Mobile Ad hoc Networks Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 7, 2016

S. Ratliff
VT iDirect
S. Jury
Cisco Systems
D. Satterwhite
Broadcom
R. Taylor
Airbus Defence & Space
B. Berry
February 4, 2016

Dynamic Link Exchange Protocol (DLEP)
draft-ietf-manet-dlep-18

Abstract

When routing devices rely on modems to effect communications over wireless links, they need timely and accurate knowledge of the characteristics of the link (speed, state, etc.) in order to make routing decisions. In mobile or other environments where these characteristics change frequently, manual configurations or the inference of state through routing or transport protocols does not allow the router to make the best decisions. A bidirectional, event-driven communication channel between the router and the modem is necessary.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 7, 2016.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 4
1.1. Requirements 7
2. Protocol Overview 7
2.1. Assumptions 9
3. Destinations 9
3.1. Router-requested Destinations 10
4. Metrics 11
5. DLEP Session Flow 12
5.1. Peer Discovery State 12
5.2. Session Initialization State 14
5.3. In-Session State 15
5.3.1. Heartbeats 16
5.4. Session Termination State 16
5.5. Session Reset state 17
5.5.1. Unexpected TCP connection termination 17
6. Transaction Model 17
7. Extensions 18
7.1. Experiments 18
8. Scalability 19
9. DLEP Signal and Message Structure 19
9.1. DLEP Signal Header 20
9.2. DLEP Message Header 20
9.3. DLEP Generic Data Item 21
10. DLEP Signals and Messages 21
10.1. Peer Discovery Signal 22
10.2. Peer Offer Signal 23
10.3. Session Initialization Message 23
10.4. Session Initialization Response Message 24
10.5. Session Update Message 26
10.6. Session Update Response Message 27
10.7. Session Termination Message 28

10.8. Session Termination Response Message 28
10.9. Destination Up Message 28
10.10. Destination Up Response Message 30
10.11. Destination Announce Message 30
10.12. Destination Announce Response Message 31
10.13. Destination Down Message 32
10.14. Destination Down Response Message 32
10.15. Destination Update Message 33
10.16. Heartbeat Message 34
10.17. Link Characteristics Request Message 35
10.18. Link Characteristics Response Message 35
11. DLEP Data Items 37
11.1. Status 38
11.2. IPv4 Connection Point 40
11.3. IPv6 Connection Point 41
11.4. Peer Type 42
11.5. Heartbeat Interval 43
11.6. Extensions Supported 43
11.7. MAC Address 44
11.8. IPv4 Address 45
11.9. IPv6 Address 46
11.10. IPv4 Attached Subnet 47
11.11. IPv6 Attached Subnet 48
11.12. Maximum Data Rate (Receive) 49
11.13. Maximum Data Rate (Transmit) 49
11.14. Current Data Rate (Receive) 50
11.15. Current Data Rate (Transmit) 51
11.16. Latency 52
11.17. Resources (Receive) 52
11.18. Resources (Transmit) 53
11.19. Relative Link Quality (Receive) 54
11.20. Relative Link Quality (Transmit) 54
11.21. Maximum Transmission Unit (MTU) 55
12. Security Considerations 56
13. IANA Considerations 56
13.1. Registrations 56
13.2. Signal/Message Type Registration 57
13.3. DLEP Data Item Registrations 57
13.4. DLEP Status Code Registrations 57
13.5. DLEP Extensions Registrations 58
13.6. DLEP Well-known Port 58
13.7. DLEP IPv4 Link-local Multicast Address 58
13.8. DLEP IPv6 Link-local Multicast Address 58
14. Acknowledgements 58
15. References 59
15.1. Normative References 59
15.2. Informative References 59
Appendix A. Discovery Signal Flows 59

Appendix B. Peer Level Message Flows 60
B.1. Session Initialization 60
B.2. Session Initialization - Refused 61
B.3. Router Changes IP Addresses 61
B.4. Modem Changes Session-wide Metrics 61
B.5. Router Terminates Session 62
B.6. Modem Terminates Session 62
B.7. Session Heartbeats 63
B.8. Router Detects a Heartbeat timeout 64
B.9. Modem Detects a Heartbeat timeout 65
Appendix C. Destination Specific Message Flows 65
C.1. Common Destination Notification 65
C.2. Multicast Destination Notification 66
C.3. Link Characteristics Request 67
Authors' Addresses 68

1. Introduction

There exist today a collection of modem devices that control links of variable datarate and quality. Examples of these types of links include line-of-sight (LOS) terrestrial radios, satellite terminals, and broadband modems. Fluctuations in speed and quality of these links can occur due to configuration, or on a moment-to-moment basis, due to physical phenomena like multipath interference, obstructions, rain fade, etc. It is also quite possible that link quality and datarate vary with respect to individual destinations on a link, and with the type of traffic being sent. As an example, consider the case of an 802.11 access point, serving two associated laptop computers. In this environment, the answer to the question "What is the datarate on the 802.11 link?" is "It depends on which associated laptop we're talking about, and on what kind of traffic is being sent." While the first laptop, being physically close to the access point, may have a datarate of 54Mbps for unicast traffic, the other laptop, being relatively far away, or obstructed by some object, can simultaneously have a datarate of only 32Mbps for unicast. However, for multicast traffic sent from the access point, all traffic is sent at the base transmission rate (which is configurable, but depending on the model of the access point, is usually 24Mbps or less).

In addition to utilizing variable datarate links, mobile networks are challenged by the notion that link connectivity will come and go over time, without an effect on a router's interface state (Up or Down). Effectively utilizing a relatively short-lived connection is problematic in IP routed networks, as routing protocols tend to rely on interface state and independent timers at OSI Layer 3 to maintain network convergence (e.g., HELLO messages and/or recognition of DEAD routing adjacencies). These dynamic connections can be better utilized with an event-driven paradigm, where acquisition of a new

neighbor (or loss of an existing one) is signaled, as opposed to a paradigm driven by timers and/or interface state. DLEP not only implements such an event-driven paradigm, but does so over a local (1 hop) TCP session, which guarantees delivery of the event messages.

Another complicating factor for mobile networks are the different methods of physically connecting the modem devices to the router. Modems can be deployed as an interface card in a router's chassis, or as a standalone device connected to the router via Ethernet or serial link. In the case of Ethernet attachment, with existing protocols and techniques, routing software cannot be aware of convergence events occurring on the radio link (e.g., acquisition or loss of a potential routing neighbor), nor can the router be aware of the actual capacity of the link. This lack of awareness, along with the variability in datarate, leads to a situation where finding the (current) best route through the network to a given destination is difficult to establish and properly maintain. This is especially true of demand-based access schemes such as Demand Assigned Multiple Access (DAMA) implementations used on some satellite systems. With a DAMA-based system, additional datarate may be available, but will not be used unless the network devices emit traffic at a rate higher than the currently established rate. Increasing the traffic rate does not guarantee additional datarate will be allocated; rather, it may result in data loss and additional retransmissions on the link.

Addressing the challenges listed above, the co-authors have developed the Dynamic Link Exchange Protocol, or DLEP. The DLEP protocol runs between a router and its attached modem devices, allowing the modem to communicate link characteristics as they change, and convergence events (acquisition and loss of potential routing destinations). The following diagrams are used to illustrate the scope of DLEP packets.

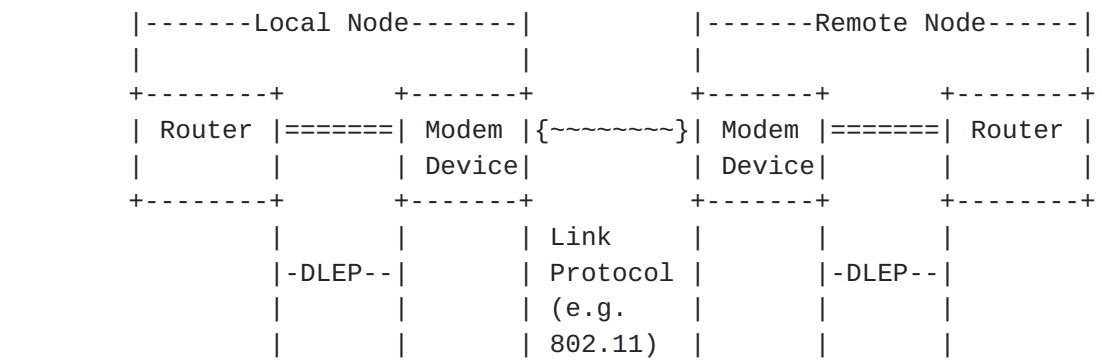


Figure 1: DLEP Network

In Figure 1, when the local modem detects the presence of a remote node, it (the local modem) sends a message to its router via the DLEP protocol. The message consists of an indication of what change has

occurred on the link (e.g., presence of a remote node detected), along with a collection of DLEP-defined Data Items that further describe the change. Upon receipt of the message, the local router may take whatever action it deems appropriate, such as initiating discovery protocols, and/or issuing HELLO messages to converge the network. On a continuing, as-needed basis, the modem devices use DLEP to report any characteristics of the link (datarate, latency, etc.) that have changed. DLEP is independent of the link type and topology supported by the modem. Note that the DLEP protocol is specified to run only on the local link between router and modem. Some over the air signaling may be necessary between the local and remote modem in order to provide some parameters in DLEP messages between the local modem and local router, but DLEP does not specify how such over the air signaling is carried out. Over the air signaling is purely a matter for the modem implementer.

Figure 2 shows how DLEP can support a configuration where routers are connected with different link types. In this example, Modem A implements a point-to-point link, and Modem B is connected via a shared medium. In both cases, the DLEP protocol is used to report the characteristics of the link (datarate, latency, etc.) to routers. The modem is also able to use the DLEP session to notify the router when the remote node is lost, shortening the time required to re-converge the network.

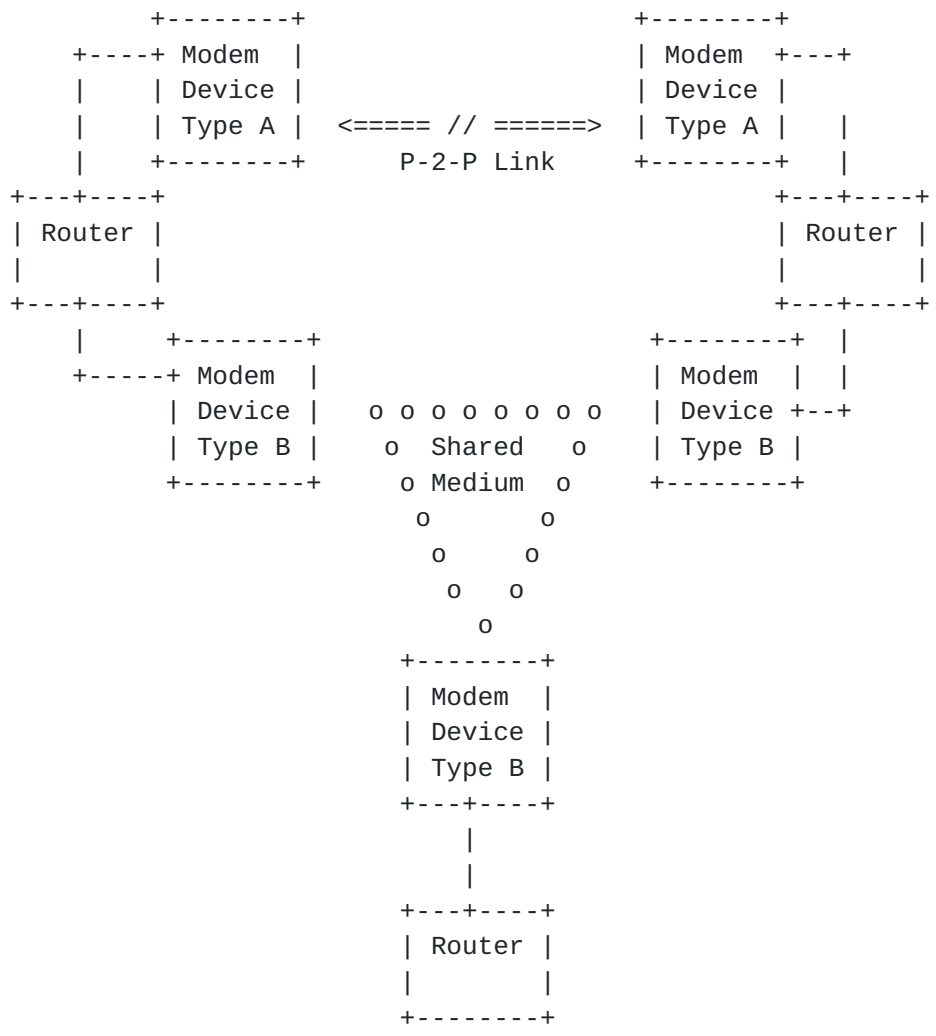


Figure 2: DLEP Network with Multiple Modem Devices

1.1. Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

2. Protocol Overview

DLEP defines a set of messages used by modems and their attached routers to communicate events that occur on the physical link(s) managed by the modem: for example, a remote node entering or leaving the network, or that the link has changed. Associated with these messages are a set of Data Items - information that describes the remote node (e.g., address information), and/or the characteristics of the link to the remote node. Throughout this document, we refer

to a modems/routers participating in a DLEP session as 'DLEP Peers', unless a specific distinction (e.g. modem or router) is required.

DLEP uses a session-oriented paradigm between the modem device and its associated router. If multiple modem devices are attached to a router (as in Figure 2), or the modem supports multiple connections (via multiple logical or physical interfaces), then separate DLEP sessions exist for each modem or connection. A router and modem form a session by completing the discovery and initialization process. This router-modem session persists unless or until it either (1) times out, based on the absence of traffic (including heartbeats), or (2) is explicitly torn down by one of the participants.

The router/modem session provides a carrier for information exchange concerning 'destinations' that are available via the modem device. Destinations can be identified by either the router or the modem, and represent a specific, addressable location that can be reached via the link(s) managed by the modem. A destination can be either physical or logical.

The example of a physical destination would be that of a remote, far-end router attached via the variable-quality network.

The example of a logical destination is Multicast. Multicast traffic destined for the variable-quality network (the network accessed via the modem) is handled in IP networks by deriving a Layer 2 MAC address based on the Layer 3 address. Leveraging on this scheme, multicast traffic is supported in DLEP simply by treating the derived MAC address as any other destination in the network. To support these logical destinations, one of the DLEP participants (typically, the router) informs the other as to the existence of the logical destination. The modem, once it is aware of the existence of this logical destination, reports link characteristics just as it would for any other destination in the network. The specific algorithms a modem would use to derive metrics on logical destinations are outside the scope of this specification, and is left to specific implementations to decide.

The DLEP messages concerning destinations thus become the way for routers and modems to maintain, and notify each other about, an information base representing the physical and logical destinations accessible via the modem device, as well as the link characteristics to those destinations.

While this document represents the best efforts of the working group to be functionally complete, it is recognized that extensions to DLEP will in all likelihood be necessary as more link types are used. Such extensions are defined as additional rules of behavior,

messages, data items and/or status codes that are not defined in this document. DLEP contains a standard mechanism for router and modem implementations to negotiate the available extensions to use on a per-session basis.

2.1. Assumptions

DLEP specifies UDP multicast for single-hop discovery signaling, and TCP for transport of the control messages. Therefore, DLEP assumes that the modem and router have topologically consistent IP addresses assigned. It is RECOMMENDED that DLEP implementations utilize IPv6 link-local addresses to reduce the administrative burden of address assignment. DLEP relies on the guaranteed- delivery of its messages between router and modem, once the 1 hop discovery process is complete, hence, the specification of TCP to carry the messages. Other reliable transports for the protocol are possible, but are outside the scope of this document.

DLEP assumes that the MAC address for delivering data traffic is the MAC address used by DLEP to identify the destination. No manipulation or substitution is performed; the MAC address supplied in all destination messages is used as the OSI Layer 2 Destination MAC address. DLEP also assumes that MAC addresses are unique within the context of a router-modem session.

The reliance on MAC addresses by DLEP forces the assumption that participating DLEP peers are on a single segment (either physical or logically, via tunneling protocols) at Layer 2. DLEP further assumes that security of the implementations (e.g., authentication of stations, encryption of traffic, or both) is dealt with by by utilizing Layer 2 security techniques. This reliance on Layer 2 mechanisms secures all DLEP messages - both the UDP discovery messages and the TCP control messages.

3. Destinations

Destination messages describe the acquisition and loss of network destinations, and control the flow of information about the destinations in the several ways. A destination MUST contain a MAC address; it MAY optionally include a Layer 3 address (or multiple addresses). The MAC address MAY reference a logical destination, as in a derived multicast MAC address, as well as a physical device. As destinations are discovered, DLEP routers and modems build an information base of destinations accessible via the modem.

