess}}1$$

$$\text{DataLost}_{\text{Committed}} = \text{DataOffered}_{\text{Committed}} - \text{DataDelivered}_{\text{Committed}}$$

$$\text{DataLost}_{\text{Excess}} = \text{DataOffered}_{\text{Excess}} - \text{DataDelivered}_{\text{Excess}}$$

$$\text{DDR}_{\text{C}} = \text{DataDelivered}_{\text{Committed}} / \text{DataOffered}_{\text{Committed}}$$

$$\text{DDR}_{\text{E}} = \text{DataDelivered}_{\text{Excess}} / \text{DataOffered}_{\text{Excess}}$$

$$\text{DDR} = \frac{(\text{DataDelivered}_{\text{Committed}} + \text{DataDelivered}_{\text{Excess}})}{(\text{DataOffered}_{\text{Committed}} + \text{DataOffered}_{\text{Excess}})}$$

The device shall record the counters for use by the next "DDR Sync" message.

4.4.5.3 Delivery of Data Delivery Ratio Results

Dependent upon provisioning, the receiver device **may** forward the calculated one-way DDR results to the initiator device using the data delivery ratio results I.F. Such forwarding **may** be done immediately, or held for inclusion in the next measurement interval.

4.4.5.4 DDR Error Handling

A lost or damaged DDR Sync message **may** result in one or more missed measurement intervals.

- If the maximum interval for counter-wrap (advertised by the peer in the capabilities information field) does not expire prior to the next successful DDR Sync message, this next complete measurement will span the period between the two received messages.
- If the maximum interval for counter-wrap occurs, the next successful DDR Sync message is treated as if it were a restart. In this case, the prior interval(s) are lost and DDR Results **shall not** be sent.

4.5 Non-Latching Loopback Message Processing

Frame Relay OA&M Diagnostics **may** be performed on a segment of a VC between two OA&M devices belonging to the same domain. There are two forms of diagnostics supported, a latching VC loopback and a non-latching loopback:

- The latching form is a service maintenance action that will remove the VC from service.
- The non-latching form is used to echo an individual OA&M frame without taking the VC out of service.

The Non-Latching Loopback procedures are contained in this section. The procedures for the Latching loopback are in section 4.6. Implementations **may** send either form of loopback prior to receiving a Hello message.

The Non-Latching Loopback message causes only the non-latching loop message itself to be looped back to the initiator. An example of messaging between the initiator and the receiver is shown in Figure B - 4.

The Non-Latching Loopback message **must** be transmitted using a specific (non-broadcast) destination location.

4.5.1 Initiating the Non-latching Loopback Request

A FROMP initiates a request for a peer device to perform a non-latching loopback by using the Non-Latching Loopback message with the latched loopback code of the non-latching loopback information field set to request. The length and content of this option data is not subject to standardization.

4.5.2 Processing the Received Non-Latching Loopback Message

A FROMP receiving the Non-Latching Loopback message **must** determine if the message's Domain Identification indicates membership within one of the domains supported at the receiving location and if the message's Destination Location Indicator indicates this OA&M device.

If the message is addressed for this location and the device supports this capability, then the message is processed.

If the non-latching loopback information field indicates a non-latched loopback request, the device **must** accept the request, and respond with a non-latching loopback message of identical length and content, except that:

1. The message source and destination locations are reversed.
2. The non-latching loopback code of the non-latching loopback information field is set to indicate a response.

If the non-latching loopback information field indicates a non-latched loopback response, the message is terminated.

4.6 Latching Loopback Message Processing

The latched loopback causes all arriving frames on the VC to be looped back towards the transmitter of the latched loopback message. Other VCs passing through this device are not affected. It is a one-way loopback that will not forward received frames further along the VC while the loopback is active. OA&M frames shall not pass through the OA&M device while the loopback is active, however OA&M frames addressed to this device shall be processed (removing from the looped data when appropriate) and responded to (adding to the looped data). This loopback is shown in Figure 23:

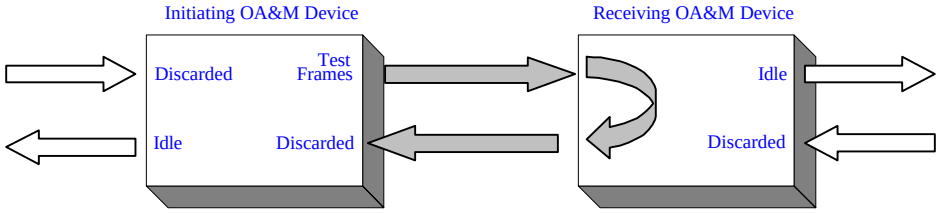


Figure 23 – VC Latched Loopback

The Latching Loopback message **must** be transmitted using a specific (non-broadcast) destination location. An example of messaging between the initiator and receiver is given in Figure B - 5.

