Mobile Ad hoc Networks Working
Group
Internet-Draft
Intended status: Standards Track
Expires: September 22, 2013

S. Ratliff
B. Berry
G. Harrison
Cisco Systems
D. Satterwhite
Broadcom
S. Jury
NetApp

March 25, 2013

Dynamic Link Exchange Protocol (DLEP)
draft-ietf-manet-dlep-04

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 forwarding 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.

Table of Contents

1. Introduction

There exist today a collection of modem devices that control links of variable bandwidth and quality. Examples of these types of links include line-of-sight (LOS) radios, satellite terminals, and cable/DSL modems. Fluctuations in speed and quality of these links can occur due to configuration (in the case of cable/DSL modems), 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 bandwidth varies with respect to individual neighbors on a link, and with the type of traffic being sent. As an example, consider the case of an 802.11g access point, serving 2 associated laptop computers. In this environment, the answer to the question "What is the bandwidth on the 802.11g 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 bandwidth of 54Mbps for unicast traffic, the other laptop, being relatively far away, or obstructed by some object, can simultaneously have a bandwidth 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 bandwidth links, mobile networks are challenged by the notion that link connectivity will come and go over time. Effectively utilizing a relatively short-lived connection is problematic in IP routed networks, as routing protocols tend to rely on independent timers at OSI Layer 3 to maintain network convergence (e.g. HELLO messages and/or recognition of DEAD routing adjacencies). These short-lived 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 timer-driven paradigm.

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, USB, or even a serial link. In the case of Ethernet or serial 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 bandwidth, leads to a situation where quality of service (QoS) profiles are extremely 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 bandwidth may be available, but will

not be used unless the network devices emit traffic at rate higher than the currently established rate. Increasing the traffic rate does not guarantee additional bandwidth will be allocated; rather, it may result in data loss and additional retransmissions on the link.

Addressing the challenges listed above, the authors have developed the Data 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 neighbors). The following diagrams are used to illustrate the scope of DLEP packets.

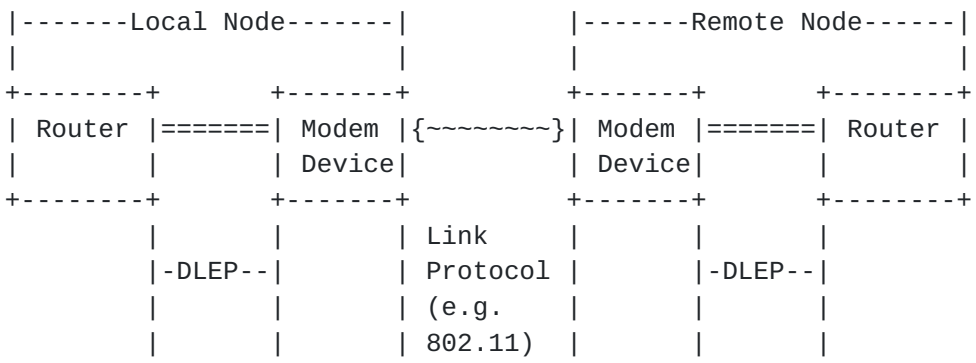


Figure 1: DLEP Network

In Figure 1, when the local modem detects the presence of a remote node, it (the local modem) sends a signal to its router via the DLEP protocol. Upon receipt of the signal, 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 utilize DLEP to report any characteristics of the link (bandwidth, latency, etc) that have changed. DLEP is independent of the link type and topology supported by the modem.

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 (bandwidth, 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.

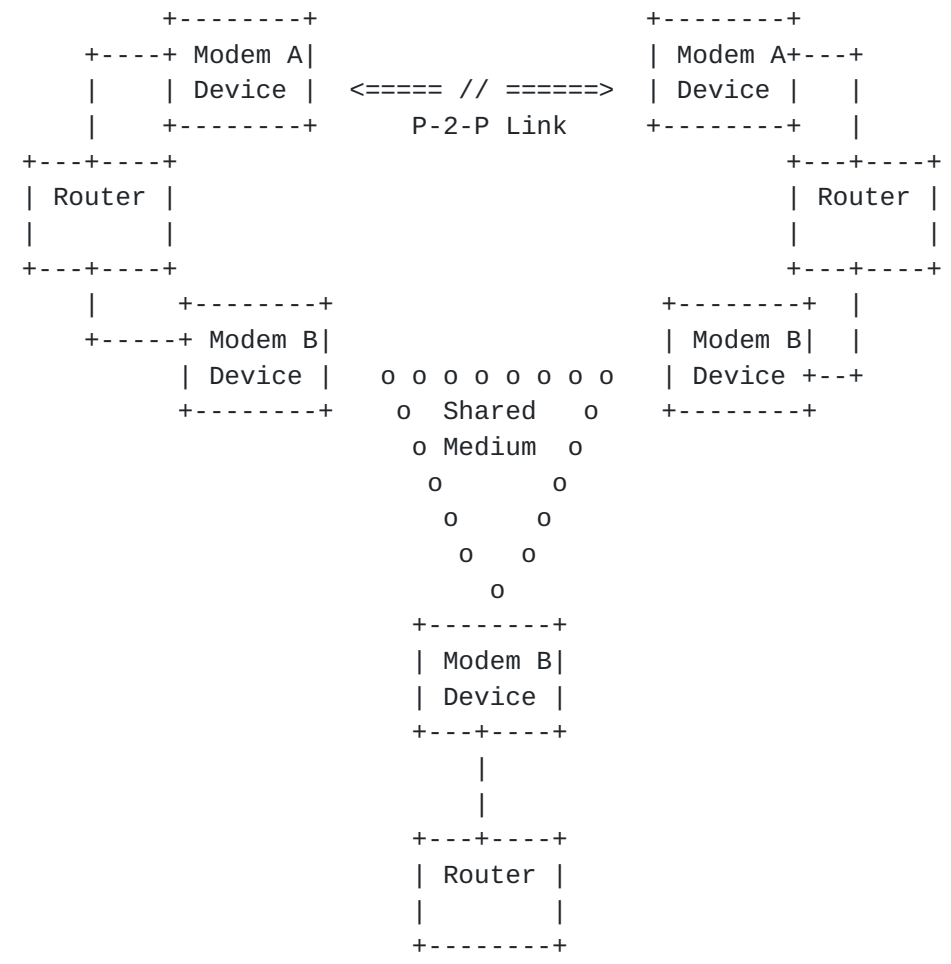


Figure 2: DLEP Network with Multiple Modem Devices

DLEP defines a set of logical signals used by modems and their attached routers. The signals are used 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 signals 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.

The protocol is defined as a collection of type-length-value (TLV) based messages, specifying the signals that are exchanged between a router and a modem, and the data items associated with the signal. This document specifies transport of DLEP signals and data items via the UDP transport. Other transports for the protocol are possible, but are outside the scope of this document.

DLEP signals are further defined as mandatory or optional. Signals will additionally have mandatory and optional data items.

Implementations MUST support all mandatory signals and their mandatory data items to be considered compliant. Implementations MAY also support some, or all, of the optional signals and data items.

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), a separate DLEP session MUST exist for each modem. If a modem device supports multiple connections to a router (via multiple logical or physical interfaces), or supports connections to multiple routers, a separate DLEP session MUST exist for each connection. This router/modem session provides a carrier for information exchange concerning neighbors (remote nodes) that are accessible via the modem device. As such, all of the neighbor-level exchanges in DLEP can be envisioned as building an information base concerning the remote nodes, and the link characteristics to those nodes.

Multicast traffic 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 neighbor. The modem, once it is aware of the existence of this logical neighbor, reports link characteristics just as it would for any other destination in the network. The specific algorithms a modem would use to report metrics on multicast (or logical) destinations is outside the scope of this specification, and is left to specific implementations to decide.

1.1 Requirements

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

2. Assumptions

Routers and modems that exist as part of the same node (e.g., that are locally connected) can utilize a discovery technique to locate each other, thus avoiding a-priori configuration. The modem is responsible for initialing the discovery process, using the Peer Discovery message.

DLEP utilizes a session-oriented paradigm. A router and modem form a session by completing the discovery process. This router-modem session persists unless or until it either (1) times out, based on

the timeout values supplied, or (2) is explicitly torn down by one of the participants. Note that use of timers in DLEP is OPTIONAL; that is, implementations can choose to run with no timers (or effectively, timers set to an infinite value).

DLEP assumes that participating modems, and their physical links, act as a transparent bridge. Specifically, the assumption is that the destination MAC address for data traffic in any frame emitted by the router should be the MAC address of a device in the remote node. DLEP also assumes that MAC addresses are unique within the context of the router-modem session.

This document refers to a remote node as a "Neighbor". Neighbors can be identified by either the router or the modem, and represent a specific destination (e.g., an address) that exists on the link(s) managed by the modem. Examples of a destination include a MAC address, a unicast Layer 3 address, or a multicast Layer 3 address. As "neighbors" are discovered, DLEP routers and modems build an information base on destinations accessible via the modem. Changes in link characteristics MAY then be reported as being "modem-wide" (effecting ALL neighbors accessed via the modem) or MAY be neighbor (destination) specific.

The DLEP signals concerning neighbors thus become the way for routers and modems to maintain, and notify each other about, an information base representing the physical and logical (e.g., multicast) destinations accessible via the modem device. The information base would contain addressing information (e.g., MAC address, and OPTIONALLY, Layer 3 addresses), link characteristics (metrics), and OPTIONALLY, flow control information (credits).

DLEP assumes that security on the session (e.g. authentication of session partners, encryption of traffic, or both) is dealt with by the underlying transport mechanism (e.g., by using a transport such as DTLS [DTLS]).

Sequence Numbers for DLEP messages start at 0 and are incremented by one for each original and retransmitted message. The unsigned 16-bit Sequence Number rolls over at 65535 to 0. Sequence Numbers are unique within the context of a DLEP session. Sequence numbers are used in DLEP to correlate a response to a request.

This document specifies an implementation of the DLEP signals and data items running over the UDP transport, utilizing a well-known UDP Port number. It is assumed that DLEP running over other transport mechanisms would be documented separately.

3. Credits

DLEP includes an OPTIONAL credit-windowing scheme analogous to the one documented in [RFC5578]. In this scheme, traffic between the router and modem is treated as two unidirectional windows. This document identifies these windows as the "Modem Receive Window", or MRW, and the "Router Receive Window", or RRW.