DLEP can support MAC addresses in either EUI-48 or EUI-64 format, with the restriction that all MAC addresses for a given DLEP session MUST be in the same format, and MUST be consistent with the MAC

address format of the connected modem (e.g., if the modem is connected to the router with an EUI-48 MAC, all destination addresses via that modem MUST be expressed in EUI-48 format).

Destination messages trigger creation/maintenance/deletion of destinations in the information base of the recipient. For example, a modem will inform its attached router of the presence of a new destination via the Destination Up message (Section 10.9). Receipt of a Destination Up causes the router to allocate the necessary resources, creating an entry in the information base with the specifics (i.e. MAC Address, Latency, Data Rate, etc.) of the destination. The loss of a destination is communicated via the Destination Down message (Section 10.13), and changes in status to the destination (e.g., varying link quality, or addressing changes) are communicated via the Destination Update message (Section 10.15).

The information on a given destination will persist in the implementation's information base until a Destination Down message is received, indicating that the peer has lost contact or interest with the remote node, or the implementation transitions to the Session Termination state.

3.1. Router-requested Destinations

Usually a modem will discover the presence of one or more remote router/modem pairs and announce each destination's arrival by sending a corresponding Destination Up message to its peer. However, there may be times when a router wishes to express an interest in the status of the link to a logical destination that has yet to be announced, typically a multicast destination. To facilitate this, DLEP provides the Destination Announce (Section 10.11) and Destination Announce Response (Section 10.12) messages. These messages have similar semantics to the Destination Up and Destination Up Response messages, but flow from router to modem.

After successfully receiving and processing a Destination Announce message, a modem then announces changes to the link to the logical destination via Destination Update messages. A modem MAY refuse a Destination Announce message by replying with a Destination Announce Response message with a 'Request Denied' status code, see Table 3.

A Destination Announce message MAY also be used by a router to request information concerning a destination that it has previously declined interest in, via the 'Not Interested' status code, see Table 3, or declared as down, via the Destination Down message.

One of the advantages of implementing DLEP is to leverage the modem's knowledge of the links between remote destinations allowing routers

to avoid using probed neighbor discovery techniques, therefore modem implementations SHOULD announce available destinations via the Destination Up message, rather than relying on Destination Announce messages.

4. Metrics

DLEP includes the ability for the router and modem to communicate metrics that reflect the characteristics (e.g., datarate, latency) of the variable-quality link in use. DLEP does not specify how a given metric value is to be calculated, rather, the protocol assumes that metrics have been calculated by a 'best effort', incorporating all pertinent data that is available to the modem device.

DLEP allows for metrics to be sent within two contexts - metrics for a specific destination within the network (e.g., a specific router), and per-session (those that apply to all destinations accessed via the modem). Most metrics can be further subdivided into transmit and receive metrics. In cases where metrics are provided at session level, the router MUST propagate the metrics to all entries in its information base for destinations that are accessed via the modem.

DLEP modem implementations MUST announce all metric items that will be reported during the session, and provide default values for those metrics, in the Session Initialization Response message (Section 10.4). In order to use a metric type that was not included in the Session Initialization Response message, modem implementations MUST terminate the session with the router (via the Session Terminate message (Section 10.7)), and establish a new session. A modem MUST include the following list of metrics in the Session Initialization Response message:

- Maximum Data Rate (Receive) (Section 11.12)
- Maximum Data Rate (Transmit) (Section 11.13)
- Current Data Rate (Receive) (Section 11.14)
- Current Data Rate (Transmit) (Section 11.15)
- Latency (Section 11.16)

A DLEP modem MAY send metrics both in a session context (via the Session Update message) and a specific destination context (via Destination Update) at any time. The most recently received metric value MUST take precedence over any earlier value, regardless of context - that is:

1. If the router receives metrics in a specific destination context (via the Destination Update message), then the specific destination is updated with the new metric.

2. If the router receives metrics in a modem-wide context (via the Session Update message), then the metrics for all destinations accessed via the modem MUST be updated with the new metric.

It is left to implementations to choose sensible default values based on their specific characteristics. Modems having static (non-changing) link metric characteristics MAY report metrics only once for a given destination (or once on a modem-wide basis, if all connections via the modem are of this static nature).

In addition to communicating existing metrics about the link, DLEP provides a message allowing a router to request a different datarate or latency from the modem. This message is the Link Characteristics Request message (Section 10.17), and gives the router the ability to deal with requisite increases (or decreases) of allocated datarate/latency in demand-based schemes in a more deterministic manner.

5. DLEP Session Flow

All Peers participating in a DLEP session transition through five (5) distinct states during the lifetime of a DLEP session:

- Peer Discovery
- Session Initialization
- In-Session
- Session Termination
- Session Reset

The Peer Discovery state is OPTIONAL to implement for routers. If it is used, this state is the initial state. If it is not used, then a preconfigured TCP address/port combination MUST be provided to the router, and the router starts in the Session Initialization state.

Modems MUST support the Peer Discovery state.

5.1. Peer Discovery State

In the Peer Discovery state, if the router implementation supports IPv6, it SHOULD send UDP packets containing a Peer Discovery signal (Section 10.1) to the DLEP well-known IPv6 link-local multicast

address (Section 13.8) and port number (Section 13.6), setting the packet source address to a valid IPv6 link-local address and the source port to a valid port number.

If the router implementation supports IPv4, it SHOULD send UDP packets containing a Peer Discovery signal (Section 10.1) to the DLEP well-known IPv4 link-local multicast address (Section 13.7) and port number (Section 13.6), setting the packet source address to a valid local IPv4 address and the source port to a valid port number.

The implementation then waits for a unicast UDP packet containing a Peer Offer signal (Section 10.2) from a potential DLEP peer modem. While in the Peer Discovery state, Peer Discovery signals MUST be sent repeatedly by a DLEP router, at regular intervals. The interval MUST be a minimum of one second; it SHOULD be a configurable parameter. Note that this operation (sending Peer Discovery and waiting for Peer Offer) is outside the DLEP Transaction Model, as the Transaction Model only describes messages on a TCP session.

In the Peer Discovery state, the DLEP modem implementation MUST listen for incoming Peer Discovery signals on the DLEP well-known link-local multicast address and port. The choice of using the well-known IPv4 or the IPv6 well- known link-local multicast address and port MUST be made by configuration. On receipt of a valid Peer Discovery signal, it MUST unicast a Peer Offer signal to the source address and port of the received UDP packet. Peer Offer signals MAY contain one or more unicast address/port combinations for TCP-based communication with the modem, via the IPv4 Connection Point data item (Section 11.2) or the IPv6 Connection Point data item (Section 11.3), on which it is prepared to accept an incoming TCP connection. If the modem does not include an IPv4 Connection Point data item, nor a IPv6 Connection Point data item, then the source address of the packet containing the Peer Offer signal MUST be used as the address on which the modem is willing to accept TCP connections.

Upon establishment of a TCP connection, both modem and router enter the Session Initialization state. Anything other than Peer Discovery signals received on the UDP socket MUST be silently dropped.

Modems MUST be prepared to accept a TCP connection from a router that is not using the Discovery mechanism, i.e. a connection attempt that occurs without a preceding Peer Discovery signal.

Routers MUST use one or more of the modem address/port combinations from the Peer Offer signal or from a priori configuration to establish a new TCP connection to the modem. If more than one modem address/port combinations is available, router implementations MAY use their own heuristics to determine the order in which they are

tried. It is RECOMMENDED that an implementation attempt to connect to any announced IPv6 address/port combinations before attempting to use IPv4 combinations. If a TCP connection cannot be achieved using any of the address/port combinations and the Discovery mechanism is in use, then the router SHOULD resume issuing Peer Discovery signals. If no IPv4 Connection Point data items, nor IPv6 Connection Point data items are included in the Peer Offer signal, the router MUST use the origin address of the UDP packet containing the signal as the IP address, and the DLEP well-known port number.

Once a TCP connection has been established with the modem, the router begins a new session and enters the Session Initialization state. It is up to the router implementation if Peer Discovery signals continue to be sent after the device has transitioned to the Session Initialization state.

5.2. Session Initialization State

On entering the Session Initialization state, the router MUST send a Session Initialization message (Section 10.3) to the modem. The router MUST then wait for receipt of a Session Initialization Response message (Section 10.4) from the modem. Receipt of the Session Initialization Response message containing a Status data item (Section 11.1) with value 'Success', see Table 3, indicates that the modem has received and processed the Session Initialization message, and the router MUST transition to the In-Session state.

On entering the Session Initialization state, the modem MUST wait for receipt of a Session Initialization message from the router. Upon receipt of a Session Initialization message, the modem MUST send a Session Initialization Response message, and the session MUST transition to the In-Session state.

DLEP provides an extension negotiation capability to be used in the Session Initialization state, see Section 7. Extensions supported by an implementation MUST be declared to potential DLEP peers using the Extensions Supported data item (Section 11.6). Once both participants have exchanged initialization messages, an implementation MUST NOT emit any message, signal, data item or status code associated with an extension that was not specified in the received initialization message from its peer.

If the router receives any message other than a valid Session Initialization Response, it MUST send a Session Termination message (Section 10.7) with the 'Unexpected Message' status code, see Table 3, and transition to the Session Termination state.

If the modem receives any message other than Session Initialization, or it fails to parse the received message, it MUST NOT send any message, and MUST terminate the TCP connection and transition to the Session Reset state.

If an additional metric is to be introduced after the session has started, the session between router and modem MUST be terminated and restarted, and the new metric described in the next Session Initialization Response message.

5.3. In-Session State

In the In-Session state, messages can flow in both directions between participants, indicating changes to the session state, the arrival or departure of reachable destinations, or changes of the state of the links to the destinations.

The In-Session state is maintained until one of the following conditions occur:

- A peer terminates the session by sending a Session Termination message (Section 10.7)), or,
- The peer terminates the session, indicated by receiving a Session Termination message.

The peer MUST then transition to the Session Termination state.

Prior to the exchange of Destination Up (Section 10.9) and Destination Up Response (Section 10.10) messages, or Destination Announce (Section 10.11) and Destination Announce Response (Section 10.12) messages, no messages concerning the logical destination identified by the MAC Address data item (Section 11.7) may be sent. A peer receiving any message with such an unannounced destination MUST terminate the session by issuing a Session Termination message (Section 10.7) with a status code of 'Invalid Destination', see Table 3, and transition to the Session Termination state.

The router receiving a Destination Up message MAY decline further messages concerning a given destination by sending a Destination Up Response with a status code of 'Not Interested'. Modems receiving such responses MUST NOT send further messages concerning that destination to the router.

After exchanging Destination Down (Section 10.13) and Destination Down Response (Section 10.14) messages, no messages concerning the logical destination identified by the MAC Address data item may be a

sent without previously sending a new Destination Up message. A peer receiving a message about a destination previously announced as 'down' MUST terminate the session by issuing a Session Termination message with a status code of 'Invalid Destination' and transition to the Session Termination state.

5.3.1. Heartbeats

In order to maintain the In-Session state, periodic Heartbeat messages (Section 10.16) MAY be exchanged between router and modem. These messages are intended to keep the session alive, and to verify bidirectional connectivity between the two participants.

If Heartbeat messages are used, the following processing rules MUST apply:

- Each DLEP peer is responsible for the creation of heartbeat messages.
- Receipt of any valid DLEP message MUST reset the heartbeat interval timer (i.e., valid DLEP messages take the place of, and obviate the need for, additional Heartbeat messages).
- DLEP peers SHOULD allow two (2) heartbeat intervals to expire with no messages from the peer before terminating the session by issuing a Session Termination message with a status code of 'Timed Out', and then transition to the Session Termination state.

5.4. Session Termination State

When a DLEP implementation enters the Session Termination state after sending a Session Termination message (Section 10.7) as the result of an invalid message or error, it MUST wait for a Session Termination Response message (Section 10.8) from its peer. If Heartbeat messages (Section 10.16) are in use, senders SHOULD allow four (4) heartbeat intervals to expire before assuming that the peer is unresponsive, and continuing with session termination. If Heartbeat messages are not in use, then if is RECOMMENDED that an interval of eight (8) seconds be used.

When the sender of the Session Termination message receives a Session Termination Response message from its peer, or times out, it MUST transition to the Session Reset state.

When an implementation enters the Session Termination state having received a Session Termination message from its peer, it MUST immediately send a Session Termination Response and transition to the Session Reset state.

Any messages received after either sending or receiving a Session Termination message MUST be silently ignored.

5.5. Session Reset state

In the Session Reset state the implementation MUST perform the following actions:

- Release all resources allocated for the session.
- Eliminate all destinations in the information base accessible via the modem represented by the session. Destination Down messages (Section 10.13) MUST NOT be sent.
- Terminate the TCP connection.

Having completed these actions the implementation SHOULD return to the relevant initial state: Peer Discovery for modems; either Peer Discovery or Session Initialization for routers, depending on configuration.

5.5.1. Unexpected TCP connection termination

If the TCP connection between peers is terminated when a participant is not in the Session Reset state, the implementation MUST immediately transition to the Session Reset state.

6. Transaction Model

DLEP defines a simple message transaction model: Only one request per destination may be in progress at a time. A message transaction is considered complete when a response matching a previously issued request is received. If a participant receives a request for a destination for which there is already an outstanding request, the implementation MUST terminate the session by issuing a Session Termination message (Section 10.7) with a status code of 'Unexpected Message', see Table 3, and transition to the Session Termination state. There is no restriction to the total number of message transactions in progress at a time, as long as each transaction refers to a different destination.

It should be noted that some requests may take a considerable amount of time for some participants to complete, for example a modem handling a multicast destination up request may have to perform a complex network reconfiguration. A sending implementation MUST be able to handle such long running transactions gracefully.

Additionally, only one session request, e.g. a Session Initialization message (Section 10.3) may be in progress at a time. As above, a session transaction is considered complete when a response matching a previously issued request is received. If a participant receives a session request while there is already a session request in progress, it MUST terminate the session by issuing a Session Termination message with a status code of 'Unexpected Message', and transition to the Session Termination state. Only the Session Termination message may be issued when a session transaction is in progress. Heartbeat messages (Section 10.16) MUST NOT be considered part of a session transaction.

DLEP transactions do not time out and are not cancellable. An implementation can detect if its peer has failed in some way by use of the session heartbeat mechanism during the In-Session state, see Section 5.3.

7. Extensions

Extensions MUST be negotiated on a per-session basis during session initialization via the Extensions Supported mechanism. Implementations are not required to support any extension in order to be considered DLEP compliant. An extension document, describing the operation of a credit windowing scheme for flow control, is described in [CREDIT].

If interoperable protocol extensions are required, they MUST be standardized either as an update to this document, or as an additional stand-alone specification. The requests for IANA-controlled registries in this document contain sufficient Reserved space for DLEP signals, messages, data items and status codes to accommodate future extensions to the protocol.

As multiple protocol extensions MAY be announced during session initialization, authors of protocol extensions MUST consider the interaction of their extension with other published extensions, and specify any incompatibilities.

7.1. Experiments

This document requests Private Use numbering space in the DLEP signal/message, data item and status code registries for experimental extensions. The intent is to allow for experimentation with new signals, messages, data items, and/or status codes, while still retaining the documented DLEP behavior.

Use of the Private Use signals, messages, data items, status codes, or behaviors MUST be announced as DLEP Extensions, during session

initialization, using extension identifiers from the Private Use space in the Extensions Supported registry (Table 4), with a value agreed upon (a priori) between the participating peers. DLEP extensions using the Private Use numbering space are commonly referred to as Experiments.

Multiple experiments MAY be announced in the Session Initialization messages. However, use of multiple experiments in a single session could lead to interoperability issues or unexpected results (e.g., clashes of experimental signals, messages, data items and/or status code types), and is therefore discouraged. It is left to implementations to determine the correct processing path (e.g., a decision on whether to terminate the session, or to establish a precedence of the conflicting definitions) if such conflicts arise.

8. Scalability

The protocol is intended to support thousands of destinations on a given modem/router pair. At large scale, implementations SHOULD consider employing techniques to prevent flooding a peer with a large number of messages in a short time. It is recommended that implementations consider a dampening algorithm to prevent a flapping device from generating a large number of Destination Up/Destination Down messages, for example. Implementations SHOULD also consider techniques such as a hysteresis to lessen the impact of rapid, minor fluctuations in link quality. The specific algorithms to be used for handling flapping destinations and minor changes in link quality are outside the scope of this specification.