4.6.1 Initiating the Latching Loopback Request

A FROMP initiates a request for a peer device to perform a latching loopback by using the Latching Loopback message with the latching loopback information field set to enable.

4.6.2 Processing the Received Latching Loopback Request

A FROMP receiving the Latching Loopback message **must** determine if the message's Domain Identification indicates membership within one of the domains supported at the receiving location and if the message's Location Indicator indicates this OA&M device. If the message is not addressed for this location, the message **must** be forwarded towards the connection terminus.

If the message is addressed for this location and the device supports this capability, then the message is processed.

If the latching loopback information field indicates a latched loopback enable request, the device **may** either accept the request or reject it. If the request is rejected, the receiver shall respond to the initiator with a Latching Loopback message and latching loopback information field indicating the rejection.

A VC latched loopback is an intrusive action that will disrupt the flow of data on the VC. If the receiving device also supports the Diagnostic Indications message, it **must** send a Diagnostic Indication message in each direction on the affected VC for each domain that it is a member of (see section 4.7). Such indications **should** be sent prior to enabling a VC loopback.

If the latching loopback information field indicates a latched loopback disable request, the device **must** accept the request. If the receiving device also supports the Diagnostic Indications message, it **must** send a Diagnostic Indication message in each direction on the affected VC for each domain that it is a member of (see section 4.7). Such indications **should** be sent after disabling a VC loopback.

4.6.3 Clearing a Latched Loopback

A FROMP may request a peer to clear a latching loopback condition by issuing a Latching Loopback message with a latching loopback information field with a disable request. This disable request may be sent by any peer in the domain, and from any direction (not only from the peer that initiated the loopback). The loopback may also be cleared by local management action.

4.7 Diagnostic Indications Message Processing

The Diagnostic Indications message is optionally used to signal peer FROMPs with indications of traffic affecting conditions. Devices should not rely upon the presence or absence of a Diagnostic Indications message. The ability of the network to deliver this message may be compromised due to the condition being signaled.

4.7.1 Initiating the Diagnostics Indication Message

A FROMP may send the diagnostics indication message when conditions necessitate. The transmitting device may transmit the message to individual destinations or use the broadcast destination address for a given domain. The message **shall** use the diagnostic indications information field with the appropriate indication. PHY_UP and PHY_DOWN **may** be used to notify peer FROMPs of a service affecting change detected at the physical interface.

4.7.2 Processing the Received Diagnostic Indications Message

A FROMP receiving the Diagnostic Indications message **must** determine if the message's Domain Identification indicates membership within one of the domains supported at the receiving location and if the message's Destination Location Indicator indicates this OA&M device (or the broadcast address).

If the message is addressed for this location and the device supports this capability, then the message is processed.

The actions to be taken upon reception of the Diagnostic Indications message are not subject to standardization.

A Appendix – General Receive Procedures

(Informative)

The following flow chart is illustrative of a possible implementation for OA&M traffic arriving at an interface. If there is a conflict between this flow chart and the main text, implementations **should** follow the text.