If credits are used, they MUST be granted by the receiver on a given window - that is, on the "Modem Receive Window" (MRW), the modem is responsible for granting credits to the router, allowing it (the router) to send data to the modem. Likewise, the router is responsible for granting credits on the RRW, which allows the modem to send data to the router.

DLEP expresses all credit data in number of octets. The total number of credits on a window, and the increment to add to a grant, are always expressed as a 64-bit unsigned quantity.

If used, credits are managed on a neighbor-specific basis; that is, separate credit counts are maintained for each neighbor requiring the service. Credits do not apply to the DLEP session that exists between routers and modems.

4. Metrics

DLEP includes the ability for the router and modem to communicate metrics that reflect the characteristics (e.g. bandwidth, latency) of the variable-quality link in use. As mentioned in the introduction section of this document, metrics have to be used within a context - for example, metrics to a unicast address in the network. DLEP allows for metrics to be sent within two contexts - metrics for a specific neighbor (those for a given destination within the network), and "modem-wide" (those that apply to all destinations accessed via the modem). Metrics supplied on DLEP Peer signals are, by definition, modem-wide; metrics supplied on Neighbor signals are, by definition, used for the specific neighbor only.

Metrics are further subdivided into transmit and receive metrics.

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

The approach of allowing for different contexts for metric data increases both the flexibility and the complexity of using metric data. This document details the mechanism whereby the data is transmitted, however, the specific algorithms (precedence, etc) for utilizing the dual-context metrics is out of scope and not addressed by this document.

5. Extensions to DLEP

While this draft represents the best efforts of the co-authors, and 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 utilized. To allow for future innovation, the draft allocates numbering space for experimental implementations of both signals and data items.

DLEP implementations MUST be capable of parsing and acting on the mandatory signals and data items as documented in this specification. DLEP signals/data items that are optional, or are in the experimental numbering range SHOULD be silently dropped by an implementation if they are not understood.

The intent of the optional signals and data items, as well as the experimental numbering space, is to allow for further development of DLEP protocol features and function. Having experimental space reserved for both signals and data items gives maximum flexibility for extending the protocol as conditions warrant. For example, experimental data items could be used by implementations to send additional metrics. A combination of experimental signals, and associated data items, could be used to implement new flow control schemes. If subsequent research and development define new features and function, then it should be standardized either as an update to this document, or as an additional stand-alone specification.

6. Normal Session Flow

At the start of a run, DLEP implementations (both router and modem) initialize the communications path. In a UDP implementation, this includes opening a socket and binding to the well-known port address (TBD). Once the communications path is established, modem implementations are free to issue a "Peer Discovery" message. The Peer Discovery MAY be sent either to the multicast address allocated for DLEP (TBD), or to a unicast address, obtained via a-priori configuration.

Routers receiving a Peer Discovery message respond with a "Peer Offer" signal to indicate readiness to participate in the DLEP

session. The receiver of a Peer Offer message responds with a "Peer Offer ACK" message, completing discovery. While the Peer Discovery message MAY be sent to the DLEP multicast address (TBD), the Peer Offer, and all subsequent traffic, is sent to the unicast address that originated the Peer Discovery. Once the Peer Offer signal is acknowledged, both participants (router and modem) transition to the "in session" state, creating a logical, stateful session between the modem and the router. Subsequent DLEP signals are then processed within the context of this router/modem session. In the UDP-based implementation, traffic between DLEP modems and routers is correlated using the UDP 4-tuple (Source Address, Source Port, Destination Address, Destination Port). DLEP partners use these signals to build their respective information bases regarding destinations that are accessible via the modem, and link characteristics associated with those destinations.

The "in session" state created by the discovery signals is maintained until one of the following conditions occur:

- The session is explicitly terminated (using Peer Termination), or
- The session times out, based on supplied timeout values.

In order to maintain the session between router and modem, OPTIONAL periodic "Heartbeat" messages MAY be exchanged. These messages are intended to keep the session alive, and to verify bidirectional connectivity between the two participants. DLEP also provides for an OPTIONAL Peer Update message, intended to communicate some change in status (e.g., a change of layer 3 address parameters, or a modem-wide link change).

In addition to the messages above, the participants will transmit DLEP messages concerning destinations in the network. These messages trigger creation/maintenance/deletion of "neighbors" 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 "Neighbor Up" signal. Receipt of a Neighbor Up causes the router to allocate the necessary resources, creating an entry in the information base with the specifics (e.g., MAC Address, Latency, Data Rate, etc) of the neighbor. The loss of a destination is communicated via the "Neighbor Down" signal, and changes in status to the destination (e.g. varying link quality, or addressing changes) are communicated via the "Neighbor Update" signal. The information on a given neighbor will persist in the router's information base until (1) a "Neighbor Down" is received, indicating that the modem has lost contact with the remote node, or (2) the router/modem session terminates, indicating that the router has lost contact with its own local modem.

Again, metrics can be expressed within the context of a specific neighbor via the Neighbor Update message, or on a modem-wide basis via the Peer Update message. In cases where metrics are provided on the router/modem session, the receiver MUST propagate the metrics to all neighbors in its information base that are accessed via the originator. A DLEP participant MAY send metrics both in a router/modem session context (via the Peer Update message) and a specific neighbor context (via Neighbor Update) at any time. The heuristics for applying received metrics is left to implementations.

In addition to receiving metrics about the link, DLEP provides an OPTIONAL signal allowing a router to request a different amount of bandwidth, or latency, from the modem. This signal is referred to as the Link Characteristics Message, and gives the router the ability to deal with requisite increases (or decreases) of allocated bandwidth/latency in demand-based schemes in a more deterministic manner.

7. Mandatory Signals and Data Items

The following DLEP signals are considered core to the specification; implementations MUST support these signals, and the associated data items, in order to be considered compliant:

Signal	Data Items
Peer Discovery	None
Peer Offer	None
Peer Offer ACK	Status
Peer Termination	None
Peer Termination ACK	Status
Neighbor Up	MAC Address Maximum Data Rate Current Data Rate
Neighbor Update	MAC Address Maximum Data Rate Current Data Rate
Neighbor Down	MAC Address

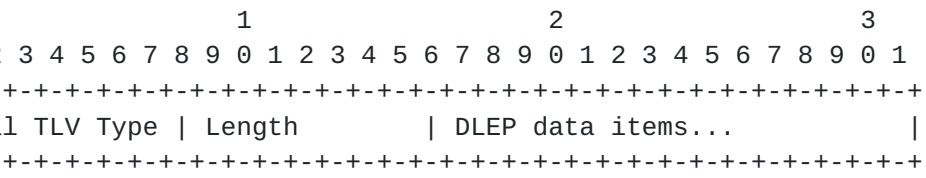
All other DLEP signals and data items are OPTIONAL. Implementations MAY choose to provide them. Implementations that do not support

optional signals and data items SHOULD parse, and silently drop, all unsupported signals and/or data items.

8. Generic DLEP Packet Definition

The Generic DLEP Packet consists of a sequence of TLVs. The first TLV represents the signal being communicated (e.g., a "Neighbor Up", or a "Peer Offer"). Subsequent TLVs contain the data items pertinent to the signal (e.g., Maximum Data Rate, or Latency, etc).

The Generic DLEP Packet Definition contains the following fields:



Signal - One of the DLEP Signal TLV type values defined in this document.

Length - The length of all of the DLEP data items associated with this signal.

DLEP data items - One or more data items, encoded in TLVs, as defined in this document.

9. DLEP Data Items

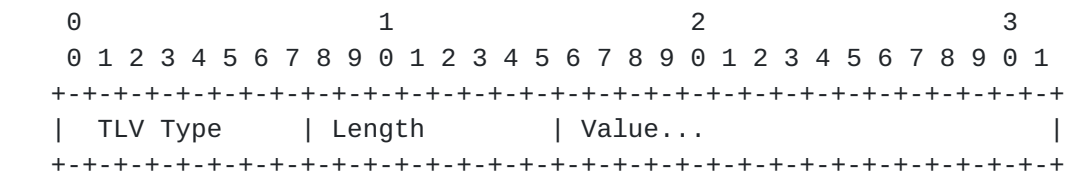
As mentioned earlier, DLEP protocol messages are transported as a collection of TLVs. The first TLV present in a DLEP message MUST be one of the Signal TLVs, documented in section [INSERT REFERENCE HERE]. The signals are followed by one or more data items, indicating the specific changes that need to be instantiated in the receiver's information base.

Valid DLEP Data Items are:

TLV Value	TLV Description
TBD	DLEP Version
TBD	Peer Type
TBD	IPv4 Address
TBD	IPv6 Address
TBD	Maximum Data Rate (Receive) (MDRR)

TBD	Maximum Data Rate (Transmit) (MDRT)
TBD	Current Data Rate (Receive) (CDRR)
TBD	Current Data Rate (Transmit) (CDRT)
TBD	Transmit Latency
TBD	Receive Resources
TBD	Transmit Resources
TBD	Expected Forwarding Time (EFT)
TBD	Relative Link Quality (Receive) (RLQR)
TBD	Relative Link Quality (Transmit) (RLQT)
TBD	Status
TBD	Heartbeat Interval/Threshold
TBD	Neighbor down ACK timer
TBD	Link Characteristics ACK timer
TBD	Credit Window Status
TBD	Credit Grant
TBD	Credit Request

DLEP data item TLVs contain the following fields:



TLV Type - An 8-bit unsigned integer field specifying the data item being sent.

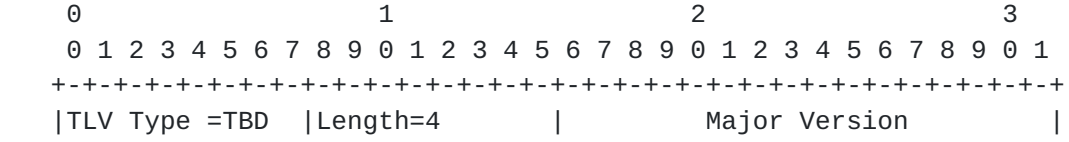
Length - An 8-bit length of the value field of the data item

Value - A field of length <Length> which contains data specific to a particular data item.