9. DLEP Signal and Message Structure

DLEP defines two protocol units used in two different ways: Signals and Messages. Signals are only used in the Discovery mechanism and are carried in UDP datagrams. Messages are used bi-directionally over a TCP connection between two peers, in the Session Initialization, In-Session and Session Termination states.

Both signals and messages consist of a header followed by an unordered list of data items. Headers consist of Type and Length information, while data items are encoded as TLV (Type-Length-Value) structures. In this document, the data items following a signal or message header are described as being 'contained in' the signal or message.

There is no restriction on the order of data items following a header, and the multiplicity of duplicate data items is defined by the definition of the signal or message declared by the type in the header.

All integers in header fields and values MUST be in network byte-order.

9.1. DLEP Signal Header

The DLEP signal header contains the following fields:

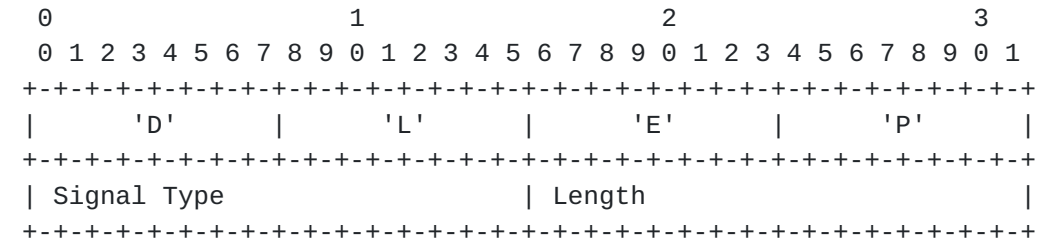


Figure 3: DLEP Signal Header

"DLEP": Every signal MUST start with the characters: U+44, U+4C, U+45, U+50.

Signal Type: An 16-bit unsigned integer containing one of the DLEP Signal/Message Type values defined in this document.

Length: The length in octets, expressed as a 16-bit unsigned integer, of all of the DLEP data items associated with this signal. This length SHALL NOT include the length of the header itself.

The DLEP signal header is immediately followed by one or more DLEP data items, encoded in TLVs, as defined in this document.

If an unrecognized, or unexpected signal is received, or a received signal contains unrecognized, invalid, or disallowed duplicate data items, the receiving participant MUST ignore the signal.

9.2. DLEP Message Header

The DLEP message header contains the following fields:

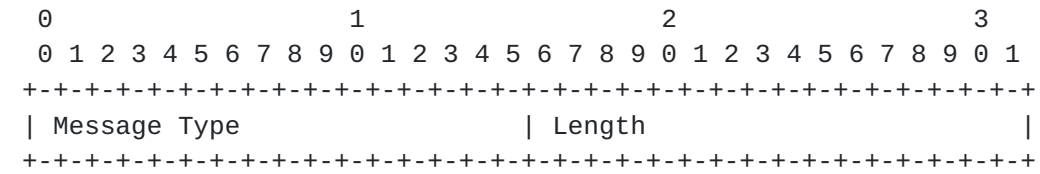


Figure 4: DLEP Message Header

Message Type: An 16-bit unsigned integer containing one of the DLEP Signal/Message Type values defined in this document.

Length: The length in octets, expressed as a 16-bit unsigned integer, of all of the DLEP data items associated with this message. This length SHALL NOT include the length of the header itself.

The DLEP message header is immediately followed by one or more DLEP data items, encoded in TLVs, as defined in this document.

If an unrecognized, or unexpected message is received, or a received message contains unrecognized, invalid, or disallowed duplicate data items, the receiving participant MUST issue a Session Termination message (Section 10.7) with a Status data item (Section 11.1) containing the most relevant status code, see Table 3, and transition to the Session Termination state.

9.3. DLEP Generic Data Item

All DLEP data items contain the following fields:

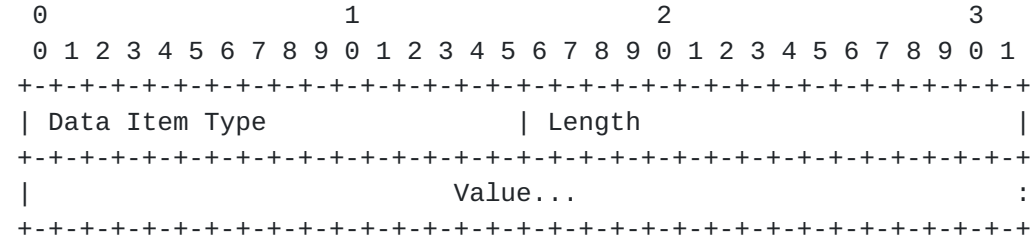


Figure 5: DLEP Generic Data Item

Data Item Type: An 16-bit unsigned integer field specifying the type of data item being sent.

Length: The length in octets, expressed as an 16-bit unsigned integer, of the value field of the data item. This length SHALL NOT include the length of the header itself.

Value: A field of <Length> octets, which contains data specific to a particular data item.

10. DLEP Signals and Messages

As mentioned above, all DLEP signals begin with the DLEP signal header, and all DLEP messages begin with the DLEP message header.

Therefore, in the following descriptions of specific signals and messages, this header is assumed, and will not be replicated.

Following is the set of core signals and messages that MUST be recognized by a DLEP compliant implementation. As mentioned before, not all messages may be used during a session, but an implementation MUST correctly process these messages when received.

The core DLEP signals and messages are:

Type Code	Description
0	Reserved
1	Peer Discovery signal (Section 10.1)
2	Peer Offer signal (Section 10.2)
3	Session Initialization message (Section 10.3)
4	Session Initialization Response message (Section 10.4)
5	Session Update message (Section 10.5)
6	Session Update Response message (Section 10.6)
7	Session Termination message (Section 10.7)
8	Session Termination Response message (Section 10.8)
9	Destination Up message (Section 10.9)
10	Destination Up Response message (Section 10.10)
11	Destination Down message (Section 10.13)
12	Destination Down Response message (Section 10.14)
13	Destination Update message (Section 10.15)
14	Heartbeat message (Section 10.16)
15	Link Characteristics Request message (Section 10.17)
16	Link Characteristics Response message (Section 10.18)
17	Destination Announce message (Section 10.11)
18	Destination Announce Response message (Section 10.12)
19-65519	Reserved for future extensions
65520-65534	Private Use. Available for experiments
65535	Reserved

Table 1: DLEP Signal/Message types

10.1. Peer Discovery Signal

A Peer Discovery signal SHOULD be sent by a DLEP router to discover DLEP modems in the network. The Peer Offer signal (Section 10.2) is required to complete the discovery process. Implementations MUST

implement their own retransmit heuristics in cases where it is determined the Peer Discovery signal has timed out.

To construct a Peer Discovery signal, the Signal Type value in the signal header is set to 1, from Table 1.

The Peer Discovery signal MAY contain the following data item:

- Peer Type (Section 11.4)

10.2. Peer Offer Signal

A Peer Offer signal MUST be sent by a DLEP modem in response to a valid Peer Discovery signal (Section 10.1).

The Peer Offer signal MUST be sent to the unicast address of the originator of the Peer Discovery signal.

To construct a Peer Offer signal, the Signal Type value in the signal header is set to 2, from Table 1.

The Peer Offer signal MAY contain the following data item:

- Peer Type (Section 11.4)

The Peer Offer signal MAY contain one or more of any of the following data items, with different values:

- IPv4 Connection Point (Section 11.2)

- IPv6 Connection Point (Section 11.3)

The IP Connection Point data items indicate the unicast address the router MUST use when connecting the DLEP TCP session. If multiple IP Connection Point data items are present in the Peer Offer signal, router implementations MAY use their own heuristics to select the address to connect to. If no IP Connection Point data items are included in the Peer Offer signal, the router MUST use the origin address of the signal as the IP address, and the DLEP well-known port number (Section 13.6) to establish the TCP connection.

10.3. Session Initialization Message

A Session Initialization message MUST be sent by a DLEP router as the first message of the DLEP TCP session. It is sent by the router after a TCP connect to an address/port combination that was obtained either via receipt of a Peer Offer, or from a priori configuration.

If any optional extensions are supported by the implementation, they MUST be enumerated in the Extensions Supported data item. If an Extensions Supported data item does not exist in a Session Initialization message, the modem MUST conclude that there is no support for extensions in the router.

Implementations supporting the Heartbeat Interval (Section 11.5) should understand that heartbeats are not fully established until receipt of Session Initialization Response message (Section 10.4), and should therefore implement their own timeout and retry heuristics for this message.

To construct a Session Initialization message, the Message Type value in the message header is set to 3, from Table 1.

The Session Initialization message MUST contain one of each of the following data items:

- Heartbeat Interval (Section 11.5)

The Session Initialization message MAY contain one of each of the following data items:

- Peer Type (Section 11.4)

- Extensions Supported (Section 11.6)

A Session Initialization message MUST be acknowledged by the modem issuing a Session Initialization Response message (Section 10.4).

As an exception to the general rule that an implementation receiving an unrecognized data item in a message terminating the session with an error, see Section 9.2, if a Session Initialization message contains one or more Extension Supported data items announcing support for extensions that the implementation does not recognize, then the implementation MAY ignore data items it does not recognize.

10.4. Session Initialization Response Message

A Session Initialization Response message MUST be sent in response to a received Session Initialization message (Section 10.3). The Session Initialization Response message completes the DLEP session establishment; the modem should transition to the In-Session state when the message is sent, and the router should transition to the In-Session state upon receipt of an acceptable Session Initialization Response message.

All supported metric data items MUST be included in the Session Initialization Response message, with default values to be used on a 'modem-wide' basis. This can be viewed as the modem 'declaring' all supported metrics at DLEP session initialization. Receipt of any DLEP message containing a metric data item not included in the Session Initialization Response message MUST be treated as an error, resulting in the termination of the DLEP session between router and modem.

If any optional extensions are supported by the modem, they MUST be enumerated in the Extensions Supported data item. If an Extensions Supported data item does not exist in a Session Initialization Response message, the router MUST conclude that there is no support for extensions in the modem.

After the Session Initialization/Session Initialization Response messages have been successfully exchanged, implementations MUST only use extensions that are supported by BOTH participants.

To construct a Session Initialization Response message, the Message Type value in the message header is set to 4, from Table 1.

The Session Initialization Response message MUST contain one of each of the following data items:

- Heartbeat Interval (Section 11.5)
- Maximum Data Rate (Receive) (Section 11.12)
- Maximum Data Rate (Transmit) (Section 11.13)
- Current Data Rate (Receive) (Section 11.14)
- Current Data Rate (Transmit) (Section 11.15)
- Latency (Section 11.16)

The Session Initialization Response message MUST contain one of each of the following data items, if the data item will be used during the lifetime of the session:

- Resources (Receive) (Section 11.17)
- Resources (Transmit) (Section 11.18)
- Relative Link Quality (Receive) (Section 11.19)
- Relative Link Quality (Transmit) (Section 11.20)

- Maximum Transmission Unit (MTU) (Section 11.21)

The Session Initialization Response message MAY contain one of each of the following data items:

- Status (Section 11.1)
- Peer Type (Section 11.4)
- Extensions Supported (Section 11.6)

A router receiving a Session Initialization Response message without a Status data item MUST behave as if a Status data item with code 'Success' had been received, see Table 3.

10.5. Session Update Message

A Session Update message MAY be sent by a DLEP participant to indicate local Layer 3 address changes, or metric changes on a modem-wide basis. It should be noted that Session Update messages can be sent by both routers and modems. For example, addition of an IPv4 address to the router MAY prompt a Session Update message to its attached modems. Also, for example, a modem that changes its Maximum Data Rate (Receive) for all destinations MAY reflect that change via a Session Update message to its attached router(s).

Concerning Layer 3 addresses: If the modem is capable of understanding and forwarding this information (via proprietary mechanisms), the address update would prompt any remote DLEP modems (DLEP-enabled modems in a remote node) to issue a Destination Update message (Section 10.15) to their local routers with the new (or deleted) addresses. Modems that do not track Layer 3 addresses SHOULD silently parse and ignore Layer 3 data items. The Session Update message MUST be acknowledged with a Session Update Response message (Section 10.6).

If metrics are supplied with the Session Update message (e.g., Maximum Data Rate), these metrics are considered to be modem-wide, and therefore MUST be applied to all destinations in the information base associated with the DLEP session.

To construct a Session Update message, the Message Type value in the message header is set to 5, from Table 1.

The Session Update message MAY contain one of each of the following data items:

- Maximum Data Rate (Receive) (Section 11.12)

- Maximum Data Rate (Transmit) (Section 11.13)
- Current Data Rate (Receive) (Section 11.14)
- Current Data Rate (Transmit) (Section 11.15)
- Latency (Section 11.16)

The Session Update message MAY contain one of each of the following data items, if the data item is in use by the session:

- Resources (Receive) (Section 11.17)
- Resources (Transmit) (Section 11.18)
- Relative Link Quality (Receive) (Section 11.19)
- Relative Link Quality (Transmit) (Section 11.20)
- Maximum Transmission Unit (MTU) (Section 11.21)

The Session Update message MAY contain one or more of the following data items, with different values:

- IPv4 Address (Section 11.8)
- IPv6 Address (Section 11.9)

A Session Update message MUST be acknowledged by the receiver issuing a Session Update Response message (Section 10.6).

10.6. Session Update Response Message

A Session Update Response message MUST be sent by implementations to indicate whether a Session Update message (Section 10.5) was successfully received.

To construct a Session Update Response message, the Message Type value in the message header is set to 6, from Table 1.

The Session Update Response message MAY contain one Status (Section 11.1) data item.

A receiver of a Session Update Response message without a Status data item MUST behave as if a Status data item with status code 'Success' had been received, see Table 3.

10.7. Session Termination Message

A Session Termination message MUST be sent by a participant when the DLEP session needs to be terminated. It should be noted that Session Termination messages can be sent by both routers and modems.

To construct a Session Termination message, the Message Type value in the message header is set to 7, from Table 1.

The Session Termination message MAY contain one Status (Section 11.1) data item.

A receiver of a Session Termination message without a Status data item MUST behave as if a Status data item with status code 'Success', see Table 3, implying graceful termination, had been received.

A Session Termination message MUST be acknowledged by the receiver issuing a Session Termination Response message (Section 10.8).

10.8. Session Termination Response Message

A Session Termination Response message MUST be sent by a DLEP participant in response to a received Session Termination message (Section 10.7).

Receipt of a Session Termination Response message completes the tear-down of the DLEP session.

To construct a Session Termination Response message, the Message Type value in the message header is set to 8, from Table 1.

The Session Termination Response message MAY contain one Status (Section 11.1) data item.

A receiver of a Session Termination Response message without a Status data item MUST behave as if a Status data item with status code 'Success', see Table 3, implying graceful termination, had been received.

10.9. Destination Up Message

A Destination Up message MUST be sent by the modem to indicate that a new destination has been detected. A Destination Up message MUST be acknowledged by the router issuing a Destination Up Response message (Section 10.10). When a Destination Up message is received and successfully processed, the router should add knowledge of the new destination to its information base, indicating that the destination is accessible via the modem.

To construct a Destination Up message, the Message Type value in the message header is set to 9, from Table 1.

The Destination Up message MUST contain one of each of the following data items:

- MAC Address (Section 11.7)

The Destination Up message MAY contain one of each of the following data items:

- Maximum Data Rate (Receive) (Section 11.12)
- Maximum Data Rate (Transmit) (Section 11.13)
- Current Data Rate (Receive) (Section 11.14)
- Current Data Rate (Transmit) (Section 11.15)
- Latency (Section 11.16)

The Destination Up message MAY contain one of each of the following data items, if the data item is in use by the session:

- Resources (Receive) (Section 11.17)
- Resources (Transmit) (Section 11.18)
- Relative Link Quality (Receive) (Section 11.19)
- Relative Link Quality (Transmit) (Section 11.20)
- Maximum Transmission Unit (MTU) (Section 11.21)

The Destination Up message MAY contain one or more of the following data items, with different values:

- IPv4 Address (Section 11.8)
- IPv6 Address (Section 11.9)
- IPv4 Attached Subnet (Section 11.10)
- IPv6 Attached Subnet (Section 11.11)

If the modem has IPv4 and/or IPv6 address information for a destination it SHOULD include the relevant data items in the

Destination Up message, reducing the need for the router to probe for any address.

10.10. Destination Up Response Message

A DLEP router MUST send a Destination Up Response message to indicate whether a Destination Up message (Section 10.9) was successfully processed.

To construct a Destination Up Response message, the Message Type value in the message header is set to 10, from Table 1.

The Destination Up Response message MUST contain one MAC Address (Section 11.7) data item.

The Destination Up Response message MAY contain one Status (Section 11.1) data item.