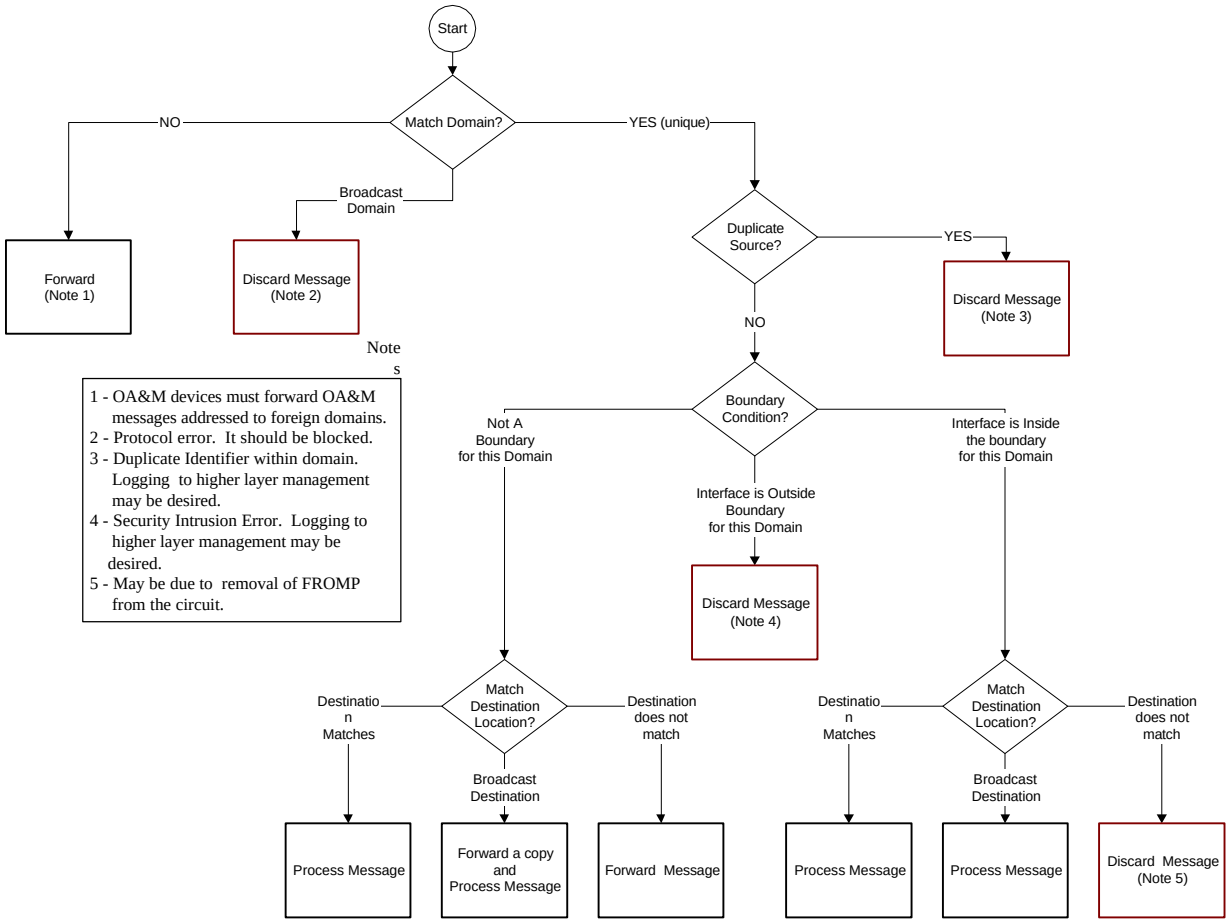


Figure A - 1 - General Receive Procedures

B Appendix – Message Flows

(Informative)

This Appendix contains informational examples of message flows between two peer OA&M devices on a VC. If there is a conflict with the text of the main document, the main document will supersede these examples.

B.1 Discovery

The Hello message is sent periodically; it contains the Capabilities I.F. Figure B - 1 below shows this sequence. Note that a subsequent message is allowed to add capabilities, but advertised capabilities are never withdrawn.