9.1 DLEP Version

The DLEP Version TLV is an OPTIONAL TLV in both the Peer Discovery and Peer Offer messages. The Version TLV is used to indicate the version of the protocol running in the originator. A participant MAY use this information to decide if the potential session partner is running at a supported level.

The DLEP Version TLV contains the following fields:



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Minor Version           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

TLV Type - TBD

Length - Length is 4

Major Version - Major version of the modem or router protocol.

Minor Version - Minor version of the modem or router protocol.

Support of this draft is indicated by setting the Major Version to '1', and the Minor Version to '3' (e.g. Version 1.3).

9.2 Peer Type

The Peer Type TLV is an OPTIONAL TLV in both the Peer Discovery and Peer Offer messages. The Peer Type TLV 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 TLV 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|TLV Type =TBD  |Length= peer   |Peer Type String               |
|               |type string len|Max Len = 80                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

TLV Type - TBD

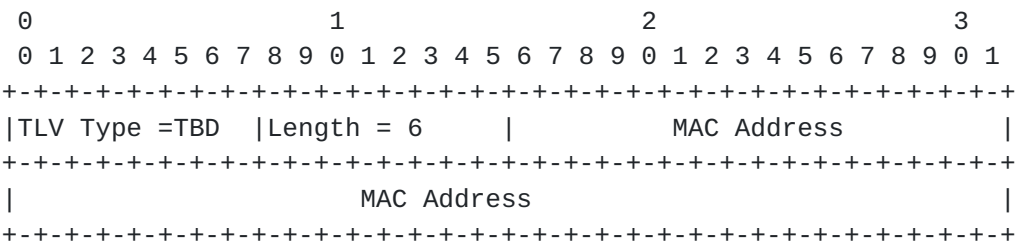
Length - Length of peer type string (80 octets maximum).

Peer Type String - Non-Null terminated string, maximum length of 80 octets. For example, a satellite modem might set this variable to 'Satellite terminal'.

9.3 MAC Address

The MAC address TLV MUST appear in all neighbor-oriented signals (e.g. Neighbor Up, Neighbor Up ACK, Neighbor Down, Neighbor Down ACK, Neighbor Update, Link Characteristics Request, and Link Characteristics ACK). The MAC Address TLV contains the address of the destination on the remote node. The MAC address MAY be either a

physical or a virtual destination. Examples of a virtual destination would be a multicast MAC address, or the broadcast MAC (0xFFFFFFFFFFFF).



TLV Type - TBD

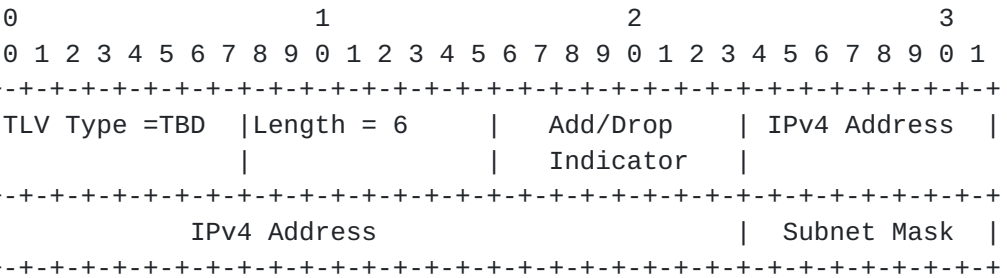
Length - 6

MAC Address - MAC Address of the destination (either physical or virtual).

9.4 IPv4 Address

The IPv4 Address TLV is an OPTIONAL TLV. If supported, it MAY appear in Neighbor Up, Neighbor Update, and Peer Update messages. When included in Neighbor messages, the IPv4 Address TLV contains the IPv4 address of the neighbor, as well as a subnet mask value. In the Peer Update message, it contains the IPv4 address of the originator of the message. In either case, the TLV 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 TLV contains the following fields:



TLV Type - TBD

Length - 6

Add/Drop - Value indicating whether this is a new or existing IPv4 address

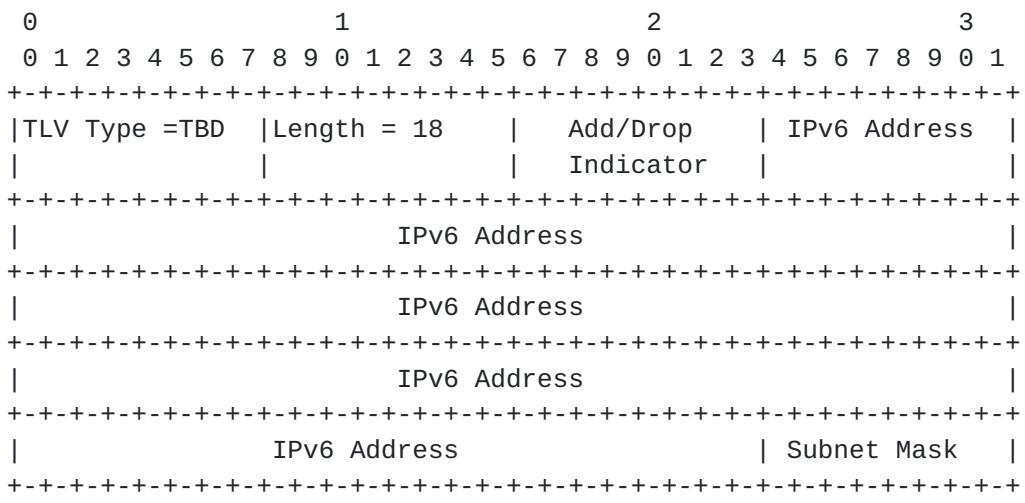
IPv4 Address - The IPv4 address of the neighbor or peer.

Subnet Mask - A subnet mask (0-32) to be applied to the IPv4 address.

9.5 IPv6 Address

The IPv6 Address TLV is an OPTIONAL TLV. If supported, it MAY be used in the Neighbor Up, Neighbor Update, Peer Discovery, and Peer Update Messages. When included in Neighbor messages, this data item contains the IPv6 address of the neighbor. In the Peer Discovery and Peer Update, it contains the IPv6 address of the originating 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, as well as a subnet mask.

The IPv6 Address TLV contains the following fields:



TLV Type - TBD

Length - 18

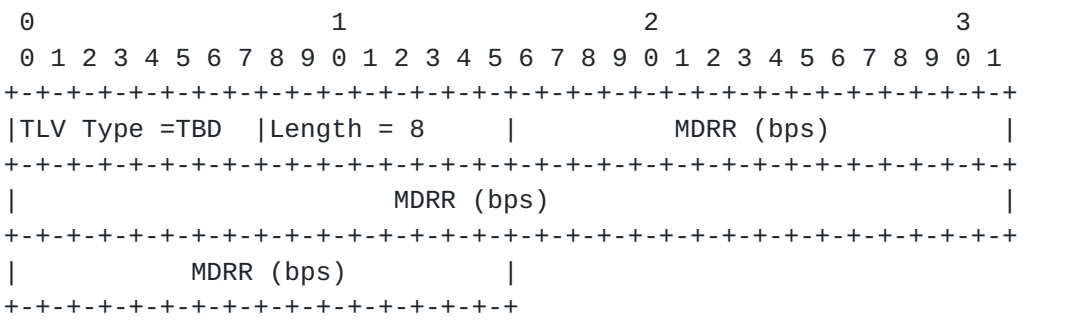
Add/Drop - Value indicating whether this is a new or existing address (0x01), or a withdrawal of an address (0x02).

IPv6 Address - IPv6 Address of the neighbor or peer.

Subnet Mask - A subnet mask value (0-128) to be applied to the Ipv6 address.

9.6 Maximum Data Rate (Receive)

The Maximum Data Rate Receive (MDRR) TLV is used in Neighbor Up, Neighbor Update, Peer Discovery, Peer Update, and Link Characteristics ACK Messages to indicate the maximum theoretical data rate, in bits per second, that can be achieved while receiving data on the link. When metrics are reported via the messages listed above, the maximum data rate receive MUST be reported. A value of 0 for the MDRR indicates that the Maximum Data Rate Receive is currently 'unknown'.



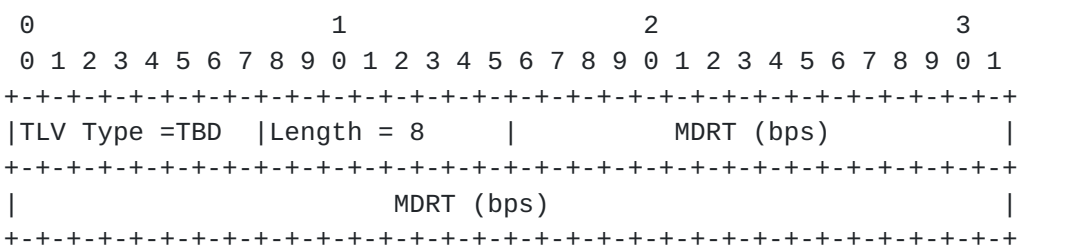
TLV Type - TBD

Length - 8

Maximum Data Rate Receive - A 64-bit unsigned number, representing the maximum theoretical data rate, in bits per second (bps), that can be achieved while receiving on the link. An MDRR value of 0 MAY be used to indicate an 'unknown' data rate.