A modem receiving a Destination Up Response message without a Status data item MUST behave as if a Status data item with status code 'Success' had been received, see Table 3.

10.11. Destination Announce Message

If a router wishes to request information concerning a destination that has not yet been announced by a mode via a Destination Up message (Section 10.9), it MAY send a Destination Announce message to the modem.

A Destination Announce message MUST be acknowledged by the modem issuing a Destination Announce Response message (Section 10.12).

To construct a Destination Announce message, the Message Type value in the message header is set to 17, from Table 1.

The Destination Announce message MUST contain one of each of the following data items:

- MAC Address (Section 11.7)

The Destination Announce message MAY contain zero or more of the following data items, with different values:

- IPv4 Address (Section 11.8)

- IPv6 Address (Section 11.9)

10.12. Destination Announce Response Message

A DLEP modem MUST send a Destination Announce Response message to indicate whether a Destination Announce message (Section 10.11) was successfully processed and the destination identified by the MAC Address data item is available.

When a Destination Announce Response message is received and successfully processed, the router should add knowledge of the new destination to its information base, indicating that the destination is accessible via the modem.

To construct a Destination Announce Response message, the Message Type value in the message header is set to 18, from Table 1.

The Destination Announce Response message MUST contain one of each of the following data items:

- MAC Address (Section 11.7)

The Destination Announce Response message MAY contain one of each of the following data items:

- Maximum Data Rate (Receive) (Section 11.12)
- Maximum Data Rate (Transmit) (Section 11.13)
- Current Data Rate (Receive) (Section 11.14)
- Current Data Rate (Transmit) (Section 11.15)
- Latency (Section 11.16)

The Destination Announce Response message MAY contain one of each of the following data items, if the data item is in use by the session:

- Resources (Receive) (Section 11.17)
- Resources (Transmit) (Section 11.18)
- Relative Link Quality (Receive) (Section 11.19)
- Relative Link Quality (Transmit) (Section 11.20)
- Maximum Transmission Unit (MTU) (Section 11.21)

The Destination Announce Response message MAY contain zero or more of the following data items, with different values:

- IPv4 Address (Section 11.8)

- IPv6 Address (Section 11.9)

If the modem has IPv4 and/or IPv6 address information for a destination it SHOULD include the relevant data items in the Destination Announce Response message, reducing the need for the router to probe for any address.

- Status (Section 11.1)

A router receiving a Destination Announce Response message without a Status data item MUST behave as if a Status data item with status code 'Success' had been received, see Table 3.

If a modem does not support Destination Announce messages, or the modem is unable to report information immediately about the requested information, if the destination is not currently accessible, for example, the status code in the Status data item SHOULD be set to 'Request Denied'.

10.13. Destination Down Message

A DLEP participant MUST send a Destination Down message to report when a destination (a remote node or a multicast group) is no longer reachable. A Destination Down Response message (Section 10.14) MUST be sent by the recipient of a Destination Down message to confirm that the relevant data has been removed from the information base.

To construct a Destination Down message, the Message Type value in the message header is set to 11, from Table 1.

The Destination Down message MUST contain one of each of the following data items:

- MAC Address (Section 11.7)

It should be noted that both modem and router may send a Destination Down message to its peer.

10.14. Destination Down Response Message

A DLEP participant MUST send a Destination Down Response message to indicate whether a received Destination Down message (Section 10.13) was successfully processed. If successfully processed, the sender of the Response MUST have removed all entries in the information base that pertain to the referenced destination.

To construct a Destination Down Response message, the Message Type value in the message header is set to 12, from Table 1.

The Destination Down Response message MUST contain one of each of the following data items:

- MAC Address (Section 11.7)

The Destination Down Response message MAY contain one of each of the following data items:

- Status (Section 11.1)

A receiver of a Destination Down Response message without a Status data item MUST behave as if a Status data item with status code 'Success' had been received, see Table 3.

10.15. Destination Update Message

A DLEP modem SHOULD send the Destination Update message when it detects some change in the information base for a given destination (remote node or multicast group). Some examples of changes that would prompt a Destination Update message are:

- Change in link metrics (e.g., Data Rates)

- Layer 3 addressing change

To construct a Destination Update message, the Message Type value in the message header is set to 13, from Table 1.

The Destination Update message MUST contain one of each of the following data items:

- MAC Address (Section 11.7)

The Destination Update message MAY contain one of each of the following data items:

- Maximum Data Rate (Receive) (Section 11.12)

- Maximum Data Rate (Transmit) (Section 11.13)

- Current Data Rate (Receive) (Section 11.14)

- Current Data Rate (Transmit) (Section 11.15)

- Latency (Section 11.16)

The Destination Update message MAY contain one of each of the following data items, if the data item is in use by the session:

- Resources (Receive) (Section 11.17)
- Resources (Transmit) (Section 11.18)
- Relative Link Quality (Receive) (Section 11.19)
- Relative Link Quality (Transmit) (Section 11.20)
- Maximum Transmission Unit (MTU) (Section 11.21)

The Destination Update message MAY contain one or more of the following data items, with different values:

- IPv4 Address (Section 11.8)
- IPv6 Address (Section 11.9)
- IPv4 Attached Subnet (Section 11.10)
- IPv6 Attached Subnet (Section 11.11)

10.16. Heartbeat Message

While Heartbeat messages are not required by DLEP implementations, it is strongly RECOMMENDED that Heartbeat messages be used.

A Heartbeat message SHOULD be sent by a DLEP participant every N seconds, where N is defined in the Heartbeat Interval data item of the Session Initialization message (Section 10.3) or Session Initialization Response message (Section 10.4).

Note that implementations setting the Heartbeat Interval to 0 effectively sets the interval to an infinite value, turning off Heartbeat messages. Great care MUST be taken when exercising this option.

The message is used by participants to detect when a DLEP session peer (either the modem or the router) is no longer communicating. Participants SHOULD allow two (2) heartbeat intervals to expire with no messages from the peer before initiating DLEP session termination procedures.

To construct a Heartbeat message, the Message Type value in the message header is set to 14, from Table 1.

There are no valid data items for the Heartbeat message.

10.17. Link Characteristics Request Message

The Link Characteristics Request message MAY be sent by a DLEP router to request that the modem initiate changes for specific characteristics of the link. The request can reference either a real destination (e.g., a remote node), or a logical destination (e.g., a multicast group) within the network.

The Link Characteristics Request message MAY contain either a Current Data Rate (CDRR or CDRT) data item to request a different datarate than what is currently allocated, a Latency data item to request that traffic delay on the link not exceed the specified value, or both. A Link Characteristics Response message (Section 10.18) is required to complete the request. Issuing a Link Characteristics Request with ONLY the MAC Address data item is a mechanism a router MAY use to request metrics (via the Link Characteristics Response) from its modem.

The router sending a Link Characteristics Request message should be aware that a request may take an extended period of time to complete.

To construct a Link Characteristics Request message, the Message Type value in the message header is set to 15, from Table 1.

The Link Characteristics Request message MUST contain one of each of the following data items:

- MAC Address (Section 11.7)

The Link Characteristics Request message MAY contain one of each of the following data items:

- Current Data Rate (Receive) (Section 11.14)
- Current Data Rate (Transmit) (Section 11.15)
- Latency (Section 11.16)

10.18. Link Characteristics Response Message

A DLEP modem MUST send a Link Characteristics Response message to indicate whether a received Link Characteristics Request message (Section 10.17) was successfully processed. The Link Characteristics Response message SHOULD contain a complete set of metric data items, and MUST contain a full set (i.e. those declared in the Session Initialization Response message (Section 10.4)), if metrics were

requested by only including a MAC address data item. It MUST contain the same metric types as the request. The values in the metric data items in the Link Characteristics Response message MUST reflect the link characteristics after the request has been processed.

If an implementation is not able to alter the characteristics of the link in the manner requested, then the message MUST contain a Status data item with status code 'Request Denied', see Table 3.

To construct a Link Characteristics Response message, the Message Type value in the message header is set to 16, from Table 1.

The Link Characteristics Response message MUST contain one of each of the following data items:

- MAC Address (Section 11.7)

The Link Characteristics Response message SHOULD contain one of each of the following data items:

- Maximum Data Rate (Receive) (Section 11.12)
- Maximum Data Rate (Transmit) (Section 11.13)
- Current Data Rate (Receive) (Section 11.14)
- Current Data Rate (Transmit) (Section 11.15)
- Latency (Section 11.16)

The Link Characteristics Response message MAY contain one of each of the following data items:

- Status (Section 11.1)

The Link Characteristics Response message MAY contain one of each of the following data items, if the data item is in use by the session:

- Resources (Receive) (Section 11.17)
- Resources (Transmit) (Section 11.18)
- Relative Link Quality (Receive) (Section 11.19)
- Relative Link Quality (Transmit) (Section 11.20)
- Maximum Transmission Unit (MTU) (Section 11.21)

A router receiving a Link Characteristics Response message without a Status data item MUST behave as if a Status data item with status code 'Success', see Table 3, had been received.

11. DLEP Data Items

Following is the list of core data items that MUST be recognized by a DLEP compliant implementation. As mentioned before, not all data items need be used during a session, but an implementation MUST correctly process these data items when correctly associated with a signal or message.

The core DLEP data items are:

Type Code	Description
0	Reserved
1	Status (Section 11.1)
2	IPv4 Connection Point (Section 11.2)
3	IPv6 Connection Point (Section 11.3)
4	Peer Type (Section 11.4)
5	Heartbeat Interval (Section 11.5)
6	Extensions Supported (Section 11.6)
7	MAC Address (Section 11.7)
8	IPv4 Address (Section 11.8)
9	IPv6 Address (Section 11.9)
10	IPv4 Attached Subnet (Section 11.10)
11	IPv6 Attached Subnet (Section 11.11)
12	Maximum Data Rate (Receive) MDRR) (Section 11.12)
13	Maximum Data Rate (Transmit) (MDRT) (Section 11.13)
14	Current Data Rate (Receive) (CDRR) (Section 11.14)
15	Current Data Rate (Transmit) (CDRT) (Section 11.15)
16	Latency (Section 11.16)
17	Resources (Receive) (RESR) (Section 11.17)
18	Resources (Transmit) (REST) (Section 11.18)
19	Relative Link Quality (Receive) (RLQR) (Section 11.19)
20	Relative Link Quality (Transmit) (RLQT) (Section 11.20)
21	Maximum Transmission Unit (MTU) (Section 11.21)
22-65407	Reserved for future extensions
65408-65534	Private Use. Available for experiments
65535	Reserved

Table 2: DLEP Data Item types

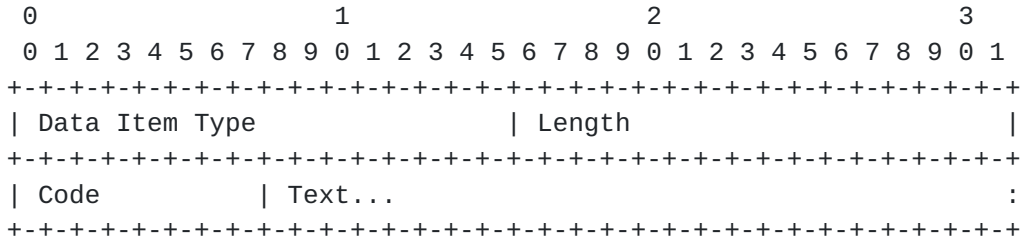
11.1. Status

The Status data item MAY appear in the Session Initialization Response (Section 10.4), Session Termination (Section 10.7), Session Termination Response (Section 10.8), Session Update Response (Section 10.6), Destination Up Response (Section 10.10), Destination Down Response (Section 10.14) and Link Characteristics Response (Section 10.18) messages.

For the Session Termination message (Section 10.7), the Status data item indicates a reason for the termination. For all acknowledgement messages, the Status data item is used to indicate the success or failure of the previously received message.

The status data item includes an optional Text field that can be used to provide a textual description of the status. The use of the Text field is entirely up to the receiving implementation, i.e., it could be output to a log file or discarded. If no Text field is supplied with the Status data item, the Length field MUST be set to 1.

The Status data item contains the following fields:



Data Item Type: 1

Length: 1 + Length of text, in octets

Status Code: One of the codes defined in Table 3 below.

Text: UTF-8 encoded string, describing the cause, used for implementation defined purposes. Since this field is used for description, implementations SHOULD limit characters in this field to printable characters. Implementations receiving this data item SHOULD check for printable characters in the field.

An implementation MUST NOT assume the Text field is NUL-terminated.

Status Code	Value	Failure Mode	Reason
Success	0	Success	The message was processed successfully.
Unknown Message	1	Terminate	The message was not recognized by the implementation.
Unexpected Message	2	Terminate	The message was not expected while the device was in the current state, e.g., a Session Initialization message (Section 10.3) in the In-Session state.
Invalid Data	3	Terminate	One or more data items in the message are invalid, unexpected or incorrectly duplicated.
Invalid Destination	4	Terminate	The destination provided in the message does not match a previously announced destination. For example, in the Link Characteristic Response message (Section 10.18).
Timed Out	5	Terminate	The session has timed out.
<Reserved>	6-90	Terminate	Reserved for future extensions.
<Private Use>	91-99	Terminate	Available for experiments.
Not Interested	100	Continue	The receiver is not interested in this message subject, e.g. a Destination Up Response message (Section 10.10) to indicate no further messages about the destination.
Request Denied	101	Continue	The receiver refuses to complete the request.
<Reserved>	102-243	Continue	Reserved for future extensions.
<Private Use>	244-254	Continue	Available for experiments.
<Reserved>	255	Terminate	Reserved.

Table 3: DLEP Status Codes

A failure mode of 'Terminate' indicates that the session MUST be terminated immediately instead of sending any relevant response message, by sending a Session Termination message (Section 10.7) containing the status code, and then transitioning to the Session Termination state.

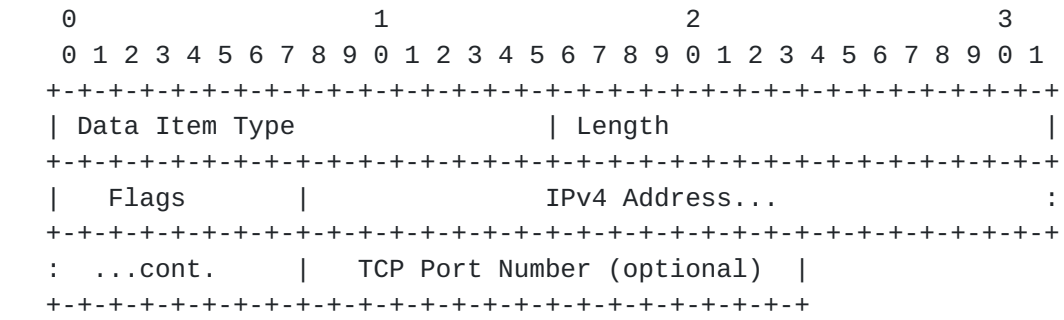
A failure mode of 'Continue' indicates that the session SHOULD continue as normal.

11.2. IPv4 Connection Point

The IPv4 Connection Point data item MAY appear in the Peer Offer signal (Section 10.2).

The IPv4 Connection Point data item indicates the IPv4 address and, optionally, the TCP port number on the DLEP modem available for connections. If provided, the router MUST use this information to perform the TCP connect to the modem.

The IPv4 Connection Point data item contains the following fields:



Data Item Type: 2

Length: 5 (or 7 if TCP Port included)

Flags: Flags field, defined below.

IPv4 Address: The IPv4 address listening on the DLEP modem.

TCP Port Number: TCP Port number on the DLEP modem.

If the Length field is 7, the port number specified MUST be used to establish the TCP session. If the TCP Port Number is omitted, i.e. the Length field is 5, the router MUST use the DLEP well-known port number (Section 13.6) to establish the TCP connection.

The Flags field is defined as:

```
 0 1 2 3 4 5 6 7
+-+-+-+-+-+-+-+-+
|  Reserved   |T|
+-+-+-+-+-+-+-+-+
```

T: Use TLS flag, indicating whether the TCP connection requires the use of TLS (1), or not (0).

Reserved: MUST be zero. Reserved for future use.

11.3. IPv6 Connection Point

The IPv6 Connection Point data item MAY appear in the Peer Offer signal (Section 10.2).

The IPv6 Connection Point data item indicates the IPv6 address and, optionally, the TCP port number on the DLEP modem available for connections. If provided, the router MUST use this information to perform the TCP connect to the modem.