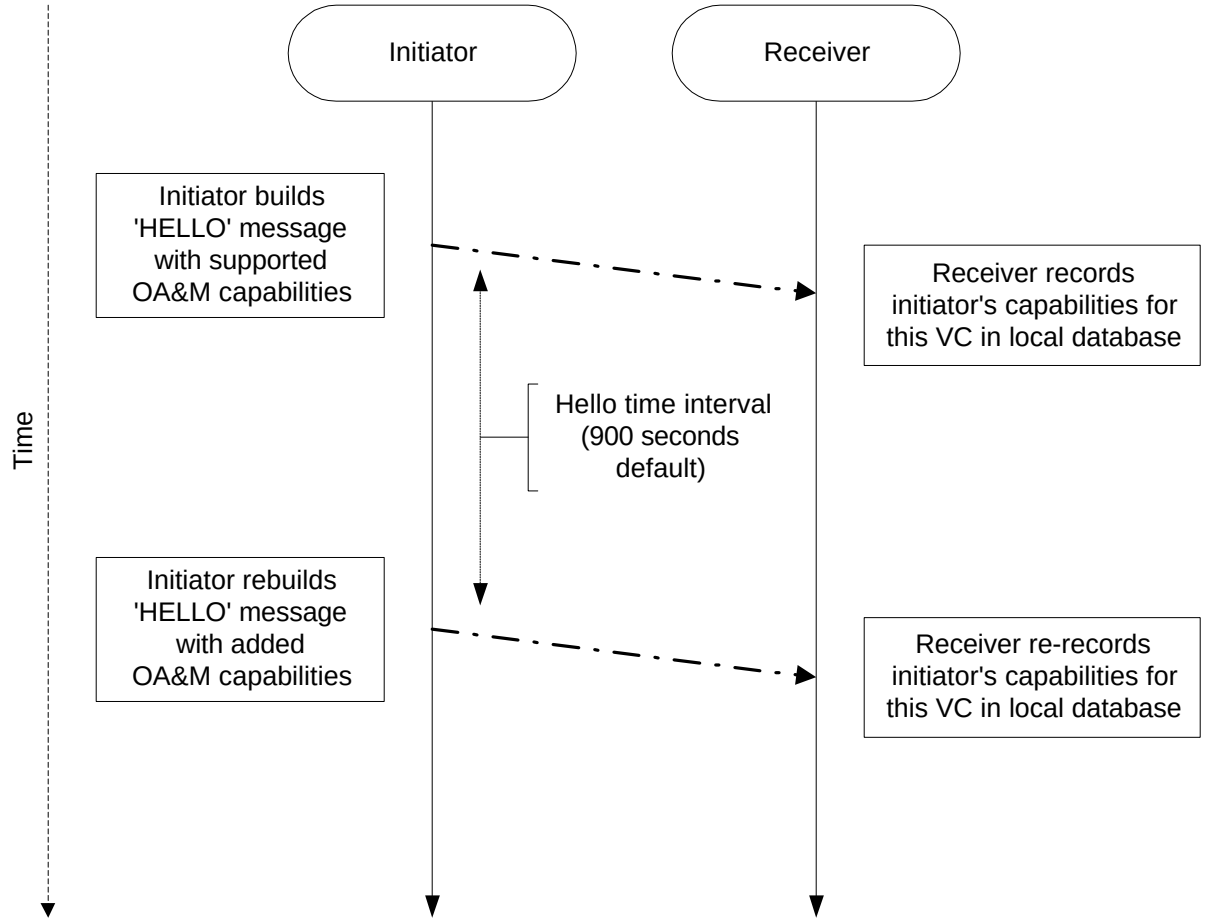


Figure B - 1 - Hello Message for Discovery

B.2 FTD Measurement

The FTD measurement can be done periodically. It requires a response as shown in Figure B - 2.

