Independent Submission
Request for Comments: 6812
Category: Informational
ISSN: 2070-1721

M. Chiba
A. Clemm
S. Medley
J. Salowey
S. Thombare
E. Yedavalli
Cisco Systems
January 2013

Cisco Service-Level Assurance Protocol

Abstract

Cisco's Service-Level Assurance Protocol (Cisco's SLA Protocol) is a Performance Measurement protocol that has been widely deployed. The protocol is used to measure service-level parameters such as network latency, delay variation, and packet/frame loss. This document describes the Cisco SLA Protocol Measurement-Type UDP-Measurement, to enable vendor interoperability.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6812.

Table of Contents

1. Introduction

Active network performance measurements are becoming critical data points for administrators monitoring the health of the network. As service providers look to differentiate their offerings, performance measurement is increasingly becoming an important tool to monitor service-level guarantees and, in general, to monitor the health of a network.

Performance metrics, both one-way and two-way, can be used for pre-deployment validation as well as for measuring in-band live network-performance characteristics. It can be used to measure service levels in L2 and L3 networks as well as for applications running on top of L3. Active performance measurements are gathered by analyzing synthetically generated request and response packets or frames. This is in contrast to passive measurements that analyze live traffic flowing through a particular network element.

There is a growing body of work on Performance Measurement standards that enable interoperability between different vendors' network elements by describing common measurement protocols as well as metrics. The IETF has actively developed Standards Track documents on the subject, such as "A One-way Active Measurement Protocol (OWAMP)" [RFC4656] and "Two-Way Active Measurement Protocol (TWAMP)" [RFC5357].

Cisco's SLA Protocol is another example of a Performance Measurement protocol that offers a rich set of measurement message types. The measurement types can be classified as those that test connectivity (ping like) by providing round-trip or one-way latency measures, and those that provide a richer set of statistics including network jitter and packet or frame loss. Each type of active measurement exchange mimics an actual protocol exchange.

Cisco's SLA Protocol UDP-Measurement message exchanges, as covered in this document to enable interoperability, simulate a UDP application and can be used to simulate either Voice or Video traffic that is encoded in RTP frames within UDP envelopes. The Measurement-Type UDP-Measurement message exchanges carry information that provide the ability to derive a robust set of statistics.

2. Terminology

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 RFC 2119 [RFC2119].

Term	Description
Control Phase	A phase during which a Control-Request and Control-Response are exchanged.
L2	OSI Data-Link Layer
L3	OSI Network Layer
Measurement Phase	Active Measurement Phase that is marked by a sequence of Measurement-Request and Measurement-Response exchanges.
Metric	A particular characteristic of the network data traffic, for example, latency, jitter, packet or frame loss.
Responder	A network element that responds to a message.
RTP	Real-time Transport Protocol
Sender	A network element that is the initiator of a message exchange.
Service-Level	This is the level of service that is agreed upon between the Provider and the Customer.
UDP	User Datagram Protocol

3. Protocol

The Cisco SLA Protocol consists of two distinct phases: the Control Phase and the Measurement Phase. Each phase is comprised of information exchanged between a network element acting as the Sender and an element designated as the Responder.