9.7 Maximum Data Rate (Transmit)

The Maximum Data Rate Transmit (MDRT) TLV is used in Neighbor Up, Neighbor Update, Peer Discovery, Peer Update, and Link Characteristics ACK Messages to indicate the maximum theoretical data rate, in bits per second, that can be achieved while transmitting data on the link. When metrics are reported via the messages listed above, the maximum data rate transmit MUST be reported. A value of 0 for the MDRT MAY be used to indicate that the Maximum Data Rate Transmit is currently unknown, or cannot be calculated.



```
|           MDRT (bps)          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

TLV Type - TBD

Length - 8

Maximum Data Rate Transmit - A 64-bit unsigned number, representing the maximum theoretical data rate, in bits per second (bps), that can be achieved while transmitting on the link. An MDRT value of 0 indicates an 'unknown' data rate.

9.8 Current Data Rate (Receive)

The Current Data Rate Receive (CDRR) TLV is used in Neighbor Up, Neighbor Update, Peer Discovery, Peer Update, Link Characteristics Request, and Link Characteristics ACK messages to indicate the rate at which the link is currently operating for receiving traffic. In the case of the Link Characteristics Request, CDRR represents the desired receive data rate for the link. When metrics are reported via the messages above (e.g. Neighbor Update), the current data rate receive MUST be reported.

The Current Data Rate Receive TLV 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|TLV Type =TBD  |TLV Flags=0x10 |Length = 8     |CDRR (bps)     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        CDRR (bps)                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        CDRR (bps)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

TLV Type - TBD

Length - 8

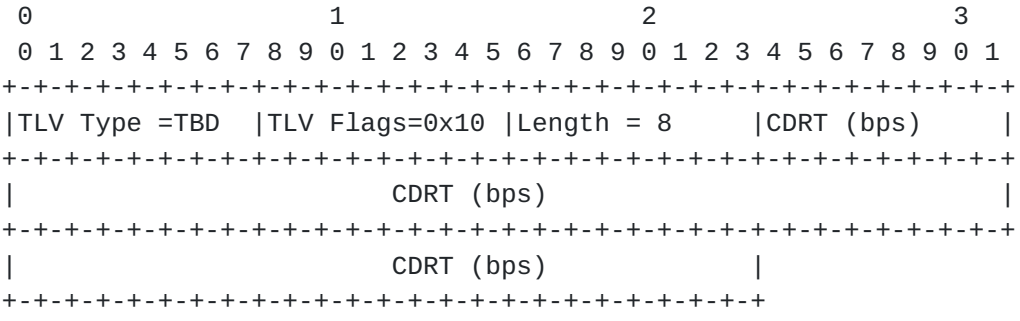
Current Data Rate Receive - A 64-bit unsigned number, representing the current data rate, in bits per second, that is currently be achieved while receiving traffic on the link. When used in the Link Characteristics Request, CDRR represents the desired receive rate, in bits per second, on the link. If there is no distinction between current

and maximum receive data rates, current data rate receive SHOULD be set equal to the maximum data rate receive. A CDRR value of 0 MAY be used to indicate the CDRT is unknown, or cannot be calculated.

9.9 Current Data Rate (Transmit)

The Current Data Rate Receive (CDRT) TLV is used in Neighbor Up, Neighbor Update, Peer Discovery, Peer Update, Link Characteristics Request, and Link Characteristics ACK messages to indicate the rate at which the link is currently operating for transmitting traffic. In the case of the Link Characteristics Request, CDRT represents the desired transmit data rate for the link. When metrics are reported via the messages above (e.g. Neighbor Update), the current data rate transmit MUST be reported.

The Current Data Rate Transmit TLV contains the following fields:



TLV Type - TBD

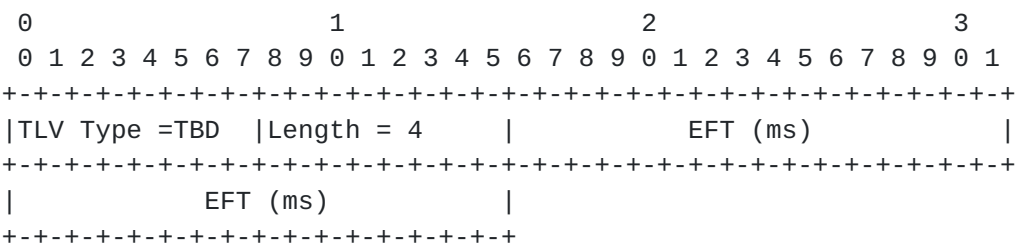
Length - 8

Current Data Rate Transmit - A 64-bit unsigned number, representing the current data rate, in bits per second, that is currently be achieved while transmitting traffic on the link. When used in the Link Characteristics Request, CDRT represents the desired transmit rate, in bits per second, 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. A CDRT value of 0 MAY be used to indicate the CDRT is 'unknown', or cannot be calculated.

9.10 Expected Forwarding Time

The Expected Forwarding Time (EFT) TLV is is an OPTIONAL data item. If supported, it MAY be used in Neighbor Up, Neighbor Update, Peer Discovery, and Peer Update messages to indicate the typical latency between the arrival of a given packet at the transmitting device and the reception of the packet at the other end of the link. EFT combines transmission time, idle time, waiting time, freezing time, and queuing time to the degree that those values are meaningful to a given transmission medium.

The Expected Forwarding Time TLV contains the following fields:



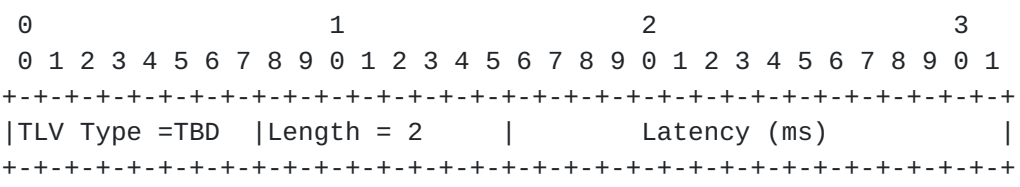
TLV Type - TBD

Length - 4

EFT - A 32-bit unsigned number, representing the expected forwarding time, in milliseconds, on the link.

9.11 Latency

The Latency TLV is an OPTIONAL data item. If supported, it is used in Neighbor Up, Neighbor Update, Peer Discovery, Peer Update, Link Characteristics Request, and Link Characteristics ACK messages to indicate the amount of latency on the link, or in the case of the Link Characteristics Request, to indicate the maximum latency required on the link.



TLV Type - TBD

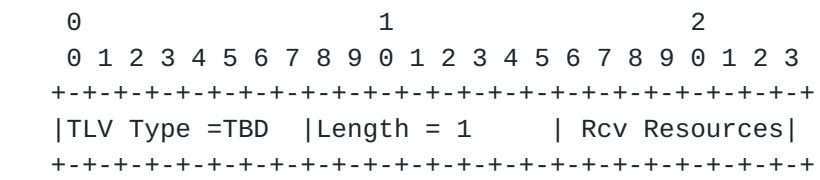
Length - 2

Latency - A 16-bit unsigned value, representing the transmission delay that a packet encounters as it is transmitted over the link. In Neighbor Up, Neighbor Update, and Link Characteristics ACK, this value is reported as delay, in milliseconds. The calculation of latency is implementation dependent. For example, the latency may be a running average calculated from the internal queuing. If a device cannot calculate latency, this TLV SHOUD NOT be issued. In the Link Characteristics Request Message, this value represents the maximum delay, in milliseconds, expected on the link.

9.12 Resources (Receive)

The Receive Resources TLV is an OPTIONAL data item. If supported, it is used in Neighbor Up, Neighbor Update, Peer Discovery, Peer Update, and Link Characteristics ACK messages to indicate a percentage (0-100) amount of resources (e.g. battery power), committed to receiving data, remaining on the originating peer.

The Resources TLV contains the following fields:



TLV Type - TBD

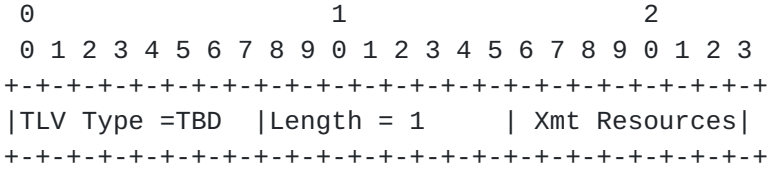
Length - 1

Receive Resources - A percentage, 0-100, representing the amount of remaining resources, such as battery power, allocated to receiving data. A value of '0' MAY be used to indicate the receive resources are unknown or cannot be calculated.

9.13 Resources (Transmit)

The Transmit Resources TLV is an OPTIONAL data item. If supported, it is used in Neighbor Up, Neighbor Update, Peer Discovery, Peer Update, and Link Characteristics ACK messages to indicate a percentage (0-100) amount of resources (e.g. battery power), committed to transmitting data, remaining on the originating peer.

The Resources TLV contains the following fields:



TLV Type - TBD

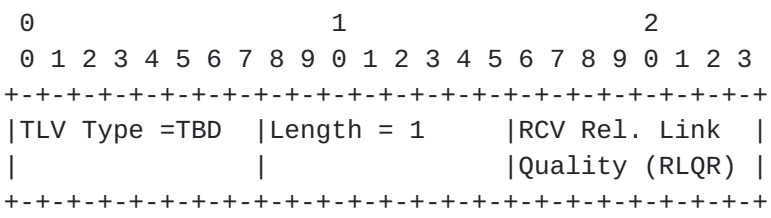
Length - 1

Transmit Resources - A percentage, 0-100, representing the amount of remaining resources, such as battery power, allocated to transmitting data. A value of '0' MAY be used to indicate the transmit resources are unknown or cannot be calculated.

9.14 Relative Link Quality (Receive)

The Relative Link Quality Receive (RLQR) TLV is an OPTIONAL data item. If supported, it is used in Neighbor Up, Neighbor Update, Peer Discovery, Peer Update, and Link Characteristics ACK messages to indicate the quality of the link for receiving data as calculated by the originating peer.

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



TLV Type - TBD

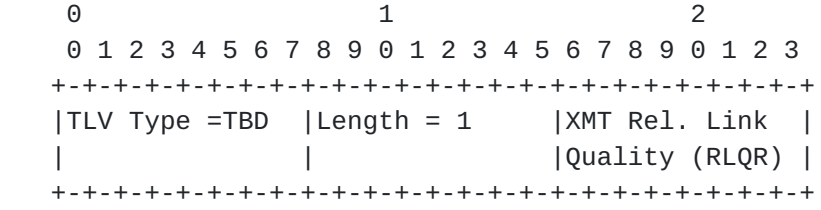
Length - 1

Relative Link Quality (Receive) - A non-dimensional number, 1-100, representing relative link quality. A value of 100 represents a link of the highest quality. A value of '0' indicated the RLQR is 'unknown', or cannot be calculated.

9.15 Relative Link Quality (Transmit)

The Transmit Link Quality Receive (RLQT) TLV is an OPTIONAL data item. If supported, it is used in Neighbor Up, Neighbor Update, Peer Discovery, Peer Update, and Link Characteristics ACK messages to indicate the quality of the link for transmitting data as calculated by the originating peer.

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



TLV Type - TBD

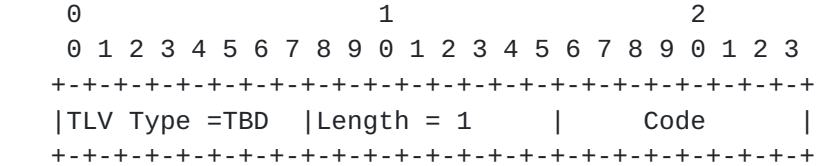
Length - 1

Relative Link Quality (Transmit) - A non-dimensional number, 1-100, representing relative link quality. A value of 100 represents a link of the highest quality. A value of '0' indicated the RLQT is 'unknown', or cannot be calculated.

9.16 Status

The Status TLV is sent as part of an acknowledgement message, from either the modem or the router, to indicate the success or failure of a given request.

The Status TLV contains the following fields:



TLV Type - TBD

Length - 1

Termination Code - 0 = Success, Non-zero = Failure. Specific values

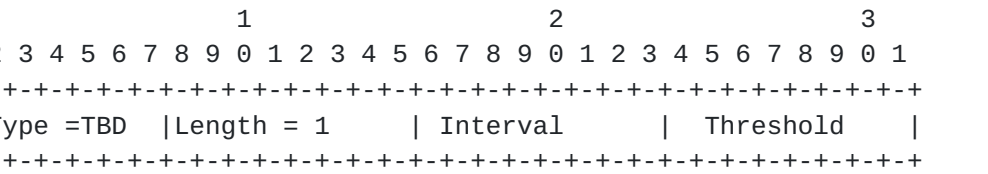
of a non-zero termination code depend on the operation requested (e.g. Neighbor Up, Neighbor Down, etc).