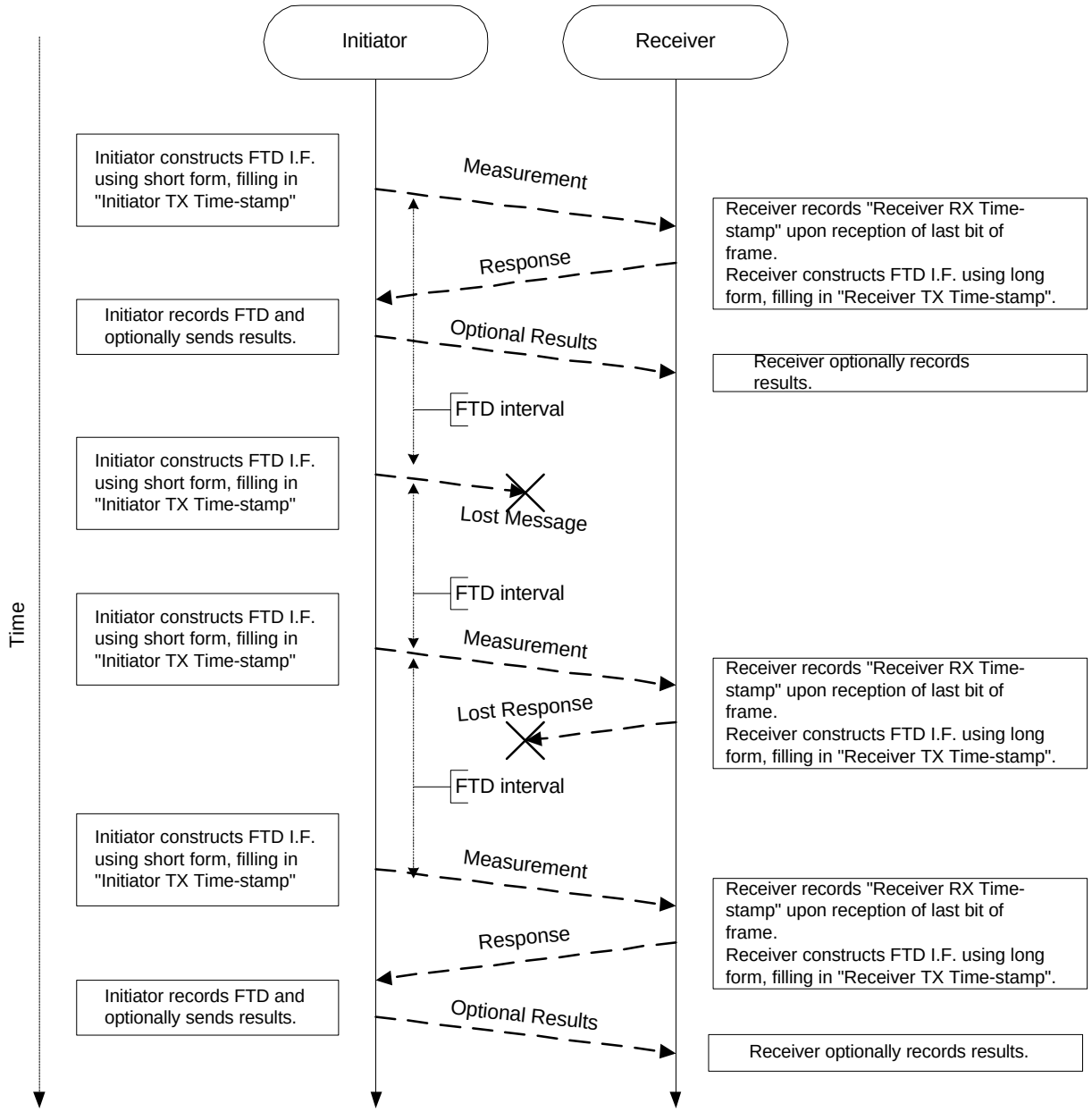


Figure B - 2 - Frame Transfer Delay Measurement

B.3 FDR/DDR Measurement

The FDR and DDR measurements may be performed periodically. An example of a FDR sequence is shown in Figure B - 3. The DDR measurement is done in the same fashion.