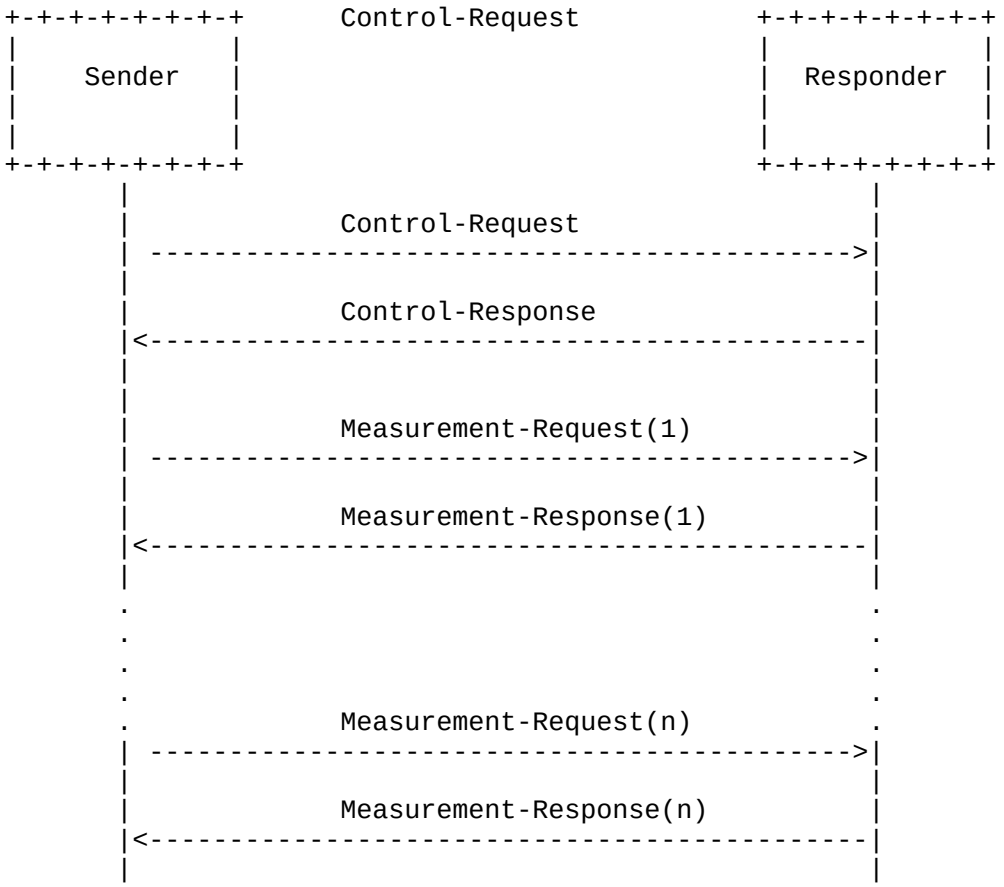
The Control Phase is the first phase of message exchanges and forms the base protocol. This phase establishes the identity of the Sender and provides information for the Measurement Phase. A single message pair of Control-Request and Control-Response marks this phase. The

Sender initiates a Control-Request message that is acknowledged by the Responder with a Control-Response message. The Control-Request may be sent multiple times if a Control-Response has not been received; the number of times the message is retried is configurable on the Sender element.

The Measurement Phase forms the second phase and is comprised of a sequence of Measurement-Request and Measurement-Response messages. These messages may be exchanged as often as required. Each Measurement-Request message is acknowledged by the Responder with a Measurement-Response message.

The number and frequency with which messages are sent SHOULD be controlled by configuration on the Sender element, along with the waiting time for a Control-Response.

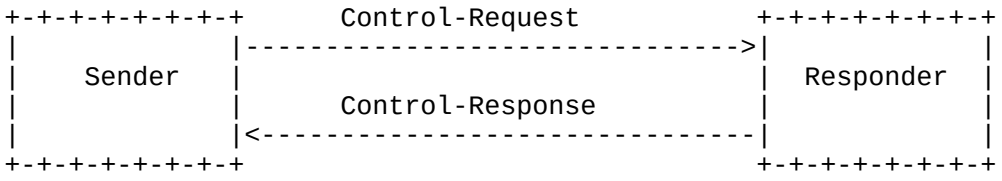
The following sequence diagram depicts the message exchanges:



3.1. Control Phase

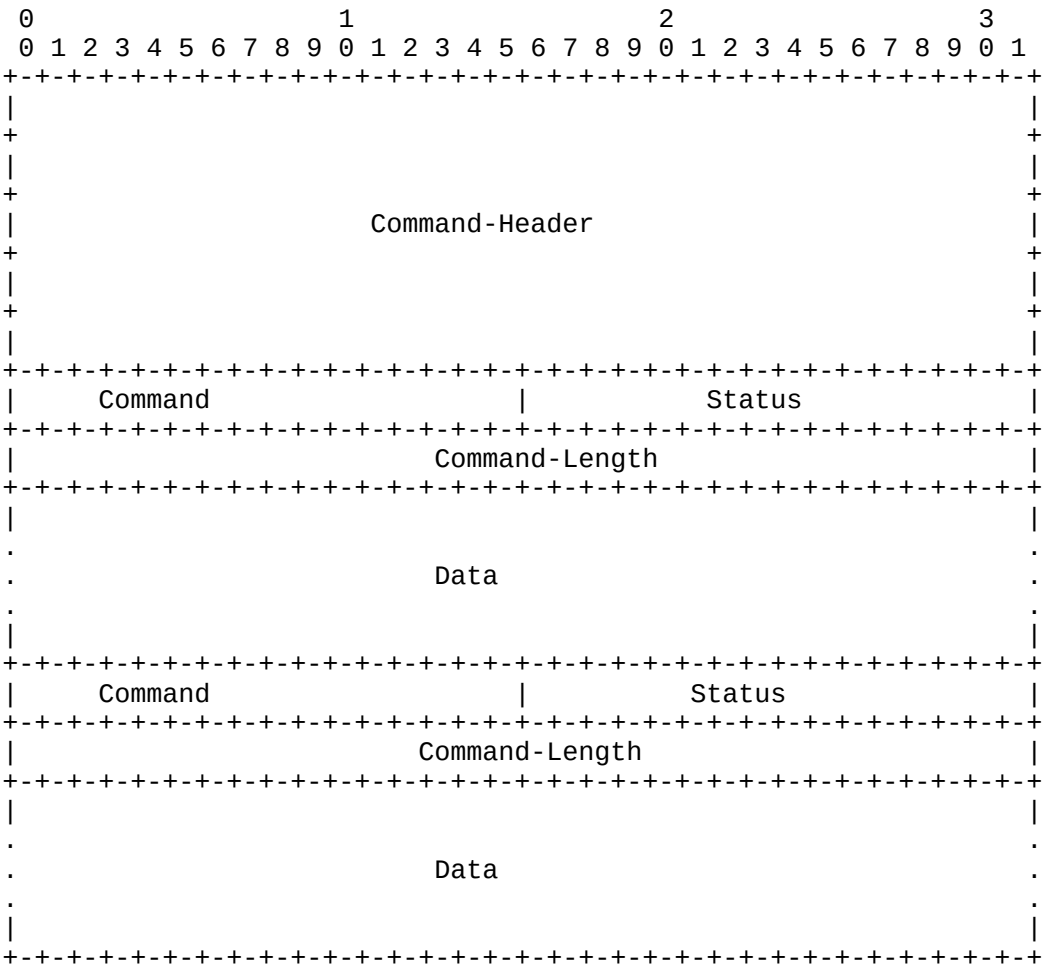
The Control Phase begins with the Sender sending a Control-Request message to the Responder. The Control-Request message is sent to UDP port 1167 on the Responder requesting that a Measurement Phase UDP port be opened and, in addition, indicates the duration for which the port needs to remain open. The Responder replies by sending a Control-Response with an appropriate Status indicating Success when the Sender identity is verified and the requested UDP port was successfully opened. In all other cases, a non-zero Status is returned in the Command-Header Status field.

The sequence of exchanges is as indicated in the following diagram:



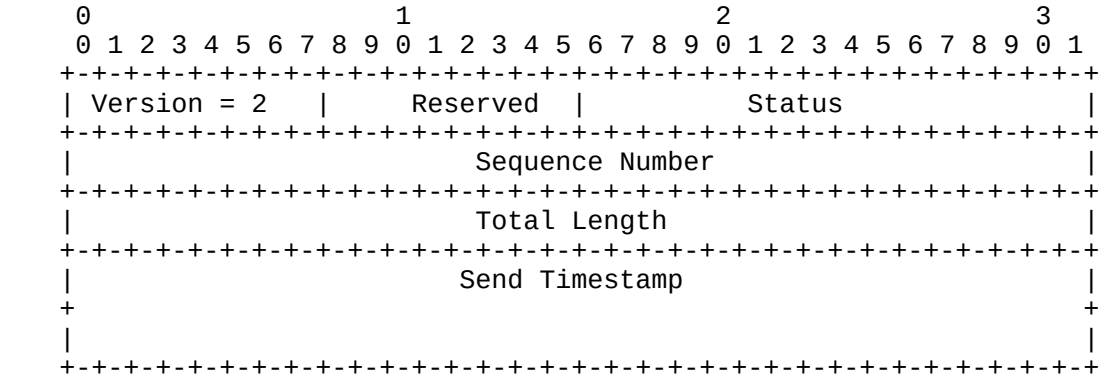
3.1.1. Control-Request Message

The Control-Request message consists of a Command-Header followed by one or more Command, Status, Length and Data sections (henceforth known as CSLD). At a minimum, there SHOULD be two CSLD sections, one of which is the authentication CSLD section and the other carries information for the Measurement Phase simulation type.



3.1.1.1. Command-Header

The Command-Header is the first section of the Control-Request message and is depicted below:



The Command-Header fields hold the following meaning:

Field	Size (bits)	Description
Version	8	Current version supported and is to be set to 2.
Reserved	8	Reserved field, MUST be set to 0.
Status	16	Indicates success or failure for the entire message. In a Control-Request, the value of the Status field is ignored by the receiver and SHOULD be set to 0.
Sequence Number	32	Used to map requests to responses. This is a monotonically increasing number. Implementations MAY reset the sequence number to 0 after a reboot, and it SHOULD wrap around after all bits have been exceeded.
Total Length	32	Carries the total length of the Control message in number of octets.

| --------- | --------- | -------------------------- |
| Send Timestamp | 64 | This field is set to the time the command was submitted for transmission and is updated for a response. This field MAY be used when security is of concern in order to prevent replay attacks. SHOULD be updated when the response is sent. When not being used, it MUST be set to all 0's. The format is as given in RFC 5905. |

The Sequence Number field MUST include a new number for each new request and is monotonically increasing. When the Control-Request is to be retried, the sequence number MUST remain unchanged.