9.17 Heartbeat Interval/Threshold

The Heartbeat Interval/Threshold TLV is an OPTIONAL TLV. If supported, it MAY be sent during Peer Discovery to indicate the desired Heartbeat timeout window. If the modem includes the Heartbeat Interval TLV in Peer Discovery, the router MUST either accept the timeout interval supplied by the modem, or reject the Peer Discovery. Peer Discovery messages that do not include the Heartbeat Interval TLV in Peer Discovery indicates a desire to establish the router/modem session without an activity timeout (e.g. an infinite timeout value). If an activity timeout is supported, implementations MAY choose to implement heuristics such that signals sent/received reset the timer window.

The Interval is used to specify a period (in seconds) for Heartbeat Messages (See Section 23). The Threshold value is used to indicate the desired number of windows, each of time (Heartbeat Interval) seconds, to wait before either participant declares the router/modem session lost. In this case, the overall amount of time before a router/modem is declared lost is expressed as (Interval * Threshold). Specifying an Interval value of 0 indicates the desire to disable Heartbeat messages entirely (e.g., the Interval is set to an infinite value). Setting the Threshold value to 0 is undefined, and TLVs with a Threshold value of 0 MUST be rejected by the recipient.

The Heartbeat Interval/Threshold TLV contains the following fields:



TLV Type - TBD

Length - 1

Interval - 0 = Do NOT use heartbeats on this peer-to-peer session. Non-zero = Interval, in seconds, for heartbeat messages.

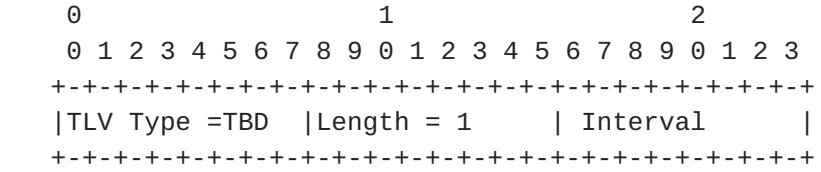
Threshold - Number of windows, of Heartbeat Interval seconds, to wait before declaring a peer-to-peer session to

be lost.

9.18 Link Characteristics ACK Timer

The Link Characteristics ACK Timer TLV is an OPTIONAL TLV. If supported, it MAY be sent during Peer Discovery to indicate the desired number of seconds to wait for a response to a Link Characteristics Request. If a router receives this TLV from a modem during Peer Discovery, the router MUST either accept the timeout value, or reject the Peer Discovery. If this TLV is omitted, implementations supporting the Link Characteristics Request SHOULD choose a default value.

The Link Characteristics ACK Timer TLV contains the following fields:



TLV Type - TBD

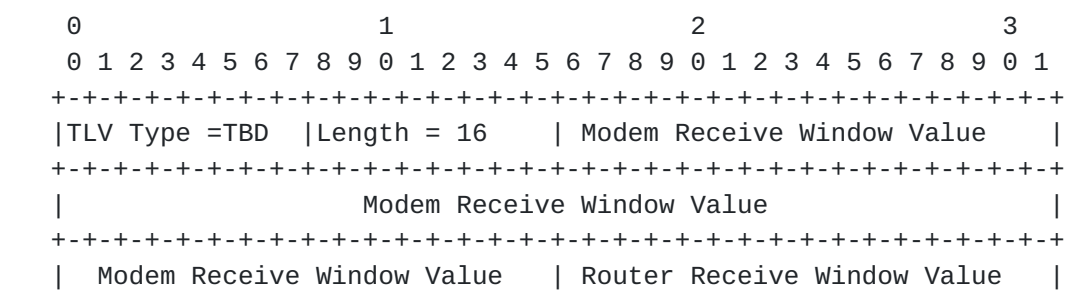
Length - 1

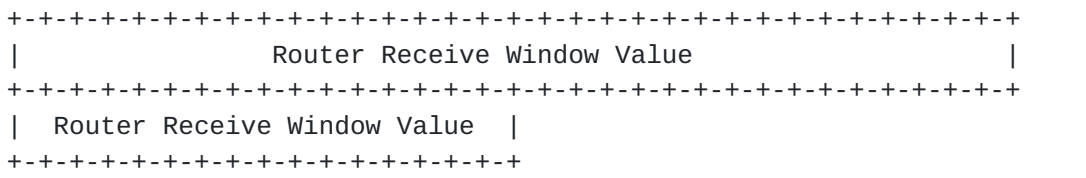
Interval - 0 = Do NOT use timeouts for Link Characteristics requests on this router/modem session. Non-zero = Interval, in seconds, to wait before considering a Link Characteristics Request has been lost.

9.19 Credit Window Status

The Credit Window Status TLV is an OPTIONAL TLV. If credits are supported by the DLEP participants (both the router and the modem), the Credit Window Status TLV MUST be sent by the participant receiving a Credit Grant Request for a given neighbor.

The Credit Window Status TLV contains the following fields:





TLV Type - TBD

Length - 16

Modem Receive Window Value - A 64-bit unsigned number, indicating the current (or initial) number of credits available on the Modem Receive Window.

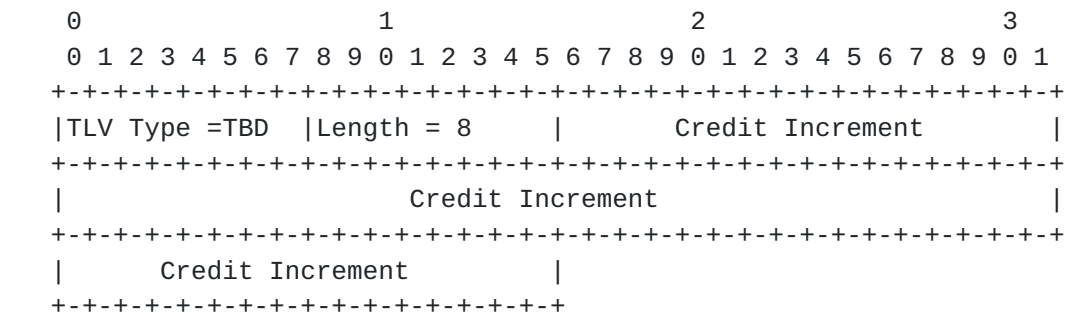
Router Receive Window Value - A 64-bit unsigned number, indicating the current (or initial) number of credits available on the Router Receive Window.

9.20 Credit Grant Request

The Credit Grant Request TLV is an OPTIONAL TLV. If credits are supported, the Credit Grant Request TLV is sent from a DLEP participant to grant an increment to credits on a window. The Credit Grant TLV is sent as a data item in either the Neighbor Up or Neighbor Update messages. The value in a Credit Grant TLV represents an increment to be added to any existing credits available on the window. Upon successful receipt and processing of a Credit Grant TLV, the receiver MUST respond with a message containing a Credit Window Status TLV to report the updated aggregate values for synchronization purposes.

In the Neighbor Up message, when credits are desired, the originating peer MUST set the initial credit value of the window it controls (e.g. the Modem Receive Window, or Router Receive Window) to an initial, non-zero value. If the receiver of a Neighbor Up message with a Credit Grant Request TLV supports credits, the receiver MUST either reject the use of credits, via a Neighbor Up ACK response with the correct Status TLV, or set the initial value from the data contained in the Credit Window Status TLV. If the initialization completes successfully, the receiver MUST respond to the Neighbor Up message with a Neighbor Up ACK message that contains a Credit Window Status TLV, initializing its receive window.

The Credit Grant TLV contains the following fields:



TLV Type - TBD

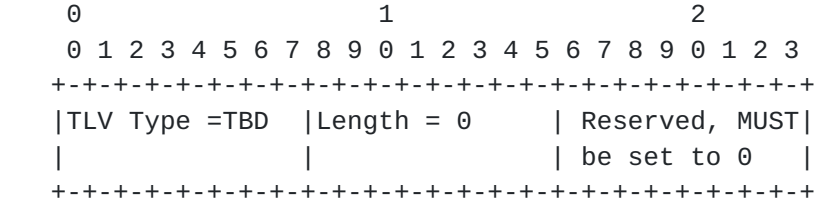
Length - 8

Reserved - A 64-bit unsigned number representing the additional credits to be assigned to the credit window. Since credits can only be granted by the receiver on a window, the applicable credit window (either the MRW or the RRW) is derived from the sender of the grant. The Credit Increment MUST NOT cause the window to overflow; if this condition occurs, implementations MUST set the credit window to the maximum value contained in a 64-bit quantity.

9.21 Credit Request

The Credit Request TLV is an OPTIONAL TLV. If credits are supported, the Credit Request TLV MAY be sent from either DLEP participant, via a Neighbor Update signal, to indicate the desire for the partner to grant additional credits in order for data transfer to proceed on the session. If the corresponding Neighbor Up message for this session did NOT contain a Credit Window Status TLV, indicating that credits are to be used on the session, then the Credit Request TLV MUST be rejected by the receiver via a Neighbor Update ACK message.

The Credit Request TLV contains the following fields:



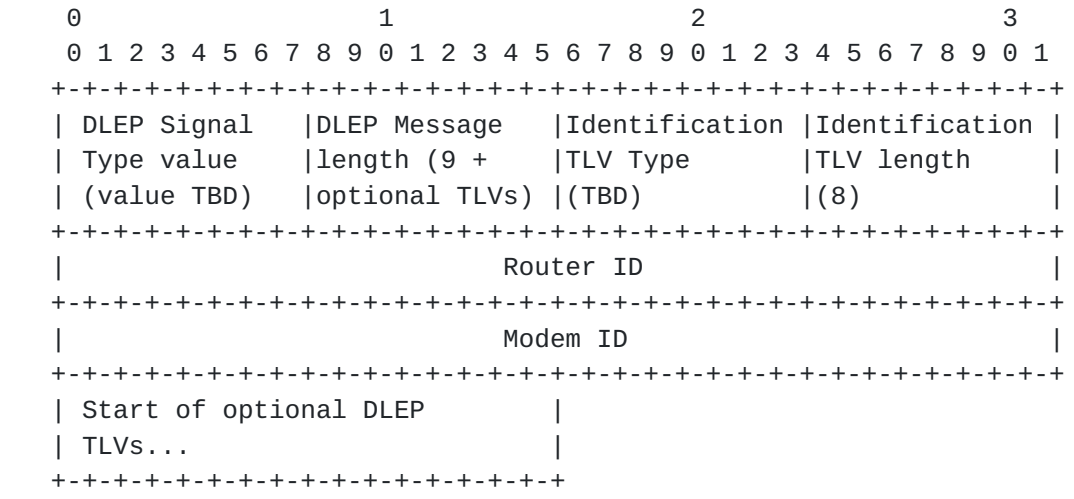
TLV Type - TBD

Length - 0

Reserved - This field is currently unused and MUST be set to 0.

10. DLEP Protocol Messages

DLEP messages are encoded as a string of Type-Length-Value (TLV) constructs. The first TLV in a DLEP message MUST be a valid DLEP signal, as defined in section 11.1 of this document. The second TLV MUST be the Identification data item, defined in section 10.1 Following those two TLVs are 0 or more TLVs, representing the data items that are appropriate for the signal. The layout of a DLEP message is thus:



All DLEP messages (signals) begin with this structure. Therefore, in the following descriptions of specific messages, this header structure is assumed, and will not be replicated.

10.1 Signal TLV Values

As mentioned above, all DLEP messages begin with the Type value of the appropriate DLEP signal. Valid DLEP signals are:

TLV Value	TLV Description
TBD	Peer Discovery
TBD	Peer Offer
TBD	Peer Offer ACK
TBD	Peer Update
TBD	Peer Update ACK

TBD	Peer Termination
TBD	Peer Termination ACK
TBD	Neighbor Up
TBD	Neighbor Up ACK
TBD	Neighbor Down
TBD	Neighbor Down ACK
TBD	Neighbor Update
TBD	Heartbeat
TBD	Link Characteristics Request
TBD	Link Characteristics ACK

11. Peer Discovery Message

The Peer Discovery Message is sent by a modem to begin a new DLEP association. The Peer Offer message is required to complete the discovery process. Implementations MAY implement their own retry heuristics in cases where it is determined the Peer Discovery Message has timed out. A Peer Discovery Message received from a modem that is already in session MUST be processed as if a Peer Termination Message had been received. A router implementation MAY then process the received Peer Discovery Message.

Note that metric data items MAY be supplied with the Peer Discovery, in order to populate default metric values, or to indicate a static, modem-wide environment. If metrics are supplied with the Peer Discovery message, these metrics MUST be used as the initial values for all neighbors (remote nodes) established via the modem.

Given the packet format described in section 11, the initial TLV Type value is set to DLEP_PEER_DISCOVERY (value TBD). OPTIONAL TLVs are then placed into the packet:

Optional Data Item TLVs:

- DLEP Version
- DLEP Peer Type
- Heartbeat Interval
- Heartbeat Threshold
- Link Characteristics ACK Timer
- Maximum Data Rate (Receive)
- Maximum Data Rate (Transmit)
- Current Data Rate (Receive)
- Current Data Rate (Transmit)
- Latency
- Expected Forwarding Time
- Resources (Receive)
- Resources (Transmit)