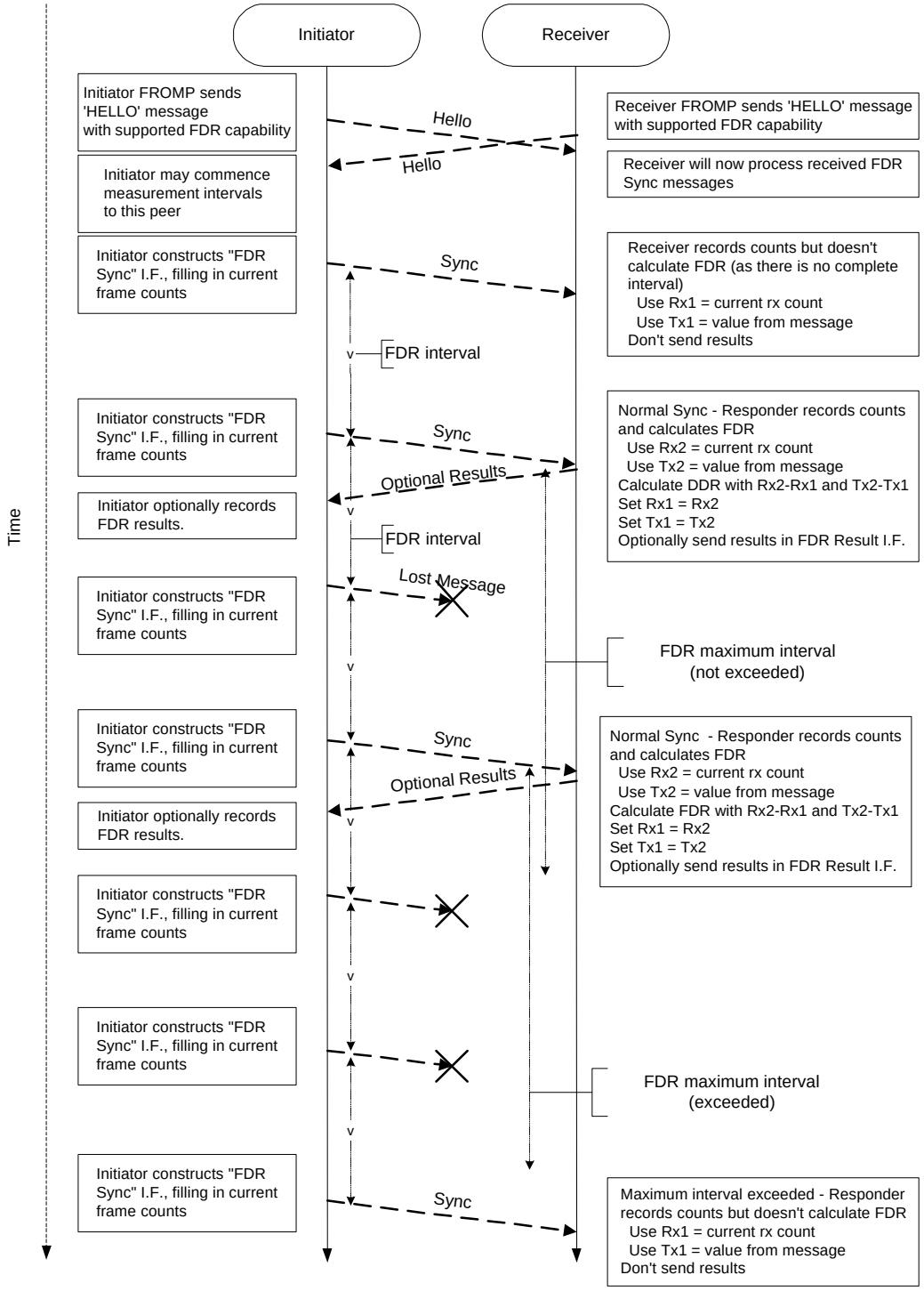


Figure B - 3 - FDR and DDR Measurements

B.4 Non-Latching Loopback

An example of the message sequencing for a device using the Non-Latching Loopback message is shown in Figure B - 4.

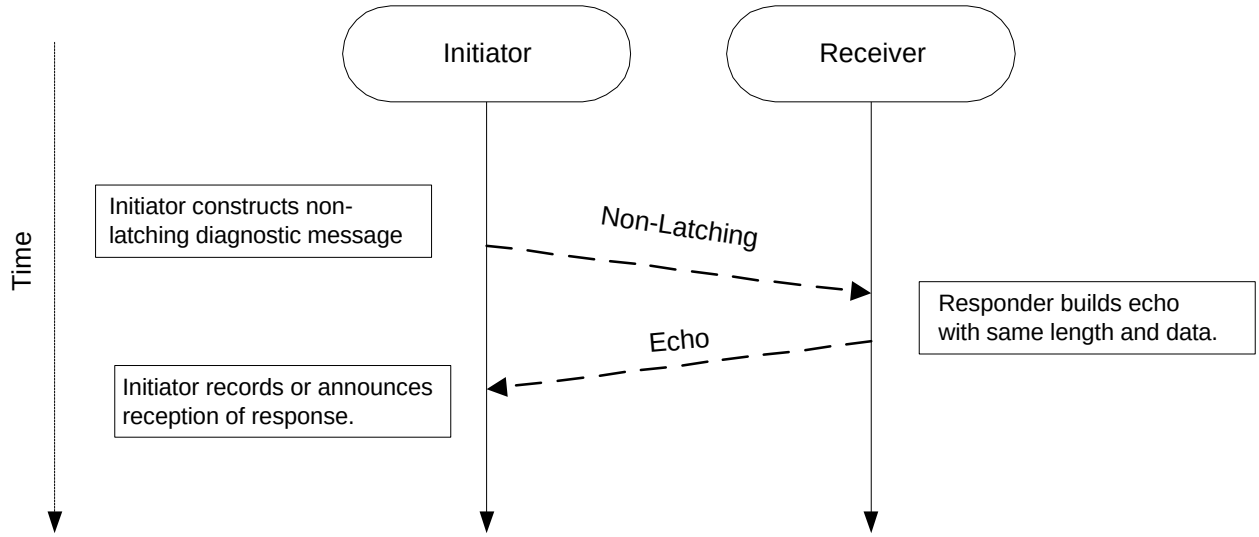


Figure B - 4 - Using the Non-Latching Loopback Message

B.5 Latching Loopback

Examples of message sequencing for a device using the Latching Loopback message are shown in Figure B - 5.