The IPv6 Connection Point data item contains the following fields:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Data Item Type                | Length                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Flags       |                IPv6 Address                   :
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:                         IPv6 Address                          :
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:                         IPv6 Address                          :
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:                         IPv6 Address                          :
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:  ...cont.     |   TCP Port Number (optional)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Data Item Type: 3

Length: 17 (or 19 if TCP Port included)

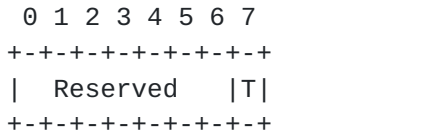
Flags: Flags field, defined below.

IPv6 Address: The IPv6 address listening on the DLEP modem.

TCP Port Number: TCP Port number on the DLEP modem.

If the Length field is 19, the port number specified MUST be used to establish the TCP session. If the TCP Port Number is omitted, i.e. the Length field is 17, the router MUST use the DLEP well-known port number (Section 13.6) to establish the TCP connection.

The Flags field is defined as:



T: Use TLS flag, indicating whether the TCP connection requires the use of TLS (1), or not (0).

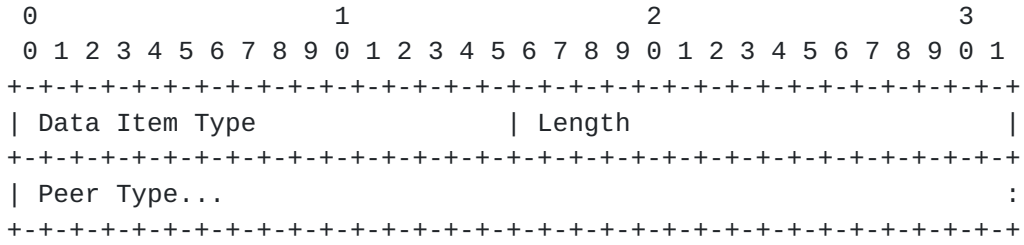
Reserved: MUST be zero. Reserved for future use.

11.4. Peer Type

The Peer Type data item MAY appear in the Peer Discovery (Section 10.1) and Peer Offer (Section 10.2) signals, and the Session Initialization (Section 10.3) and Session Initialization Response (Section 10.4) messages.

The Peer Type data item is used by the router and modem to give additional information as to its type. The peer type is a string and is envisioned to be used for informational purposes (e.g., as output in a display command).

The Peer Type data item contains the following fields:



Data Item Type: 4

Length: Length of peer type string, in octets.

Peer Type: UTF-8 encoded string. For example, a satellite modem might set this variable to "Satellite terminal". Since this data item is intended to provide additional information for display commands, sending implementations SHOULD limit the data to

printable characters, and receiving implementations SHOULD check the data for printable characters.

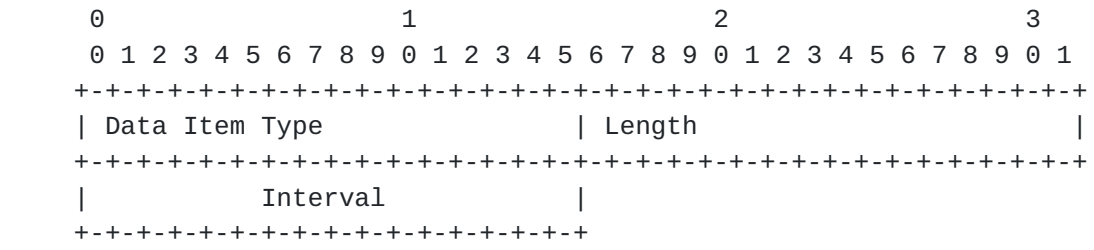
An implementation MUST NOT assume the Peer Type field is NUL-terminated.

11.5. Heartbeat Interval

The Heartbeat Interval data item MUST appear in both the Session Initialization (Section 10.3) and Session Initialization Response (Section 10.4) messages to indicate the Heartbeat timeout window to be used by the sender.

The Interval is used to specify a period (in seconds) for Heartbeat messages (Section 10.16). By specifying an Interval value of 0, implementations MAY indicate the desire to disable Heartbeat messages entirely (i.e., the Interval is set to an infinite value). However, it is RECOMMENDED that implementations use non-0 timer values.

The Heartbeat Interval data item contains the following fields:



Data Item Type: 5

Length: 2

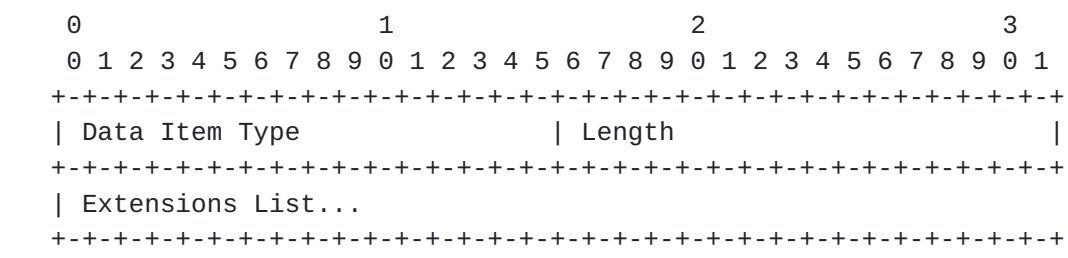
Interval: 0 = Do not use heartbeats on this DLEP session. Non-zero = Interval, in seconds, for heartbeat messages.

11.6. Extensions Supported

The Extensions Supported data item MAY be used in both the Session Initialization (Section 10.3) and Session Initialization Response (Section 10.4) messages.

The Extensions Supported data item is used by the router and modem to negotiate additional optional functionality they are willing to support. The Extensions List is a concatenation of the types of each supported extension, found in the IANA DLEP Extensions repository. Each Extension Type definition includes which additional signals and data-items are supported.

The Extensions Supported data item contains the following fields:



Data Item Type: 6

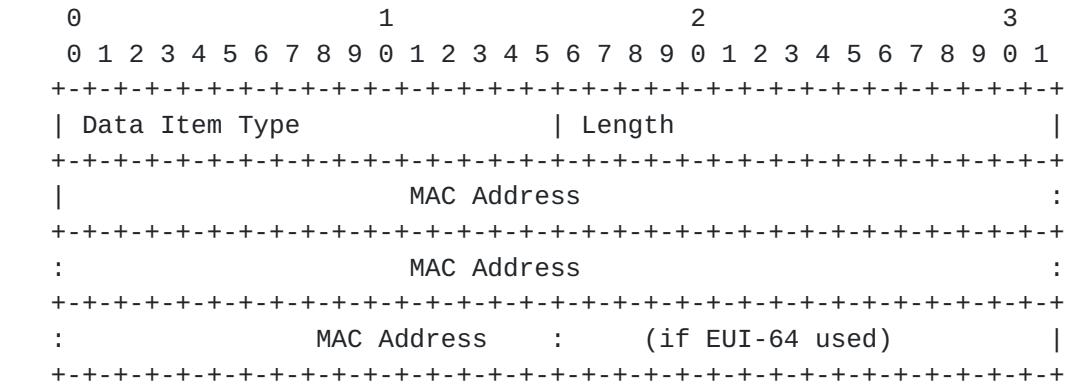
Length: Length of the extensions list in octets. This is twice (2x) the number of extensions.

Extension List: A list of extensions supported, identified by their 2-octet value as listed in the extensions registry.

11.7. MAC Address

The MAC address data item MUST appear in all destination-oriented messages (i.e., Destination Up (Section 10.9), Destination Up Response (Section 10.10), Destination Down (Section 10.13), Destination Down Response (Section 10.14), Destination Update (Section 10.15), Link Characteristics Request (Section 10.17), and Link Characteristics Response (Section 10.18)).

The MAC Address data item contains the address of the destination on the remote node. The MAC address MAY be either a physical or a virtual destination, and MAY be expressed in EUI-48 or EUI-64 format. Examples of a virtual destination would be a multicast MAC address, or the broadcast MAC (FF:FF:FF:FF:FF:FF).



Data Item Type: 7

Length: 6 for EUI-48 format, or 8 for EUI-64 format

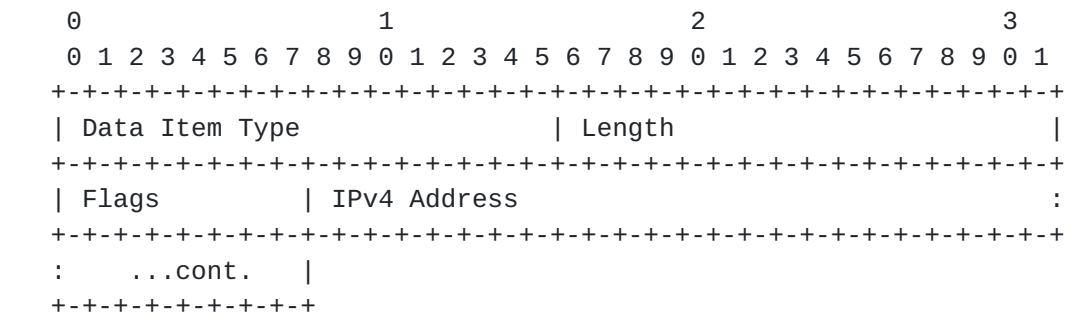
MAC Address: MAC Address of the destination.

11.8. IPv4 Address

The IPv4 Address data item MAY appear in the Session Update (Section 10.5), Destination Up (Section 10.9) and Destination Update (Section 10.15) messages.

When included in Destination messages, this data item contains the IPv4 address of the destination. When included in the Session Update message, this data item contains the IPv4 address of the peer. In either case, the data item also contains an indication of whether this is a new or existing address, or is a deletion of a previously known address.

The IPv4 Address data item contains the following fields:



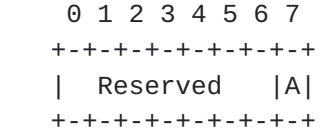
Data Item Type: 8

Length: 5

Flags: Flags field, defined below.

IPv4 Address: The IPv4 address of the destination or peer.

The Flags field is defined as:



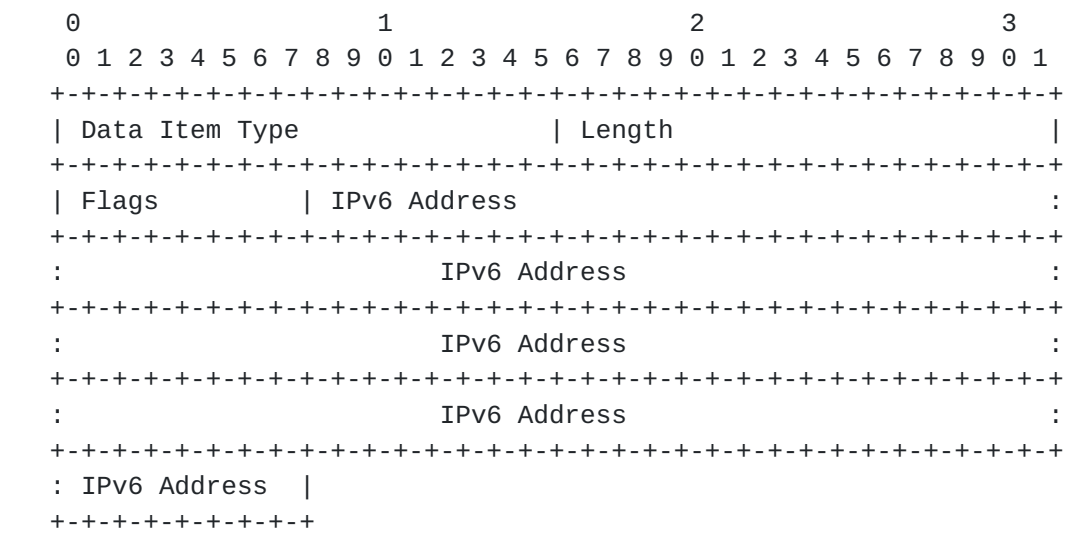
A: Add/Drop flag, indicating whether this is a new or existing address (1), or a withdrawal of an address (0).

Reserved: MUST be zero. Reserved for future use.

11.9. IPv6 Address

The IPv6 Address data item MAY appear in the Session Update (Section 10.5), Destination Up (Section 10.9) and Destination Update (Section 10.15) messages. When included in Destination messages, this data item contains the IPv6 address of the destination. When included in the Session Update message, this data item contains the IPv6 address of the peer. In either case, the data item also contains an indication of whether this is a new or existing address, or is a deletion of a previously known address.

The IPv6 Address data item contains the following fields:



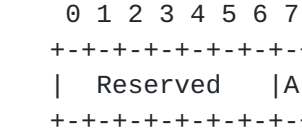
Data Item Type: 9

Length: 17

Flags: Flags field, defined below.

IPv6 Address: IPv6 Address of the destination or peer.

The Flags field is defined as:



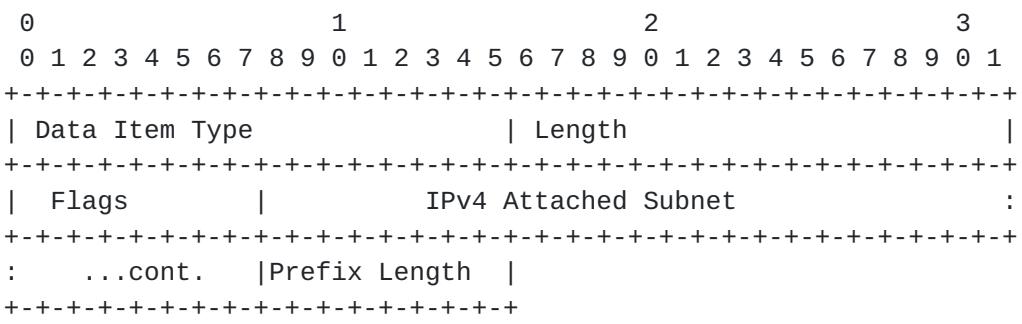
A: Add/Drop flag, indicating whether this is a new or existing address (1), or a withdrawal of an address (0).

Reserved: MUST be zero. Reserved for future use.

11.10. IPv4 Attached Subnet

The DLEP IPv4 Attached Subnet allows a device to declare that it has an IPv4 subnet (e.g., a stub network) attached, that it has become aware of an IPv4 subnet being present at a remote destination, or that it has become aware of the loss of a subnet at the remote destination. The IPv4 Attached Subnet data item MAY appear in the Destination Up (Section 10.9) and Destination Update (Section 10.15) messages.

The DLEP IPv4 Attached Subnet data item contains the following fields:



Data Item Type: 10

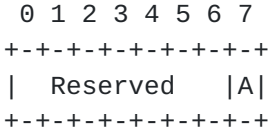
Length: 6

Flags: Flags field, defined below.

IPv4 Subnet: The IPv4 subnet reachable at the destination.

Prefix Length: Length of the prefix (1-32) for the IPv4 subnet. A prefix length outside the specified range MUST be considered as invalid.

The Flags field is defined as:



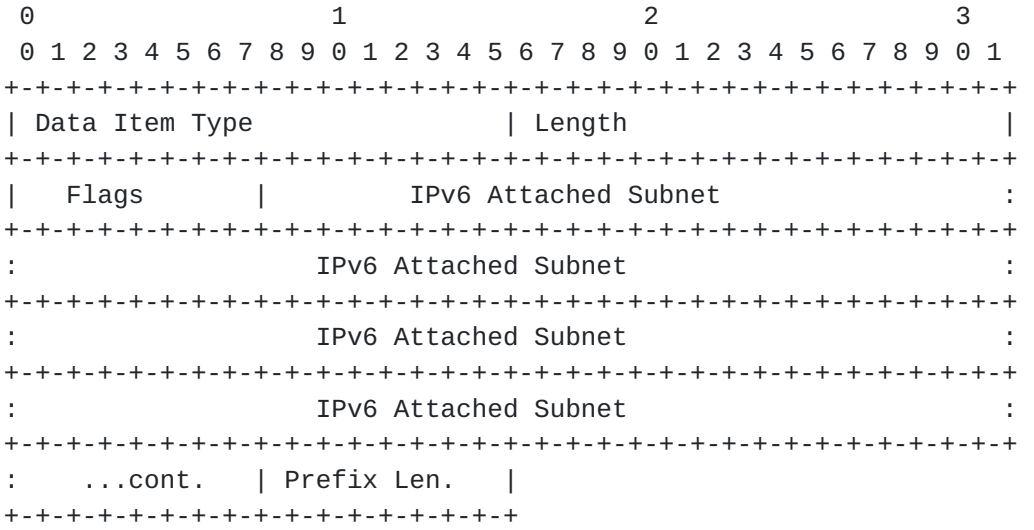
A: Add/Drop flag, indicating whether this is a new or existing subnet address (1), or a withdrawal of a subnet address (0).

Reserved: MUST be zero. Reserved for future use.