- Relative Link Quality (Receive)
- Relative Link Quality (Transmit)

12. Peer Offer Message

The Peer Offer Message is sent by a DLEP router in response to a Peer Discovery Message. Upon receipt, and processing, of a Peer Offer message, the modem MUST respond with a Peer Offer ACK message, completing the discovery phase of DLEP. Both DLEP participants (router and modem) would then enter an "in session" state. Any subsequent Discovery messages sent or received on this session MUST be considered an error, and the session MUST be terminated as if a Peer Termination Message had been received.

The Peer Offer message MUST be sent to the unicast address of the originator of Peer Discovery, regardless of whether the discovery was received on the DLEP multicast address (TBD) or on a unicast address.

To construct a Peer Offer message, the initial TLV type value is set to DLEP_PEER_OFFER (value TBD). The signal TLV is then followed by any OPTIONAL Data Item TLVs the implementation supports:

Optional Data Item TLVs:

- DLEP Version
- Peer Type
- IPv4 Address
- IPv6 Address
- Status
- Heartbeat Interval
- Heartbeat Threshold
- Link Characteristics ACK Timer

13. Peer Offer ACK Message

The Peer Offer ACK message acknowledges receipt of a Peer Offer message, and completes the router/modem session establishment for DLEP. The Peer Offer ACK message MUST be sent to unicast address of the originator of a Peer Offer message. The Peer Offer ACK message MUST contain an OPTIONAL Status data item, indicating success or failure of the attempt to establish a router/modem session.

To construct a Peer Offer ACK message, the initial TLV type value is set to DLEP_PEER_OFFER_ACK (value TBD). Mandatory data item TLV's are placed into the packet next:

Mandatory Data Item TLVs:

- Status

Note that there are NO OPTIONAL data item TLVs specified for this

message.

14. Peer Update Message

The Peer Update message is an OPTIONAL message, sent by a DLEP peer to indicate local Layer 3 address changes, or for metric changes on a modem-wide basis. For example, addition of an IPv4 address to the router would prompt a Peer Update message to its attached DLEP modems. Also, a modem that changes its Maximum Data Rate for all destinations MAY reflect that change via a Peer 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 "Neighbor Update" message to their local routers with the new (or deleted) addresses. Modems that do not track Layer 3 addresses SHOULD silently parse and ignore the Peer Update Message. Modems that track Layer 3 addresses MUST acknowledge the Peer Update with a Peer Update ACK message. Routers receiving a Peer Update with metric changes MUST apply the new metric to all neighbors (remote nodes) accessible via the modem. Supporting implementations are free to employ heuristics to retransmit Peer Update messages. The sending of Peer Update Messages for Layer 3 address changes SHOULD cease when a either participant (router or modem) determines that the other implementation does NOT support Layer 3 address tracking.

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

To construct a Peer Update message, the initial TLV type value is set to DLEP_PEER_UPDATE (value TBD). The Signal TLV is followed by any OPTIONAL Data Item TLVs.

Optional Data Item TLVs:

- IPv4 Address
- IPv6 Address
- Maximum Data Rate (Receive)
- Maximum Data Rate (Transmit)
- Current Data Rate (Receive)
- Current Data Rate (Transmit)
- Latency
- Expected Forwarding Time
- Resources (Receive)
- Resources (Transmit)

- Relative Link Quality (Receive)
- Relative Link Quality (Transmit)

15. Peer Update ACK Message

The Peer Update ACK message is an OPTIONAL message, and is sent by implementations supporting Layer 3 address tracking and/or modem-wide metrics to indicate whether a Peer Update Message was successfully processed. If the Peer Update ACK is issued, it MUST contain a Status data item, indicating the success or failure of processing the received Peer Update.

To construct a Peer Update ACK message, the initial TLV type value is set to DLEP_PEER_UPDATE_ACK (value TBD). The Status data item TLV is placed in the packet next, completing the Peer Update ACK.

Optional Data Item TLVs:

- Status

Note that there are NO OPTIONAL data item TLVs specified for this message.

16. Peer Termination Message

The Peer Termination Message is sent by a DLEP participant when the router/modem session needs to be terminated. Implementations receiving a Peer Termination message MUST send a Peer Termination ACK message to confirm the termination process. The sender of a Peer Termination message is free to define its heuristics in event of a timeout. The receiver of a Peer Termination Message MUST release all resources allocated for the router/modem session, and MUST eliminate all neighbors in the information base accessible via the router/modem pair represented by the session. Router and modem state machines are returned to the "discovery" state. No Neighbor Down messages are sent.

To construct a Peer Termination message, the initial TLV type value is set to DLEP_PEER_TERMINATION (value TBD). The Signal TLV is followed by any OPTIONAL Data Item TLVs the implementation supports:

Optional Data Item TLVs:

- Status

17. Peer Termination ACK Message

The Peer Termination Message ACK is sent by a DLEP peer in response

to a received Peer Termination order. Receipt of a Peer Termination ACK message completes the teardown of the router/modem session.

To construct a Peer Termination ACK message, the initial TLV type value is set to DLEP_PEER_TERMINATION_ACK (value TBD). The Identification data item TLV is placed in the packet next, followed by any OPTIONAL TLVs the implementation supports:

Optional Data Item TLVs:

- Status

18. Neighbor Up Message

A DLEP participant sends the Neighbor Up message to report that a new destination has been detected. A Neighbor Up ACK Message is required to confirm a received Neighbor Up. A Neighbor Up message can be sent either by the modem, to indicate that a new remote node has been detected, or by the router, to indicate the presence of a new logical destination (e.g., a Multicast group) exists in the network.

The sender of the Neighbor Up Message is free to define its retry heuristics in event of a timeout. When a Neighbor Up message is received and successfully parsed, the receiver should add knowledge of the new destination to its information base, indicating that the destination is accessible via the modem/router pair.

To construct a Neighbor Up message, the initial TLV type value is set to DLEP_NEIGHBOR_UP (value TBD). The MAC Address data item TLV is placed in the packet next, followed by any supported OPTIONAL Data Item TLVs into the packet:

Optional Data Item TLVs:

- IPv4 Address
- IPv6 Address
- Maximum Data Rate (Receive)
- Maximum Data Rate (Transmit)
- Current Data Rate (Receive)
- Current Data Rate (Transmit)
- Latency
- Expected Forwarding Time
- Resources (Receive)
- Resources (Transmit)
- Relative Link Factor (Receive)
- Relative Link Factor (Transmit)
- Credit Window Status

19. Neighbor Up ACK Message

A DLEP participant sends the Neighbor Up ACK Message to indicate whether a Neighbor Up Message was successfully processed.

To construct a Neighbor Up ACK message, the initial TLV type value is set to DLEP_NEIGHBOR_UP_ACK (value TBD). The MAC Address data item TLV is placed in the packet next, containing the MAC address of the DLEP neighbor. The implementation would then place any supported OPTIONAL Data Item TLVs into the packet:

Optional Data Item TLVs:

- Credit Window Status

20. Neighbor Down Message

A DLEP peer sends the Neighbor Down message to report when a destination (a remote node or a multicast group) is no longer reachable. The Neighbor Down message MUST contain the MAC Address data item TLV. Other TLVs as listed are OPTIONAL, and MAY be present if an implementation supports them. A Neighbor Down ACK Message MUST be sent by the recipient of a Neighbor Down message to confirm that the relevant data has been removed from the information base. The sender of the Neighbor Down message is free to define its retry heuristics in event of a timeout.

To construct a Neighbor Down message, the initial TLV type value is set to DLEP_NEIGHBOR_DOWN (value TBD). The signal TLV is followed by the mandatory MAC Address data item TLV.

Note that there are NO OPTIONAL data item TLVs for this message.

21. Neighbor Down ACK Message