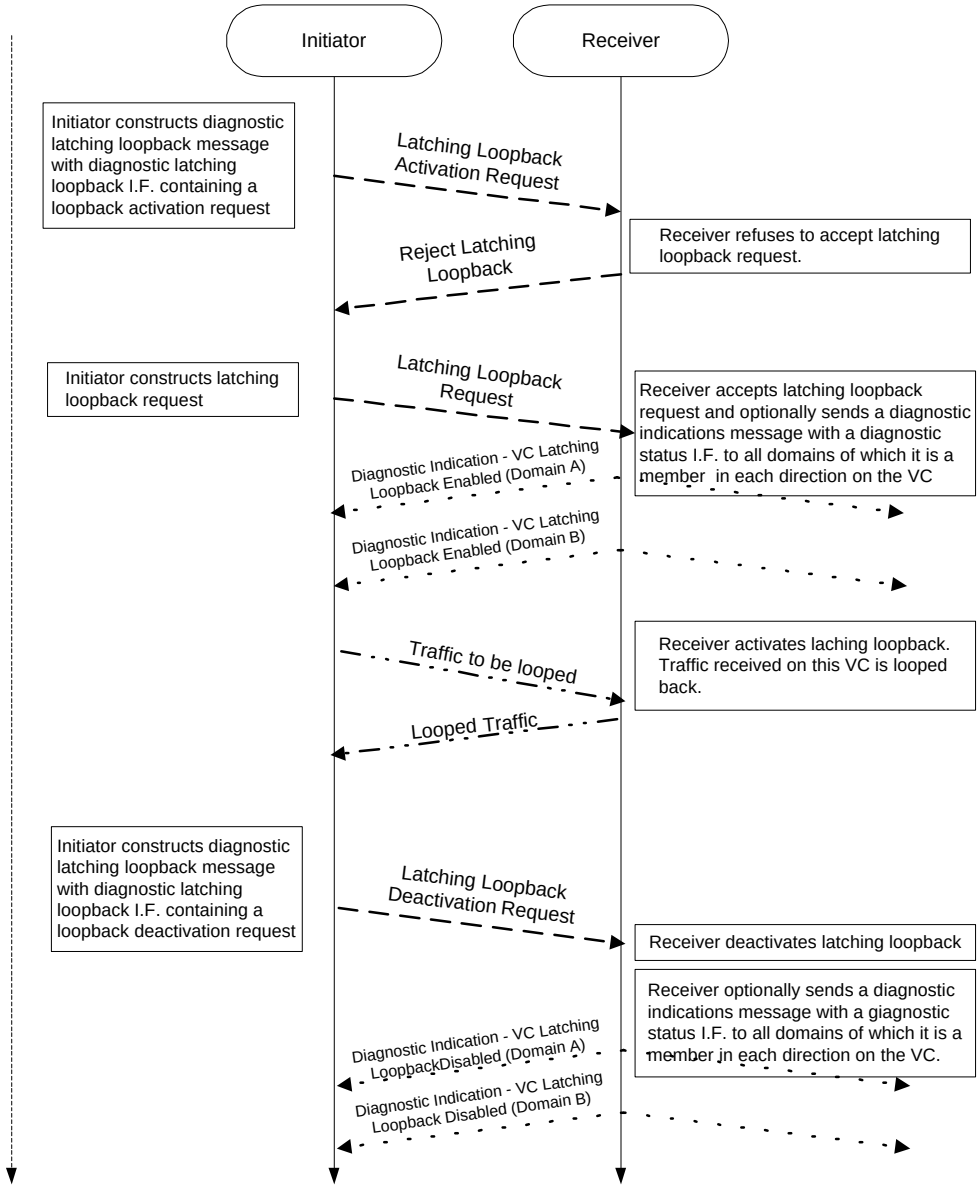


Figure B - 5 - Using the Latching Loopback Message

C Appendix – Example of Deliv ery Ratio Calculation

(Informative)

The method used for obtaining Frame Delivery Ratio and Data Delivery Ratio results depends upon implementation-specific choices beyond the scope of this IA. This Appendix presents one method of obtaining the data to calculate these ratios. Other methods are possible.

Frame Relay Service Level Agreements (SLAs) include expectations for Frame Delivery Ratio and Data Delivery Ratio performance. Delivery success ratios are possible for several grades of traffic, as shown in Table C - 1**.**

Traffic Grade	Description
Committed	frames transmitted to the network within the CIR
Excess	frames transmitted to the network in excess of CIR
Total	all frames transmitted to the network.

Table C - 1

This Annex describes a procedure to calculate delivery success ratios for each of the grades using the messages defined by the frame relay OA&M protocol. The procedure evaluates one-way delivery success between two Measurement Points (MP) in a network. The point where the frames enter the network segment is called the ingress MP. The point where the frames exit the network segment is called the egress MP. Refer to Figure C - 1 for a reference diagram of a typical circuit where Location A1 is the ingress MP and Location A2 is the egress MP. The procedure is independently executed for the reverse one-way flow to produce delivery success ratios for both directions. In the example shown in Figure C - 1, Location A2 becomes the ingress MP for the reverse one-way flow.