11.11. IPv6 Attached Subnet

The DLEP IPv6 Attached Subnet allows a device to declare that it has an IPv6 subnet (e.g., a stub network) attached, or that it has become aware of an IPv6 subnet being present at a remote destination. The IPv6 Attached Subnet data item MAY appear in the Destination Up (Section 10.9) and Destination Update (Section 10.15) messages.

The DLEP IPv6 Attached Subnet data item contains the following fields:



Data Item Type: 11

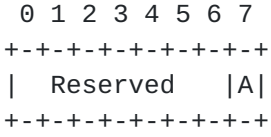
Length: 18

Flags: Flags field, defined below.

IPv6 Attached Subnet: The IPv6 subnet reachable at the destination.

Prefix Length: Length of the prefix (1-128) for the IPv6 subnet. A prefix length outside the specified range MUST be considered as invalid.

The Flags field is defined as:



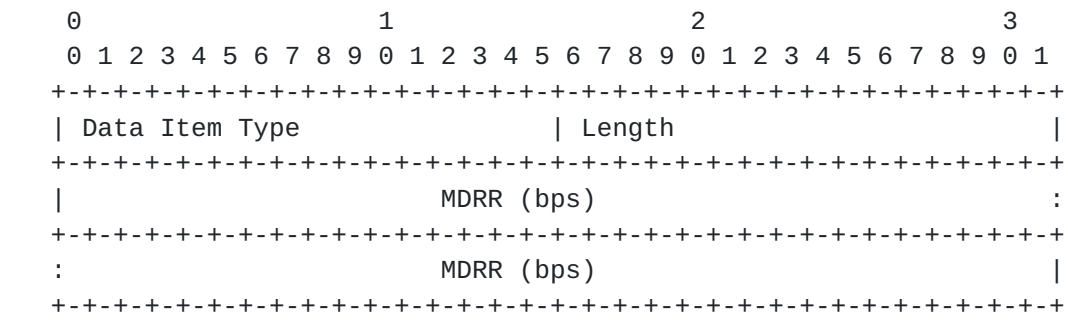
A: Add/Drop flag, indicating whether this is a new or existing subnet address (1), or a withdrawal of a subnet address (0).

Reserved: MUST be zero. Reserved for future use.

11.12. Maximum Data Rate (Receive)

The Maximum Data Rate (Receive) (MDRR) data item MUST appear in the Session Initialization Response message (Section 10.4), and MAY appear in the Session Update (Section 10.5), Destination Up (Section 10.9), Destination Update (Section 10.15) and Link Characteristics Response (Section 10.18) messages to indicate the maximum theoretical data rate, in bits per second, that can be achieved while receiving data on the link.

The Maximum Data Rate (Receive) data item contains the following fields:



Data Item Type: 12

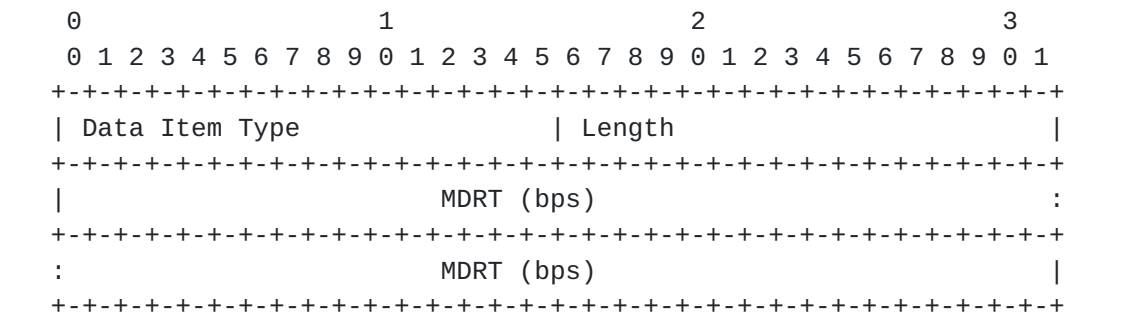
Length: 8

Maximum Data Rate (Receive): A 64-bit unsigned integer, representing the maximum theoretical data rate, in bits per second (bps), that can be achieved while receiving on the link.

11.13. Maximum Data Rate (Transmit)

The Maximum Data Rate (Transmit) (MDRT) data item MUST appear in the Session Initialization Response message (Section 10.4), and MAY appear in the Session Update (Section 10.5), Destination Up (Section 10.9), Destination Update (Section 10.15) and Link Characteristics Response (Section 10.18) messages to indicate the maximum theoretical data rate, in bits per second, that can be achieved while transmitting data on the link.

The Maximum Data Rate (Transmit) data item contains the following fields:



Data Item Type: 13

Length: 8

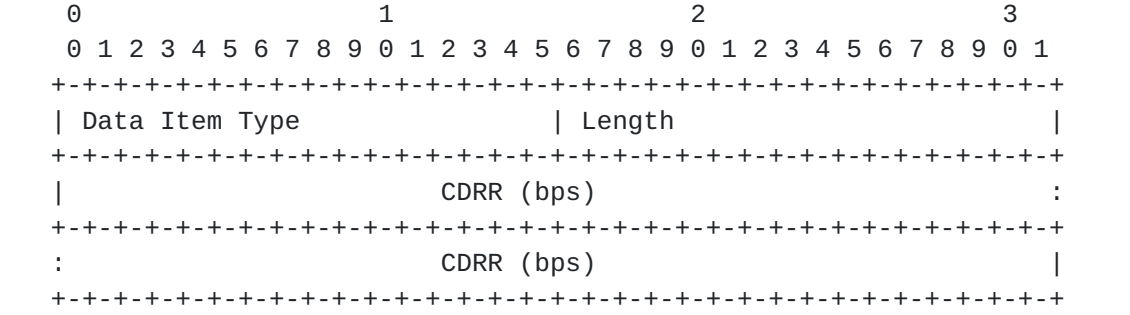
Maximum Data Rate (Transmit): A 64-bit unsigned integer, representing the maximum theoretical data rate, in bits per second (bps), that can be achieved while transmitting on the link.

11.14. Current Data Rate (Receive)

The Current Data Rate (Receive) (CDRR) data item MUST appear in the Session Initialization Response message (Section 10.4), and MAY appear in the Session Update (Section 10.5), Destination Up (Section 10.9), Destination Update (Section 10.15) and Link Characteristics Response (Section 10.18) messages to indicate the rate at which the link is currently operating for receiving traffic.

When used in the Link Characteristics Request message (Section 10.17), CDRR represents the desired receive rate, in bits per second, on the link.

The Current Data Rate (Receive) data item contains the following fields:



Data Item Type: 14

Length: 8

Current Data Rate (Receive): A 64-bit unsigned integer, representing the current data rate, in bits per second, that can currently be achieved while receiving traffic on the link.

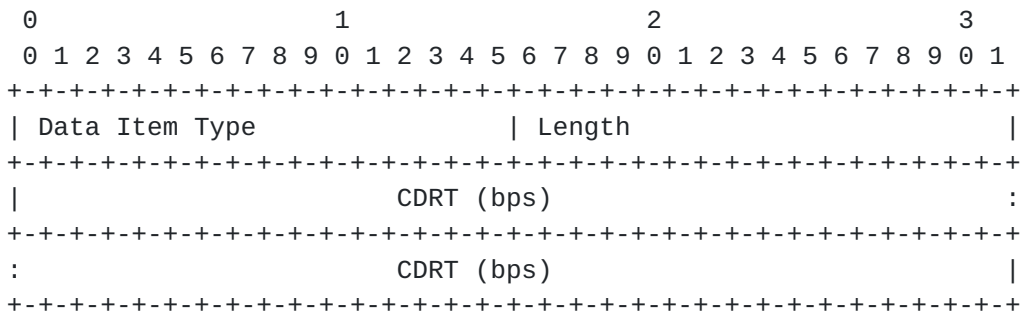
If there is no distinction between current and maximum receive data rates, current data rate receive MUST be set equal to the maximum data rate receive.

11.15. Current Data Rate (Transmit)

The Current Data Rate Transmit (CDRT) data item MUST appear in the Session Initialization Response message (Section 10.4), and MAY appear in the Session Update (Section 10.5), Destination Up (Section 10.9), Destination Update (Section 10.15), and Link Characteristics Response (Section 10.18) messages to indicate the rate at which the link is currently operating for transmitting traffic.

When used in the Link Characteristics Request message (Section 10.17), CDRT represents the desired transmit rate, in bits per second, on the link.

The Current Data Rate (Transmit) data item contains the following fields:



Data Item Type: 15

Length: 8

Current Data Rate (Transmit): A 64-bit unsigned integer, representing the current data rate, in bits per second, that can currently be achieved while transmitting traffic on the link.

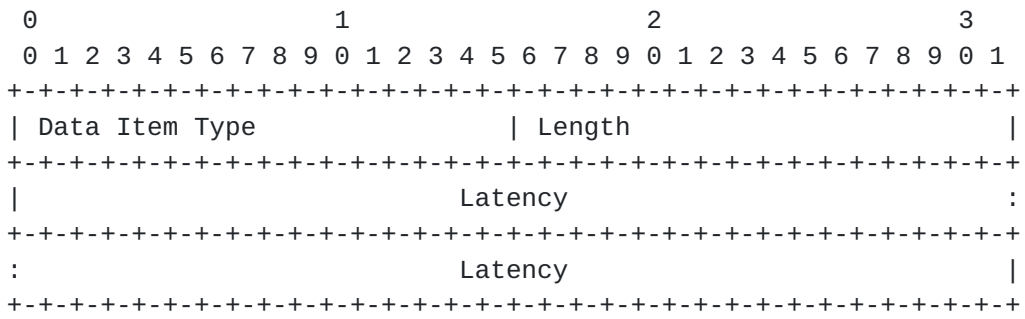
If there is no distinction between current and maximum transmit data rates, current data rate transmit MUST be set equal to the maximum data rate transmit.

11.16. Latency

The Latency data item MUST appear in the Session Initialization Response message (Section 10.4), and MAY appear in the Session Update (Section 10.5), Destination Up (Section 10.9), Destination Update (Section 10.15), and Link Characteristics Response (Section 10.18) messages to indicate the amount of latency, in microseconds, on the link.

When used in the Link Characteristics Request message (Section 10.17), Latency represents the maximum latency desired on the link.

The Latency value is reported as delay. The calculation of latency is implementation dependent. For example, the latency may be a running average calculated from the internal queuing.



Data Item Type: 16

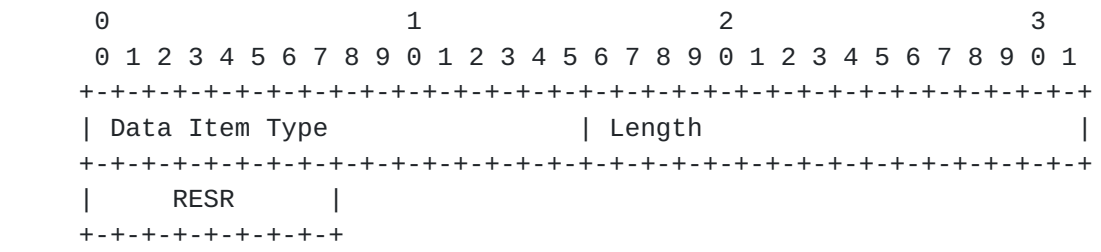
Length: 8

Latency: A 64-bit unsigned integer, representing the transmission delay, in microseconds, that a packet encounters as it is transmitted over the link.

11.17. Resources (Receive)

The Resources (Receive) (RESR) data item MAY appear in the Session Initialization Response message (Section 10.4), Session Update (Section 10.5), Destination Up (Section 10.9), Destination Update (Section 10.15) and Link Characteristics Response (Section 10.18) messages to indicate the amount of resources for reception (with 0 meaning 'no resources available', and 100 meaning 'all resources available') at the destination. The list of resources that might be considered is beyond the scope of this document, and is left to implementations to decide.

The Resources (Receive) data item contains the following fields:



Data Item Type: 17

Length: 1

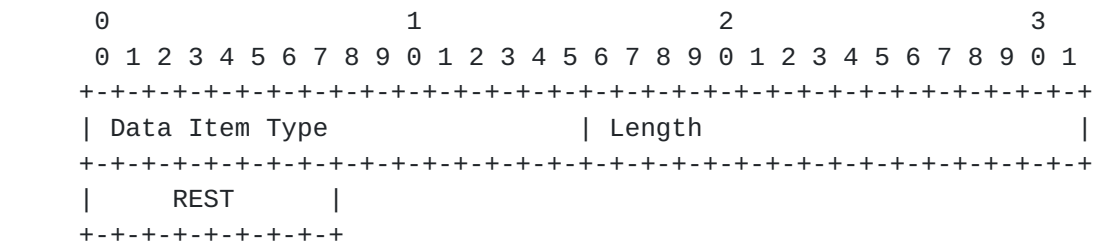
Resources (Receive): An 8-bit integer percentage, 0-100, representing the amount of resources allocated to receiving data. Any value greater than 100 MUST be considered as invalid.

If a device cannot calculate RESR, this data item SHOULD NOT be issued.

11.18. Resources (Transmit)

The Resources (Transmit) (REST) data item MAY appear in the Session Initialization Response message (Section 10.4), Session Update (Section 10.5), Destination Up (Section 10.9), Destination Update (Section 10.15) and Link Characteristics Response (Section 10.18) messages to indicate the amount of resources for transmission (with 0 meaning 'no resources available', and 100 meaning 'all resources available') at the destination. The list of resources that might be considered is beyond the scope of this document, and is left to implementations to decide.

The Resources (Transmit) data item contains the following fields:



Data Item Type: 18

Length: 1

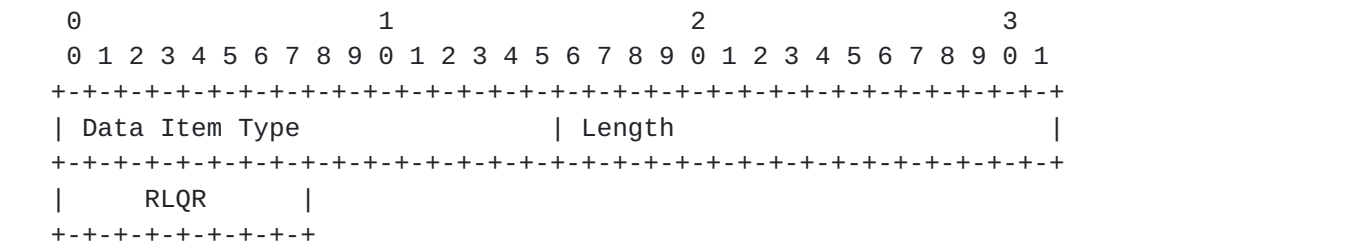
Resources (Transmit): An 8-bit integer percentage, 0-100, representing the amount of resources allocated to transmitting data. Any value greater than 100 MUST be considered as invalid.

If a device cannot calculate REST, this data item SHOULD NOT be issued.

11.19. Relative Link Quality (Receive)

The Relative Link Quality (Receive) (RLQR) data item MAY appear in the Session Initialization Response message (Section 10.4), Session Update (Section 10.5), Destination Up (Section 10.9), Destination Update (Section 10.15) and Link Characteristics Response (Section 10.18) messages to indicate the quality of the link for receiving data.

The Relative Link Quality (Receive) data item contains the following fields:



Data Item Type: 19

Length: 1

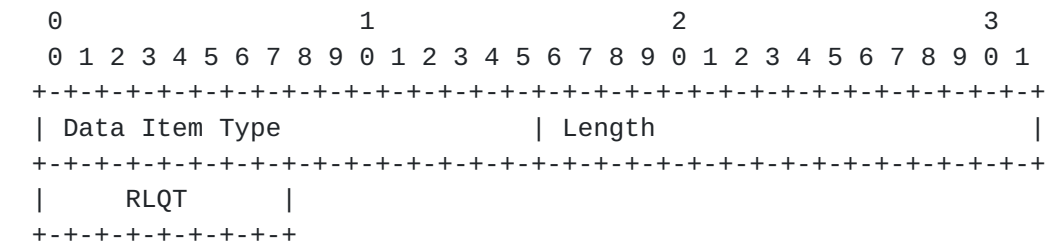
Relative Link Quality (Receive): A non-dimensional 8-bit integer, 0-100, representing relative link quality. A value of 100 represents a link of the highest quality. Any value greater than 100 MUST be considered as invalid.

If a device cannot calculate the RLQR, this data item SHOULD NOT be issued.

11.20. Relative Link Quality (Transmit)

The Relative Link Quality (Transmit) (RLQT) data item MAY appear in the Session Initialization Response message (Section 10.4), Session Update (Section 10.5), Destination Up (Section 10.9), Destination Update (Section 10.15) and Link Characteristics Response (Section 10.18) messages to indicate the quality of the link for transmitting data.