A DLEP participant sends the Neighbor Down ACK Message to indicate whether a received Neighbor Down Message was successfully processed. If successfully processed, the sender of the ACK MUST have removed all entries in the information base that pertain to the referenced neighbor. As with the Neighbor Down message, there are NO OPTIONAL Data Item TLVs defined for the Neighbor Down ACK message.

To construct a Neighbor Down message, the initial TLV type value is set to DLEP_NEIGHBOR_DOWN_ACK (value TBD). The mandatory data item TLVs follow:

- MAC Address Data item
- Status data item

22. Neighbor Update Message

A DLEP participant sends the Neighbor Update message when it detects some change in the information base for a given neighbor (remote node or multicast group). Some examples of changes that would prompt a Neighbor Update message are:

- Change in link metrics (e.g., Data Rates)
- Layer 3 addressing change (for implementations that support it)

To construct a Neighbor Update message, the initial TLV type value is set to DLEP_NEIGHBOR_UPDATE (value TBD). Following the signal TLV are the mandatory Data Item TLVs:

MAC Address data item TLV

After placing the mandatory data item TLV into the packet, the implementation would place any supported OPTIONAL data item TLVs. Possible OPTIONAL data item TLVs are:

- IPv4 Address
- IPv6 Address
- Maximum Data Rate (Receive)
- Maximum Data Rate (Transmit)
- Current Data Rate (Receive)
- Current Data Rate (Transmit)
- Latency
- Resources (Receive)
- Resources (Transmit)
- Relative Link Quality (Receive)
- Relative Link Quality (Transmit)
- Credit Window Status
- Credit Grant
- Credit Request

23. Heartbeat Message

A Heartbeat Message is sent by a DLEP participant every N seconds, where N is defined in the "Heartbeat Interval" field of the discovery message. Note that implementations omitting the Heartbeat Interval effectively set the interval to an infinite value, therefore, in those cases, this message would NOT be sent.

The message is used by participants to detect when a DLEP session partner (either the modem or the router) is no longer communicating. Participants SHOULD allow some integral number of heartbeat intervals

(default 4) to expire with no traffic on the router/modem session before initiating DLEP session termination procedures.

To construct a Heartbeat message, the initial TLV type value is set to DLEP_PEER_HEARTBEAT (value TBD). The signal TLV is followed by the mandatory Heartbeat Interval/Threshold data item.

Note that there are NO OPTIONAL data item TLVs for this message.

24. Link Characteristics Request Message

The Link Characteristics Request Message is an OPTIONAL message, and is sent by the router to request that the modem initiate changes for specific characteristics of the link. Since the request specifies a neighbor, it can reference either a real destination (e.g., a remote node), or a logical destination (e.g., a multicast destination) within the network.

The Link Characteristics Request message contains either a Current Data Rate (CDRR or CDRT) TLV to request a different amount of bandwidth than what is currently allocated, a Latency TLV to request that traffic delay on the link not exceed the specified value, or both. A Link Characteristics ACK Message is required to complete the request. Implementations are free to define their retry heuristics in event of a timeout. Issuing a Link Characteristics Request with ONLY the MAC Address TLV is a mechanism a peer MAY use to request metrics (via the Link Characteristics ACK) from its partner.

To construct a Link Characteristics Request message, the initial TLV type value is set to DLEP_NEIGHBOR_LINK_CHAR_REQ (value TBD). Following the signal TLV is the mandatory Data Item TLV:

MAC Address data item TLV

After placing the mandatory data item TLV into the packet, the implementation would place any supported OPTIONAL data item TLVs. Possible OPTIONAL data item TLVs are:

Current Data Rate - If present, this value represents the NEW (or unchanged, if the request is denied) Current Data Rate in bits per second (bps).

Latency - If present, this value represents the maximum desired latency (e.g., it is a not-to-exceed value) in milliseconds on the link.

25. Link Characteristics ACK Message

The LInk Characteristics ACK message is an OPTIONAL message, and is sent by modems supporting it to the router letting the router know the success or failure of a requested change in link characteristics. The Link Characteristics ACK message SHOULD contain a complete set of metric data item TLVs. It MUST contain the same TLV types as the request. The values in the metric data item TLVs in the Link Characteristics ACK message MUST reflect the link characteristics after the request has been processed.

To construct a Link Characteristics Request ACK message, the initial TLV type value is set to DLEP_NEIGHBOR_LINK_CHAR_ACK (value TBD). Following the signal TLV is the mandatory Data Item TLV:

MAC Address data item TLV

After placing the mandatory data item TLV into the packet, the implementation would place any supported OPTIONAL data item TLVs. Possible OPTIONAL data item TLVs are:

Current Data Rate - If present, this value represents the requested data rate in bits per second (bps).

Latency - If present, this value represents the NEW maximum latency (or unchanged, if the request is denied), expressed in milliseconds, on the link.

26. Security Considerations

The protocol does not contain any mechanisms for security (e.g. authentication or encryption). The protocol assumes that any security would be implemented in the underlying transport (for example, by use of DTLS or some other mechanism), and is therefore outside the scope of this document.

27. IANA Considerations

This section specifies requests to IANA.

27.1 Registrations

This specification defines:

o A new repository for DLEP signals, with fifteen values currently assigned.

o Reservation of numbering space for Experimental DLEP signals.

- A new repository for DLEP Data Items, with twenty-one values currently assigned.

- Reservation of numbering space in the Data Items repository for experimental data items.

- A request for allocation of a well-known port for DLEP communication.

- A request for allocation of a multicast address for DLEP discovery.

27.2 Expert Review: Evaluation Guidelines

No additional guidelines for expert review are anticipated.

27.3 Signal (Message) TLV Type Registration

A new repository must be created with the values of the DLEP signals. Valid signals are:

- Peer Discovery
- Peer Offer
- Peer Offer ACK
- Peer Update
- Peer Update ACK
- Peer Termination
- Peer Termination ACK
- Neighbor Up
- Neighbor Up ACK
- Neighbor Down
- Neighbor Down ACK
- Neighbor Update
- Heartbeat
- Link Characteristics Request
- Link Characteristics ACK

It is also requested that the repository contain space for experimental signal types.

27.4 DLEP Data Item Registrations

A new repository for DLEP Data Items must be created. Valid Data Items are:

- DLEP Version
- Peer Type
- MAC Address
- IPv4 Address
- IPv6 Address
- Maximum Data Rate (Receive)
- Maximum Data Rate (Transmit)
- Current Data Rate (Receive)
- Current Data Rate (Transmit)
- Latency
- Expected Forwarding Time
- Resources (Receive)
- Resources (Transmit)
- Relative Link Quality (Receive)
- Relative Link Quality (Transmit)
- Status
- Heartbeat Interval/Threshold
- Link Characteristics ACK Timer
- Credit Window Status
- Credit Grant
- Credit Request

It is also requested that the registry allocation contain space for experimental data items.

27.5 DLEP Well-known Port

It is requested that IANA allocate a well-known port number for DLEP communication.

27.6 DLEP Multicast Address

It is requested that IANA allocate a multicast address for DLEP discovery messages.

30. Appendix A.

30.1 Peer Level Message Flows

30.1.1 Modem Device Restarts Discovery

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

<-------Peer Discovery---------    Modem initiates discovery
```

```
    ---------Peer Offer----------->   Router detects a problem, sends
      w/ Non-zero Status TLV          Peer Offer w/Status TLV indicating
                                      the error.

                                      Modem accepts failure, restarts
                                      discovery process.

   <-------Peer Discovery---------    Modem initiates discovery


    ---------Peer Offer----------->   Router accepts, sends Peer Offer
         w/ Zero Status TLV           w/ Status TLV indicating success.

                                      Discovery completed.
```