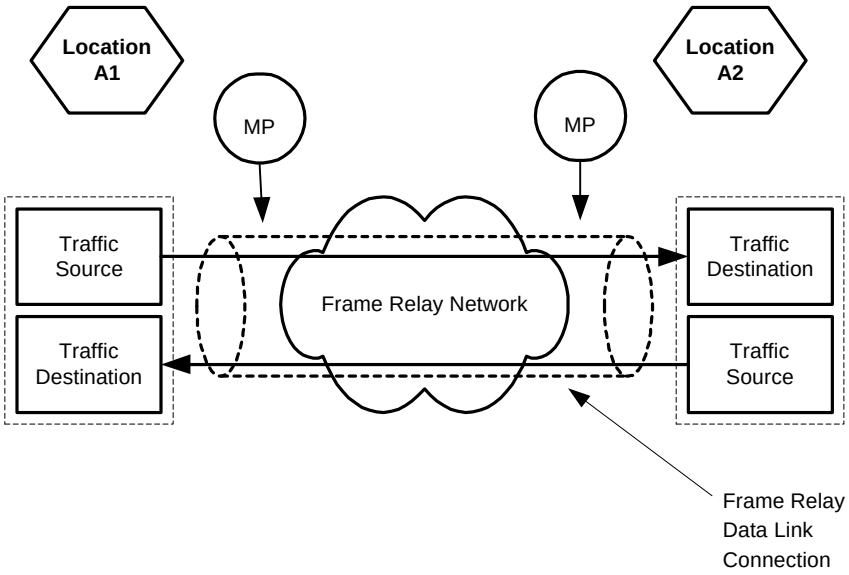


Figure C - 1

The operation of delivery success measurement occurs in time intervals determined by the ingress MP. The interval starts at T_0 following successful completion of the restart procedure (sections 4.4.4.1 and 4.4.5.1) or at the conclusion of the previous interval. Interval duration (T_d) is implementation-specific but bounded by counter-wrapping considerations. The egress MP uses received Service Verification messages containing a Frame Delivery Ratio Sync I.F. to detect the interval boundaries following completion of the restart procedure.

The following description of processing is focused on determination of Frame Delivery Ratio results. The technique is applicable to Data Delivery Ratio result calculation with the use of the appropriate Service Verification message information fields.

C.1 Ingress Processing

The ingress MP determines the traffic grade of a frame. The method used to assign frames to particular traffic grades is implementation-specific. A discussion of traffic classification is provided in ITU I.370 [2]. This method does not rely upon an indication of the assigned traffic grade of each individual frame to the egress processor. The ingress MP maintains a frame count for each traffic grade. Upon detection of a frame within a given traffic grade, the frame count for that grade is incremented by one. At time T_d, a Service Verification message containing a Frame Delivery Ratio Sync Information Field is transmitted from the ingress MP to the egress MP.

The Frame Delivery Ratio Sync I.F. contains two fields: $FramesOffered_{Committed}$ and $FramesOffered_{Excess}$. The fields contain the frame counts for the corresponding grades. The counts will wrap back to zero periodically, the frequency determined by physical access speed, frame sizes, and frame arrival rates.

C.2 Egress Processing

The egress MP counts frames exiting the network during an interval. A single count of total frames exiting the network is maintained, as the frames are NOT identified by Traffic Grade.

Upon receipt of a Service Verification message containing a Frame Delivery Ratio Sync I.F., the egress MP performs the following actions:

1. The running count of total frames exiting the network during the interval is assigned to FramesReceived.
2. The $FramesOffered_{Committed}$ Count for the interval is computed by subtracting the value reported by the ingress MP at the end of the last interval from the value reported by the ingress MP in the just received Service Verification message. The calculation **must** detect and adjust for counter-wrap.
3. The $FramesOffered_{Excess}$ Count for the interval is computed by subtracting the value reported by the ingress MP at the end of the last interval from the value reported by the ingress MP in the just received Service Verification message. The calculation **must** detect and adjust for counter-wrap.
4. The Total Lost Frame Count for the interval just ended is calculated as follows:

   $$FramesLost = (FramesOffered_{Committed} + FramesOffered_{Excess}) - FramesReceived$$

5. The counts of committed and excess frames delivered successfully are calculated as follows:

   If $FramesLost >= FramesOffered_{Excess}$

   $FramesDelivered_{Excess} = 0$

   $FramesDelivered_{Committed} = FramesReceived$

   If $FramesLost < FramesOffered_{Excess}$

   $FramesDelivered_{Excess} = FramesOffered_{Excess} - FramesLost$

   $FramesDelivered_{Committed} = FramesOffered_{Committed}$

6. The Frame Delivery Ratio for the Committed Traffic Grade is calculated as follows:

$$FDR_{committed} = FramesDelivered_{Committed} / FramesOffered_{Committed}$$

7. The Frame Delivery Ratio for the Excess Traffic Grade is calculated as follows:

$$FDR_{excess} = FramesDelivered_{Excess} / FramesOffered_{Excess}$$

8. The Frame Delivery Ratio for the Total Traffic Grade is calculated as follows:

$$FDR_{total} = FramesReceived / (FramesOffered_{Committed} + FramesOffered_{Excess})$$

9. The counts of committed and excess frames lost are calculated as follows:

$$FramesLost_{Committed} = FramesOffered_{Committed} - FramesDelivered_{Committed}$$

$$FramesLost_{Excess} = FramesOffered_{Excessd} - FramesDelivered_{Excess}$$