The Relative Link Quality (Transmit) data item contains the following fields:



Data Item Type: 20

Length: 1

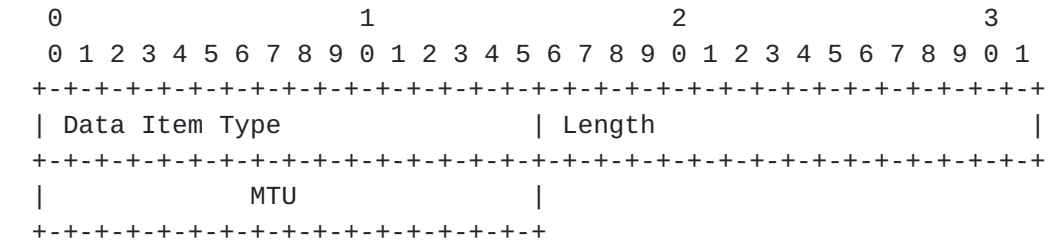
Relative Link Quality (Transmit): A non-dimensional 8-bit integer, 0-100, representing relative link quality. A value of 100 represents a link of the highest quality. Any value greater than 100 MUST be considered as invalid.

If a device cannot calculate the RLQT, this data item SHOULD NOT be issued.

11.21. Maximum Transmission Unit (MTU)

The Maximum Transmission Unit (MTU) data item MAY appear in the Session Initialization Response message (Section 10.4), Session Update (Section 10.5), Destination Up (Section 10.9), Destination Update (Section 10.15) and Link Characteristics Response (Section 10.18) messages to indicate the maximum size, in octets, of an IP packet that can be transmitted without fragmentation, including headers, but excluding any lower layer headers.

The Maximum Transmission Unit (MTU) data item contains the following fields:



Data Item Type: 21

Length: 2

Maximum Transmission Unit (MTU): The maximum size, in octets, of an IP packet that can be transmitted without fragmentation, including headers, but excluding any lower layer headers.

If a device cannot calculate the MTU, this data item SHOULD NOT be issued.

12. Security Considerations

The potential security concerns when using DLEP are:

1. An attacker might pretend to be a DLEP peer, either at DLEP session initialization, or by injection of messages once a session has been established, and/or

2. DLEP data items could be altered by an attacker, causing the receiving implementation to inappropriately alter its information base concerning network status.

Since DLEP is restricted to operation over a single (possibly logical) hop at layer 2, implementations requiring authentication and/or encryption of traffic MUST take steps to secure the Layer 2 link.

To avoid potential denial of service attack, it is RECOMMENDED that implementations using the Peer Discovery mechanism maintain an information base of hosts that persistently fail Session Initialization having provided an acceptable Discovery signal, and ignore Peer Discovery signals from such hosts.

This specification does not address security of the data plane, as it (the data plane) is not affected, and standard security procedures can be employed.

13. IANA Considerations

This section specifies requests to IANA.

13.1. Registrations

This specification defines:

- A new repository for DLEP signals and messages, with eighteen (18) values currently assigned.

- Reservation of a Private Use numbering space within the above repository for experimental DLEP signals and messages.

- A new repository for DLEP data items, with twenty-one (21) values currently assigned.

- Reservation of a Private Use numbering space within the data items repository for experimental data items.
- A new repository for DLEP status codes, with eight (8) currently assigned.
- Reservation of a Private Use numbering space within the status codes repository for experimental status codes.
- A new repository for DLEP extensions, with one (1) value currently assigned.
- Reservation of a Private Use numbering space within the extension repository for experimental extensions.
- A request for allocation of a well-known port for DLEP TCP and UDP communication.
- A request for allocation of a link-local multicast IPv4 address for DLEP discovery.
- A request for allocation of a link-local multicast IPv6 address for DLEP discovery.

13.2. Signal/Message Type Registration

A new repository must be created with the values of the DLEP signals and messages, entitled "Message Type Values for the Dynamic Link Event Protocol (DLEP)". The repository is to be managed using the "Specification Required" policy documented in [RFC5226].

All signal and message values are in the range [0..65535], defined in Table 1.

13.3. DLEP Data Item Registrations

A new repository for DLEP data items must be created, entitled "Data Item Type Values for the Dynamic Link Event Protocol (DLEP)". The repository is to be managed using the "Specification Required" policy documented in [RFC5226].

All data item values are in the range [0..65535], defined in Table 2.

13.4. DLEP Status Code Registrations

A new repository for DLEP status codes must be created, entitled "Status Code Values for the Dynamic Link Event Protocol (DLEP)". The

repository is to be managed using the "Specification Required" policy documented in [RFC5226].

All status codes are in the range [0..255], defined in Table 3.

13.5. DLEP Extensions Registrations

A new repository for DLEP extensions must be created, entitled "Extension Type Values for the Dynamic Link Event Protocol (DLEP)". The repository is to be managed using the "Specification Required" policy documented in [RFC5226].

All extension values are in the range [0..65535]. Current allocations are:

Code	Description
0	Reserved
1	Credit Windowing
2-65519	Unassigned. Available for future extensions
65520-65534	Private Use. Available for experiments
65535	Reserved

Table 4: DLEP Extension types

13.6. DLEP Well-known Port

It is requested that IANA allocate a single well-known port number for both TCP and UDP, for DLEP communication. SCTP port allocation is not required.

13.7. DLEP IPv4 Link-local Multicast Address

It is requested that IANA allocate an IPv4 link-local multicast address for DLEP discovery signals.

13.8. DLEP IPv6 Link-local Multicast Address

It is requested that IANA allocate an IPv6 link-local multicast address for DLEP discovery signals.

14. Acknowledgements

We would like to acknowledge and thank the members of the DLEP design team, who have provided invaluable insight. The members of the

design team are: Teco Boot, Bow-Nan Cheng, John Dowdell, and Henning Rogge.

We would also like to acknowledge the influence and contributions of Greg Harrison, Chris Olsen, Martin Duke, Subir Das, Jaewon Kang, Vikram Kaul, Nelson Powell, Lou Berger, and Victoria Mercieca.

15. References

15.1. Normative References

[CREDIT] Ratliff, S., "Credit Windowing extension for DLEP", draft-ietf-manet-credit-window-00 IETF draft, October 2015.

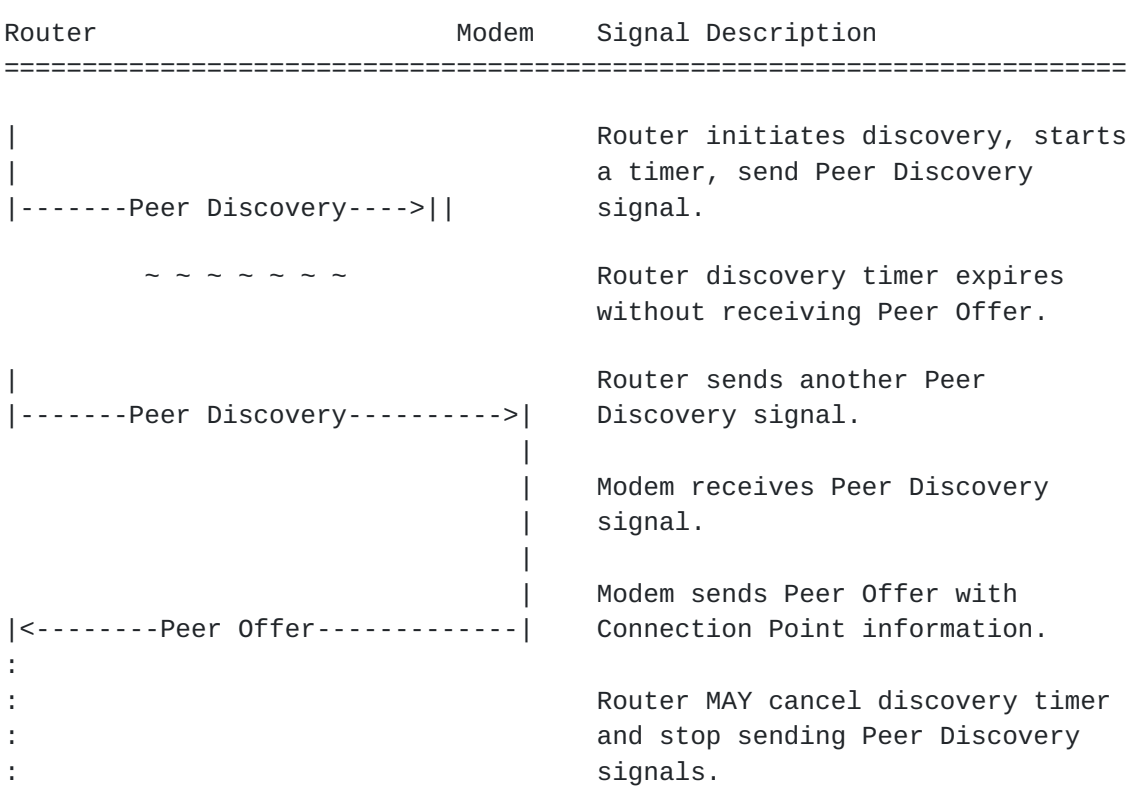
[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

15.2. Informative References

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

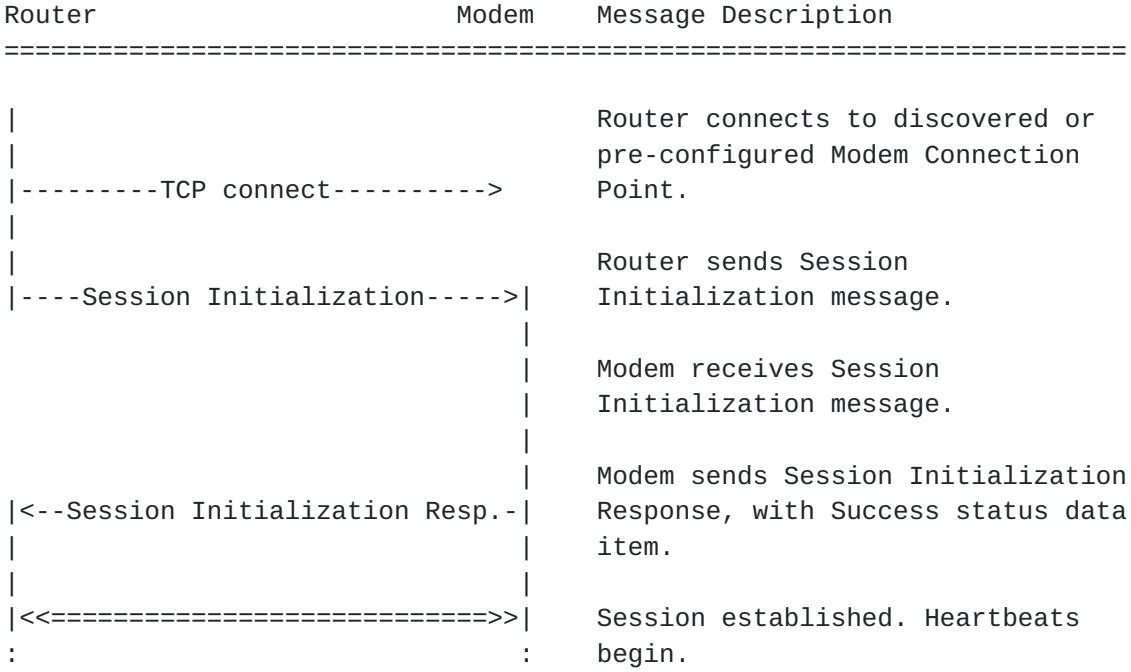
[RFC5578] Berry, B., Ed., Ratliff, S., Paradise, E., Kaiser, T., and M. Adams, "PPP over Ethernet (PPPoE) Extensions for Credit Flow and Link Metrics", RFC 5578, DOI 10.17487/RFC5578, February 2010, <http://www.rfc-editor.org/info/rfc5578>.