30.1.2 Modem Device Detects Peer Offer Timeout

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

   <-------Peer Discovery---------    Modem initiates discovery, starts
                                      a guard timer.

                                      Modem guard timer expires. Modem
                                      restarts discovery process.

    <-------Peer Discovery---------   Modem initiates discovery, starts
                                      a guard timer.

    ---------Peer Offer----------->   Router accepts, sends Peer Offer
         w/ Zero Status TLV           w/ Status TLV indicating success.

                                      Discovery completed.
```

30.1.3 Router Peer Offer Lost

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

<-------Peer Discovery---------    Modem initiates discovery, starts
                                   a guard timer.

 ---------Peer Offer-------||      Router offers availability

                                   Modem times out on Peer Offer,
                                   restarts discovery process.

<-------Peer Discovery---------    Modem initiates discovery

 ---------Peer Offer----------->   Router detects subsequent
                                   discovery, internally terminates
                                   the previous, accepts the new
                                   association, sends Peer Offer
                                   w/Status TLV indicating success.


                                   Discovery completed.
```

30.1.4 Discovery Success

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

<-------Peer Discovery---------    Modem initiates discovery

 ---------Peer Offer----------->   Router offers availability

 -------Peer Heartbeat--------->

<-------Peer Heartbeat---------

 -------Peer Heartbeat--------->

<============================>    Neighbor Sessions

<-------Peer Heartbeat---------

 -------Peer Heartbeat--------->

 --------Peer Term Req--------->   Terminate Request
```

```
   <--------Peer Term Res---------    Terminate Response
```

30.1.5 Router Detects a Heartbeat timeout

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

   <-------Peer Heartbeat---------

    -------Peer Heartbeat--------->

      ||---Peer Heartbeat---------

           ~ ~ ~ ~ ~ ~ ~

    -------Peer Heartbeat--------->

      ||---Peer Heartbeat---------
                                     Router Heartbeat Timer expires,
                                     detects missing heartbeats. Router
                                     takes down all neighbor sessions
                                     and terminates the Peer
                                     association.

    ------Peer Terminate ---------->  Peer Terminate Request

                                     Modem takes down all neighbor
                                     sessions, then acknowledges the
                                     Peer Terminate

   <----Peer Terminate ACK---------   Peer Terminate ACK
```

30.1.6 Modem Detects a Heartbeat timeout

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

   <-------Peer Heartbeat---------

    -------Peer Heartbeat------||

   <-------Peer Heartbeat---------

           ~ ~ ~ ~ ~ ~ ~

    -------Peer Heartbeat------||

   <-------Peer Heartbeat---------
```

```
                                    Modem Heartbeat Timer expires,
                                    detects missing heartbeats. Modem
                                    takes down all neighbor sessions

    <-------Peer Terminate--------    Peer Terminate Request

                                    Router takes down all neighbor
                                    sessions, then acknowledges the
                                    Peer Terminate

    ------Peer Terminate ACK----->    Peer Terminate ACK
```

30.1.7 Peer Terminate (from Modem) Lost

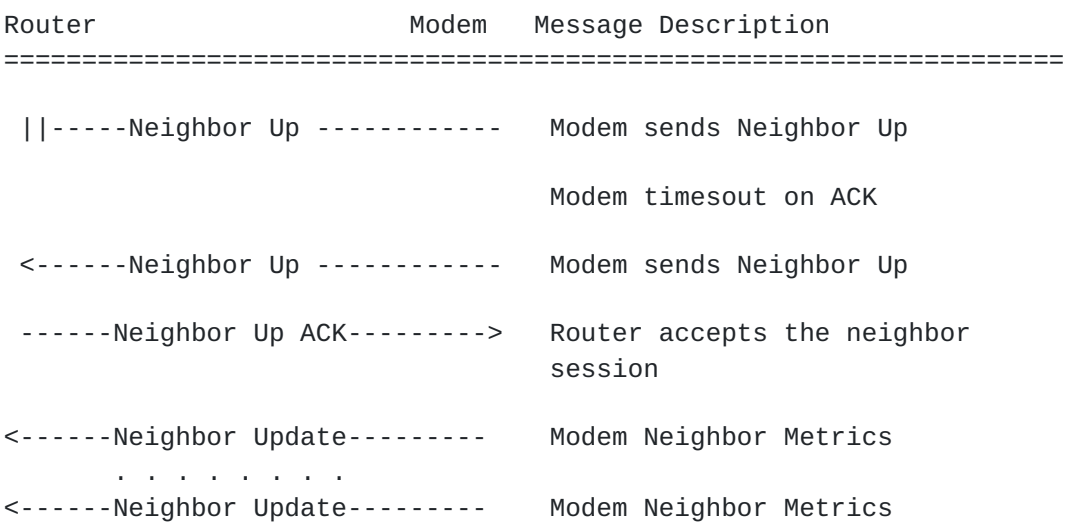
```
   Router                    Modem   Message Description
   ================================================================

     ||------Peer Terminate--------   Modem Peer Terminate Request

                                    Router Heartbeat times out,
                                    terminates association.

    --------Peer Terminate------->    Router Peer Terminate

    <-----Peer Terminate ACK------    Modem sends Peer Terminate ACK
```

30.1.8 Peer Terminate (from Router) Lost

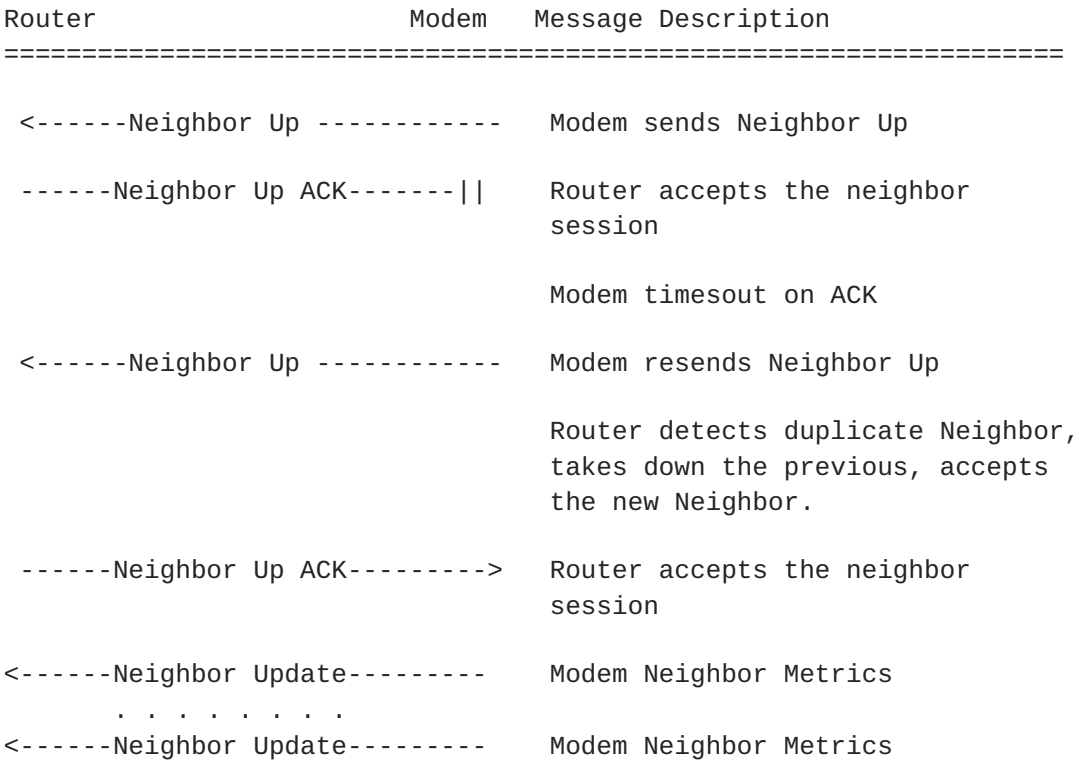
```
   Router                    Modem   Message Description
   ================================================================

    -------Peer Terminate-------->    Router Peer Terminate Request

                                    Modem HB times out,
                                    terminates association.

    <------Peer Terminate--------     Modem Peer Terminate

    ------Peer Terminate ACK----->    Peer Terminate ACK
```

30.2 Neighbor Specific Message Flows

30.2.1 Modem Neighbor Up Lost



30.2.2 Router Detects Duplicate Neighbor Ups



30.2.3 Neighbor Up, No Layer 3 Addresses

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

 <------Neighbor Up ------------   Modem sends Neighbor Up

 ------Neighbor Up ACK--------->   Router accepts the neighbor
                                   session

                                   Router ARPs for IPv4 if defined.
                                   Router drives ND for IPv6 if
                                   defined.

<------Neighbor Update---------    Modem Neighbor Metrics
       . . . . . . . .
<------Neighbor Update---------    Modem Neighbor Metrics
```

30.2.4 Neighbor Up with IPv4, No IPv6

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

 <------Neighbor Up ------------   Modem sends Neighbor Up with
                                   the IPv4 TLV

 ------Neighbor Up ACK--------->   Router accepts the neighbor
                                   session

                                   Router drives ND for IPv6 if
                                   defined.

<------Neighbor Update---------    Modem Neighbor Metrics
       . . . . . . . .
<------Neighbor Update---------    Modem Neighbor Metrics
```

30.2.5 Neighbor Up with IPv4 and IPv6

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

 <------Neighbor Up ------------   Modem sends Neighbor Up with
                                   the IPv4 and IPv6 TLVs

 ------Neighbor Up ACK--------->   Router accepts the neighbor
                                   session
```

```
   <------Neighbor Update---------    Modem Neighbor Metrics
          . . . . . . . . .
```

30.2.6 Neighbor Session Success

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


    ---------Peer Offer----------->   Router offers availability

    -------Peer Heartbeat--------->


   <------Neighbor Up -----------      Modem

    ------Neighbor Up ACK-------->     Router

   <------Neighbor Update---------     Modem
          . . . . . . . . .
   <------Neighbor Update---------     Modem

                                       Modem initiates the terminate

   <------Neighbor Down ----------     Modem

    ------Neighbor Down ACK------->    Router

                                       or

                                       Router initiates the terminate

    ------Neighbor Down ---------->    Router

   <------Neighbor Down ACK-------     Modem
```

Acknowledgements

The authors would like to acknowledge the influence and contributions of Chris Olsen, Teco Boot, Subir Das, Jaewon Kang, Vikram Kaul, Rick Taylor, John Dowdell, Nelson Powell, Bow-Nan Cheng, and Henning Rogge.

Normative References

[RFC5578] Berry, B., Ed., "PPPoE with Credit Flow and Metrics",

RFC 5578, February 2010.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

Informative References

[DTLS] Rescorla, E., Ed,. "Datagram Transport Layer Security", RFC 4347, April 2006.

Author's Addresses

Stan Ratliff
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA
EMail: sratliff@cisco.com

Bo Berry
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA
EMail: boberry@cisco.com

Greg Harrison
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA
EMail: greharri@cisco.com

Shawn Jury
NetApp
7301 Kit Creek Road, Building 2
Research Triangle Park, NC 27709
USA
Email: shawn.jury@netapp.com

Darryl Satterwhite
Broadcom
USA
Email: dsatterw@broadcom.com