Appendix A. Discovery Signal Flows

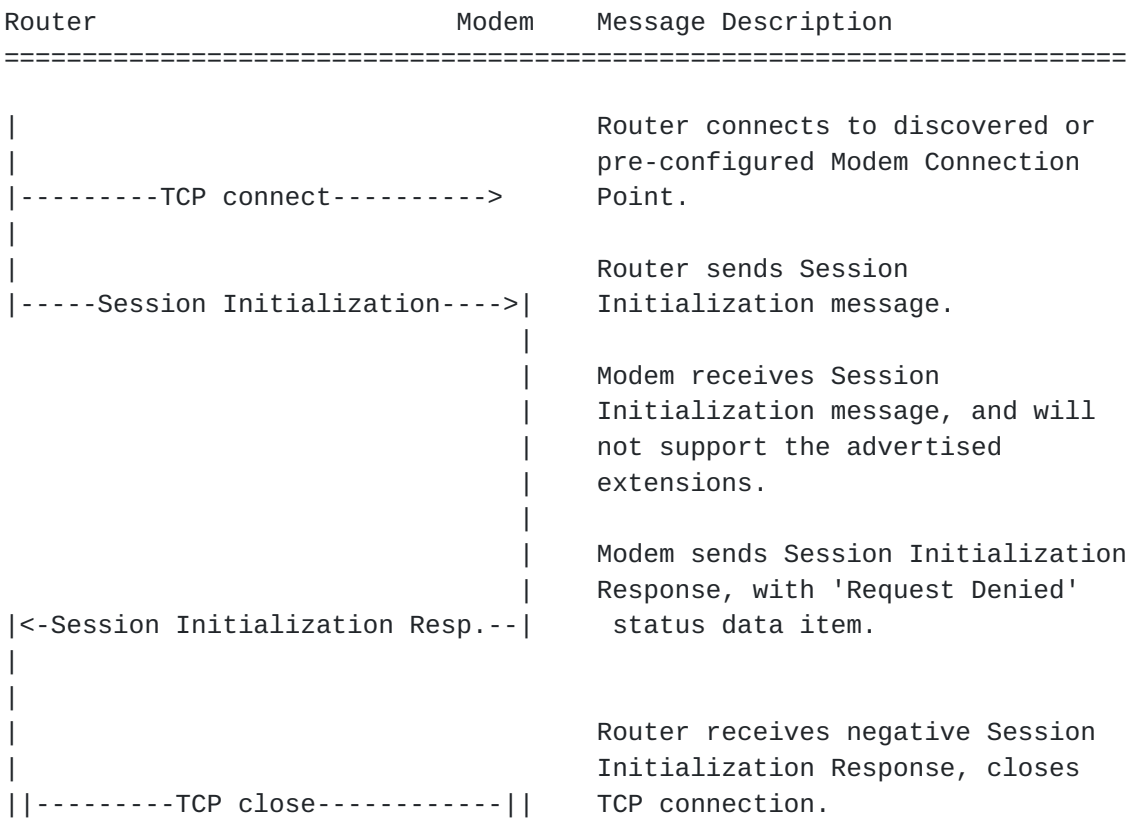


Appendix B. Peer Level Message Flows

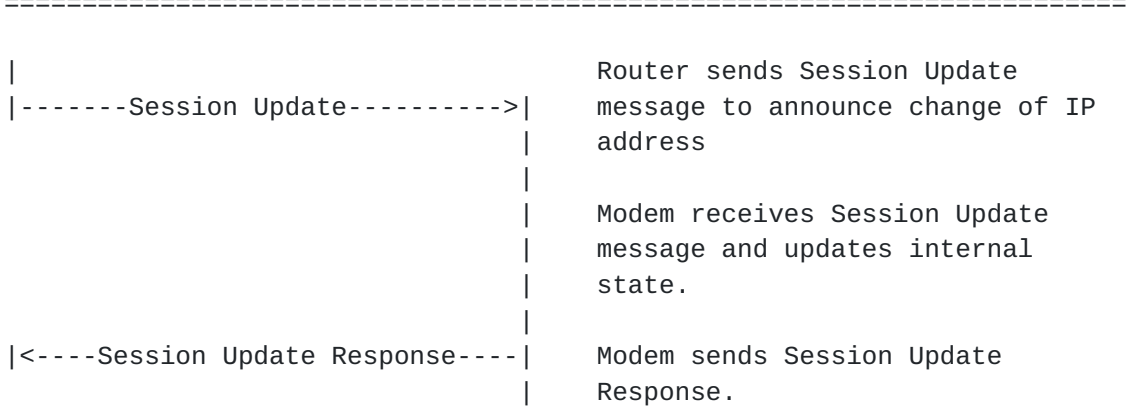
B.1. Session Initialization



B.2. Session Initialization - Refused



B.3. Router Changes IP Addresses



B.4. Modem Changes Session-wide Metrics

```
Router                          Modem    Message Description
=============================================================================

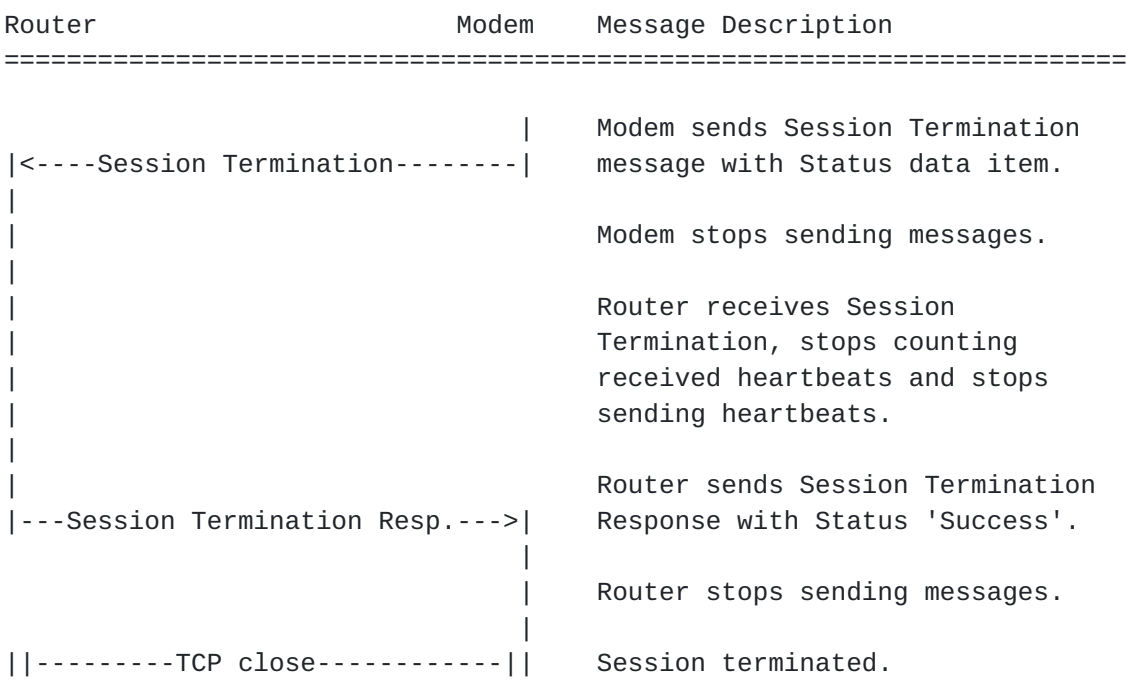
                                    |    Modem sends Session Update message
                                    |    to announce change of modem-wide
|<--------Session Update---------|    metrics
|
|                                       Router receives Session Update
|                                       message and updates internal
|                                       state.
|
|----Session Update Response---->|    Router sends Session Update
                                    |    Response.
```

B.5. Router Terminates Session

```
Router                          Modem    Message Description
=============================================================================

|                                       Router sends Session Termination
|------Session Termination------>|    message with Status data item.
|                                 |
|-------TCP shutdown (send)--->   |    Router stops sending messages.
                                  |
                                  |    Modem receives Session
                                  |    Termination, stops counting
                                  |    received heartbeats and stops
                                  |    sending heartbeats.
                                  |
                                  |    Modem sends Session Termination
|<---Session Termination Resp.---|    Response with Status 'Success'.
|
|                                       Modem stops sending messages.
|
||---------TCP close------------||    Session terminated.
```

B.6. Modem Terminates Session



B.7. Session Heartbeats

```
Router                        Modem    Message Description
=============================================================================

|----------Heartbeat------------>|    Router sends heartbeat message
                                 |
                                 |    Modem resets heartbeats missed
                                 |    counter.

         ~ ~ ~ ~ ~ ~ ~

|---------[Any message]--------->|    When the Modem receives any
                                 |    message from the Router.
                                 |
                                 |    Modem resets heartbeats missed
                                 |    counter.

         ~ ~ ~ ~ ~ ~ ~

|<---------Heartbeat-------------|    Modem sends heartbeat message
|
|                                     Router resets heartbeats missed
|                                     counter.

         ~ ~ ~ ~ ~ ~ ~

|<--------[Any message]----------|    When the Router receives any
|                                     message from the Modem.
|
|                                     Modem resets heartbeats missed
|                                     counter.
```

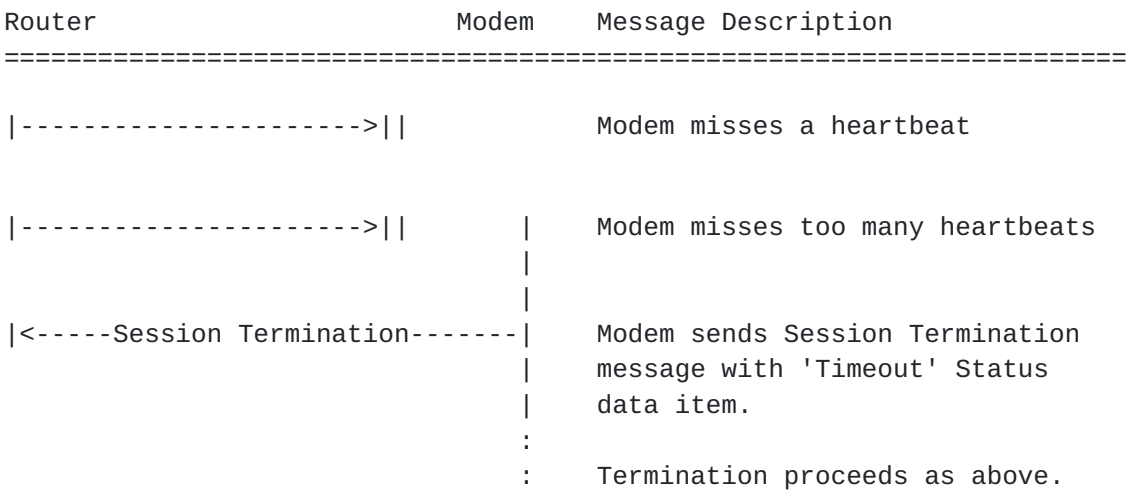
B.8. Router Detects a Heartbeat timeout

```
Router                        Modem    Message Description
=============================================================================

        ||<----------------------|    Router misses a heartbeat

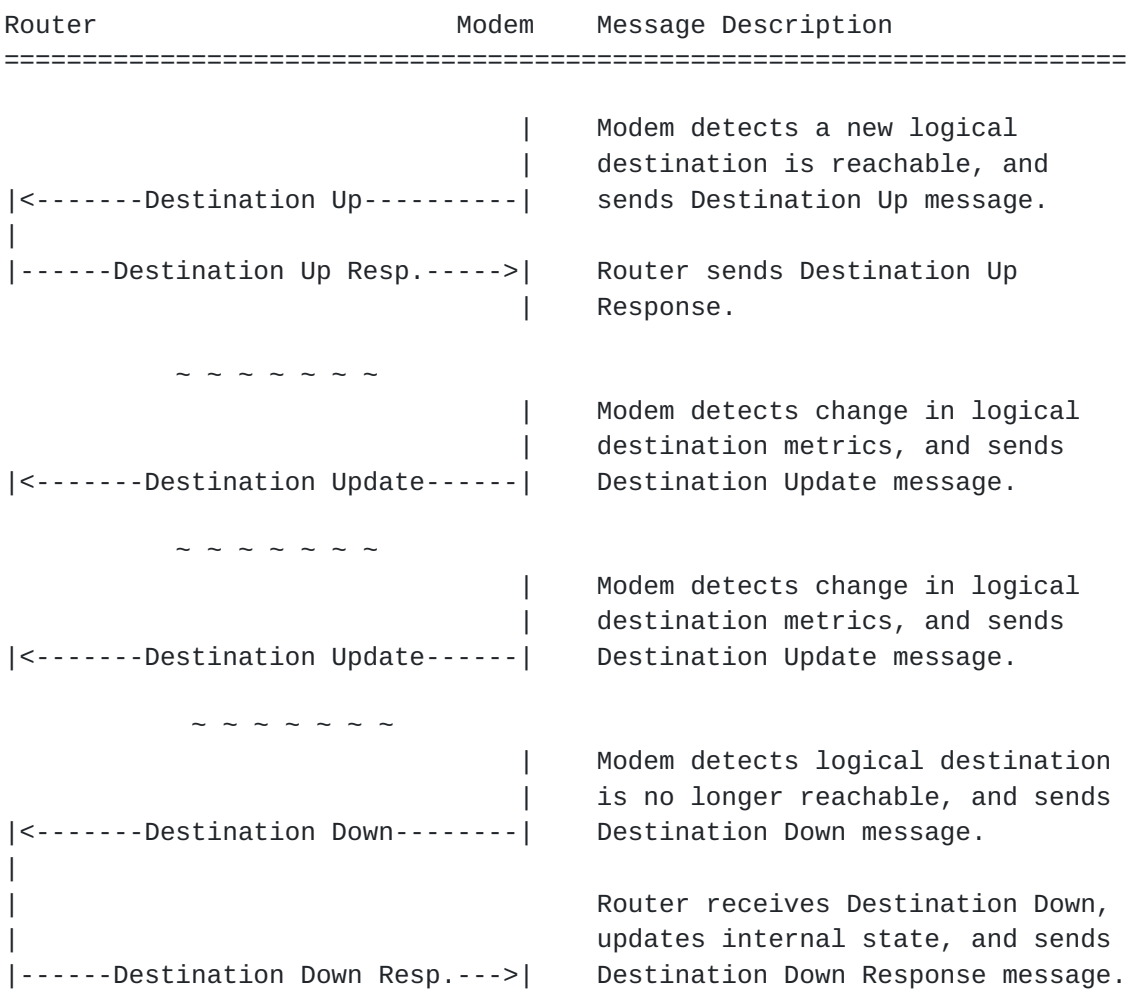

|       ||<----------------------|    Router misses too many heartbeats
|
|
|------Session Termination------>|    Router sends Session Termination
|                                     message with 'Timeout' Status
|                                     data item.
:
:                                     Termination proceeds as above.
```

B.9. Modem Detects a Heartbeat timeout

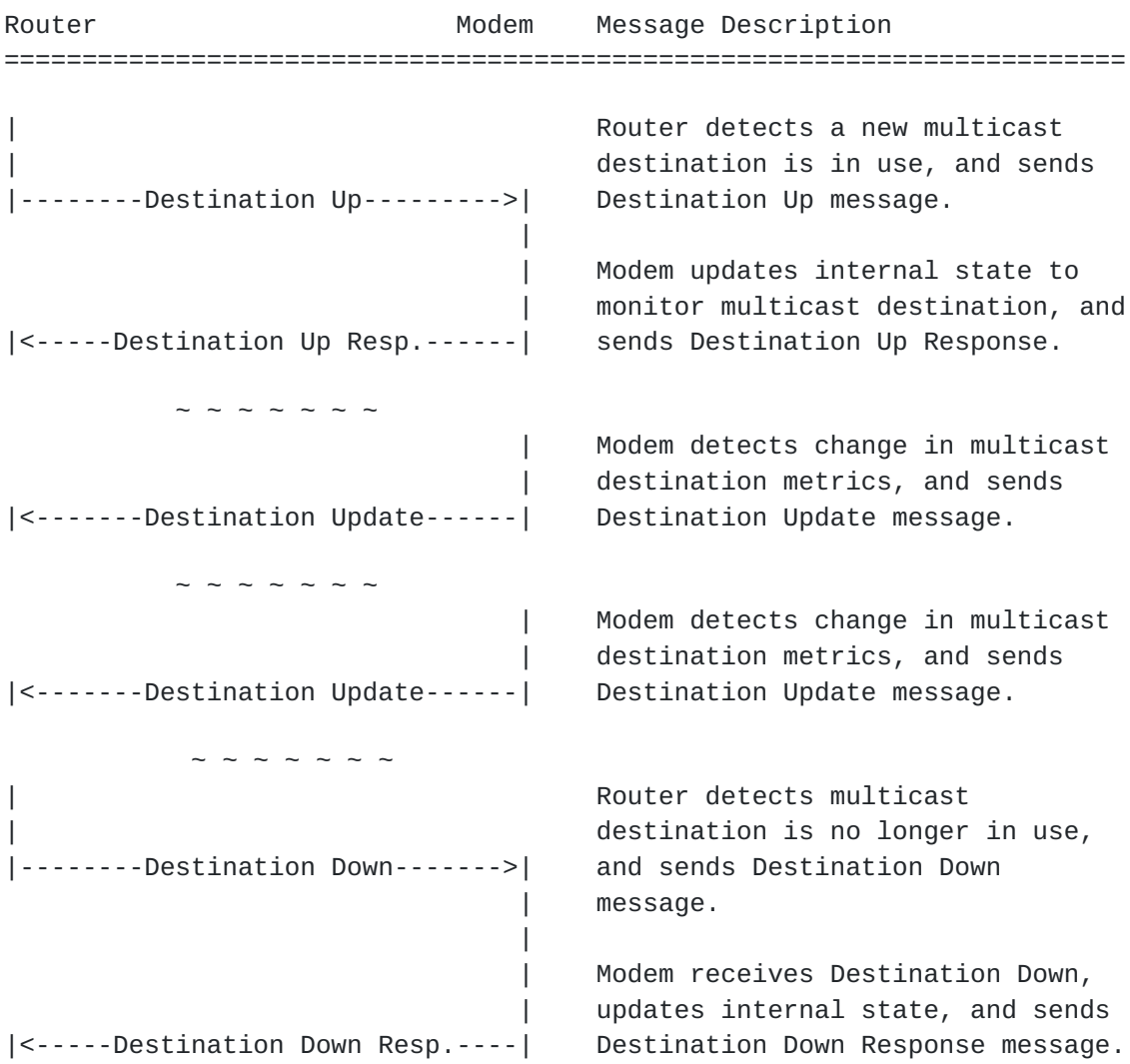


Appendix C. Destination Specific Message Flows

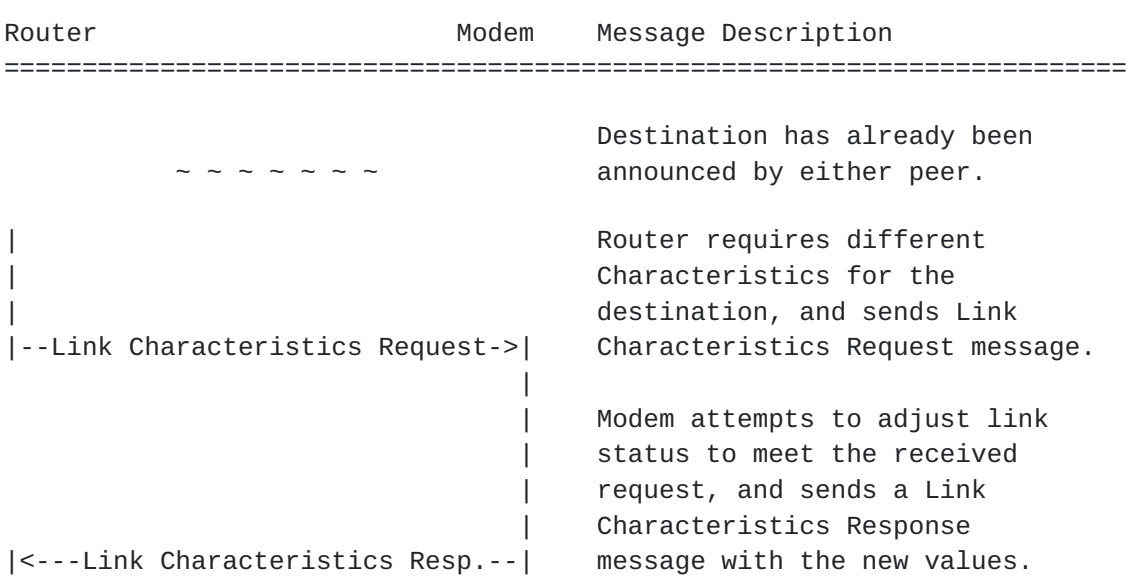
C.1. Common Destination Notification



C.2. Multicast Destination Notification



C.3. Link Characteristics Request



Authors' Addresses

Stan Ratliff
VT iDirect
13861 Sunrise Valley Drive, Suite 300
Herndon, VA 20171
USA

Email: sratliff@idirect.net

Shawn Jury
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134
USA

Email: sjury@cisco.com

Darryl Satterwhite
Broadcom

Email: dsatterw@broadcom.com

Rick Taylor
Airbus Defence & Space
Quadrant House
Celtic Springs
Coedkernew
Newport NP10 8FZ
UK

Email: rick.taylor@airbus.com

Bo Berry