3.1.1.2. CSLDs

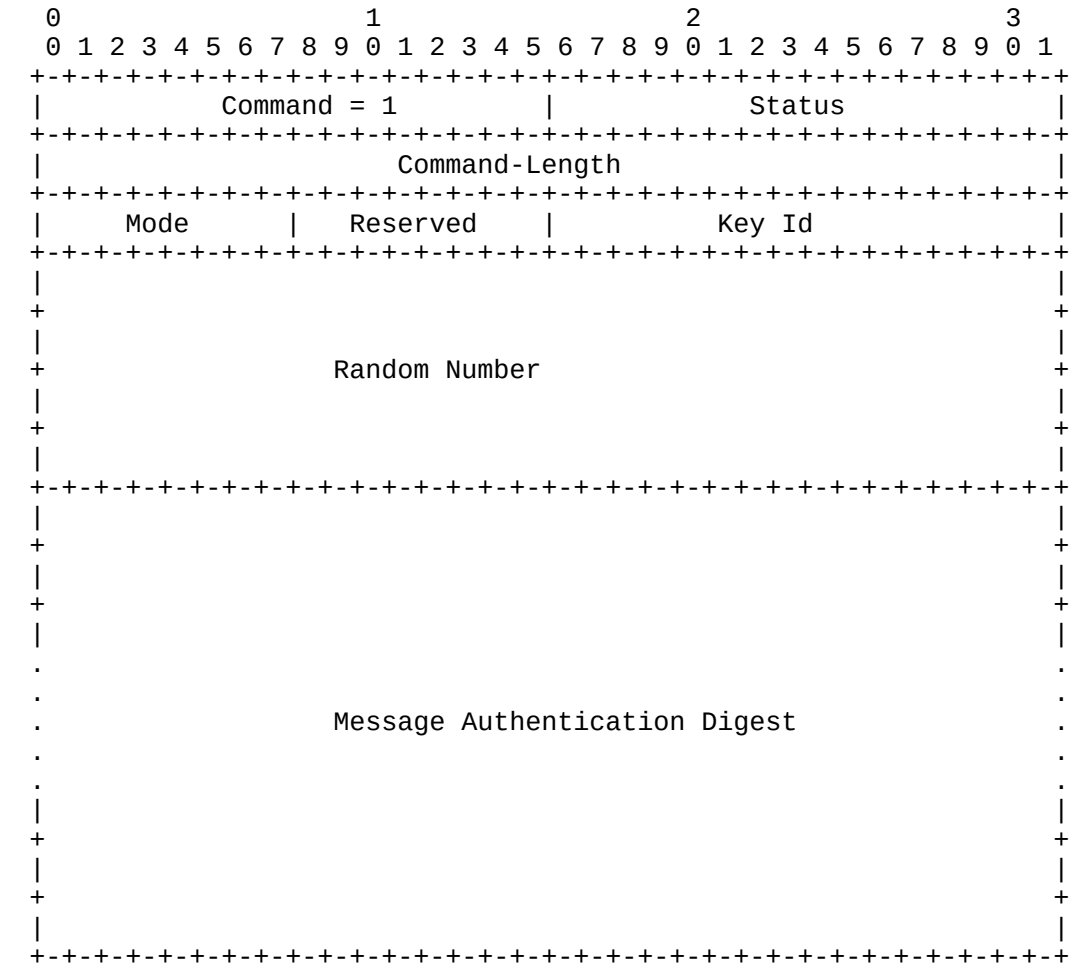
The ordered list of the two CSLDs to be included along with the Command-Header are:

- The Authentication CSLD
- A Measurement-Type CSLD

In this revision of the protocol, only a single Measurement-Type CSLD has been defined, the UDP-Measurement CSLD. For future extensions, it is possible to add more Measurement-Type CSLDs. For more details, see Section 5 on extensions.

3.1.1.2.1. Authentication CSLD

The Authentication CSLD provides message authentication and verifies that the requester knows the shared secret. The following is the format for the Authentication CSLD:

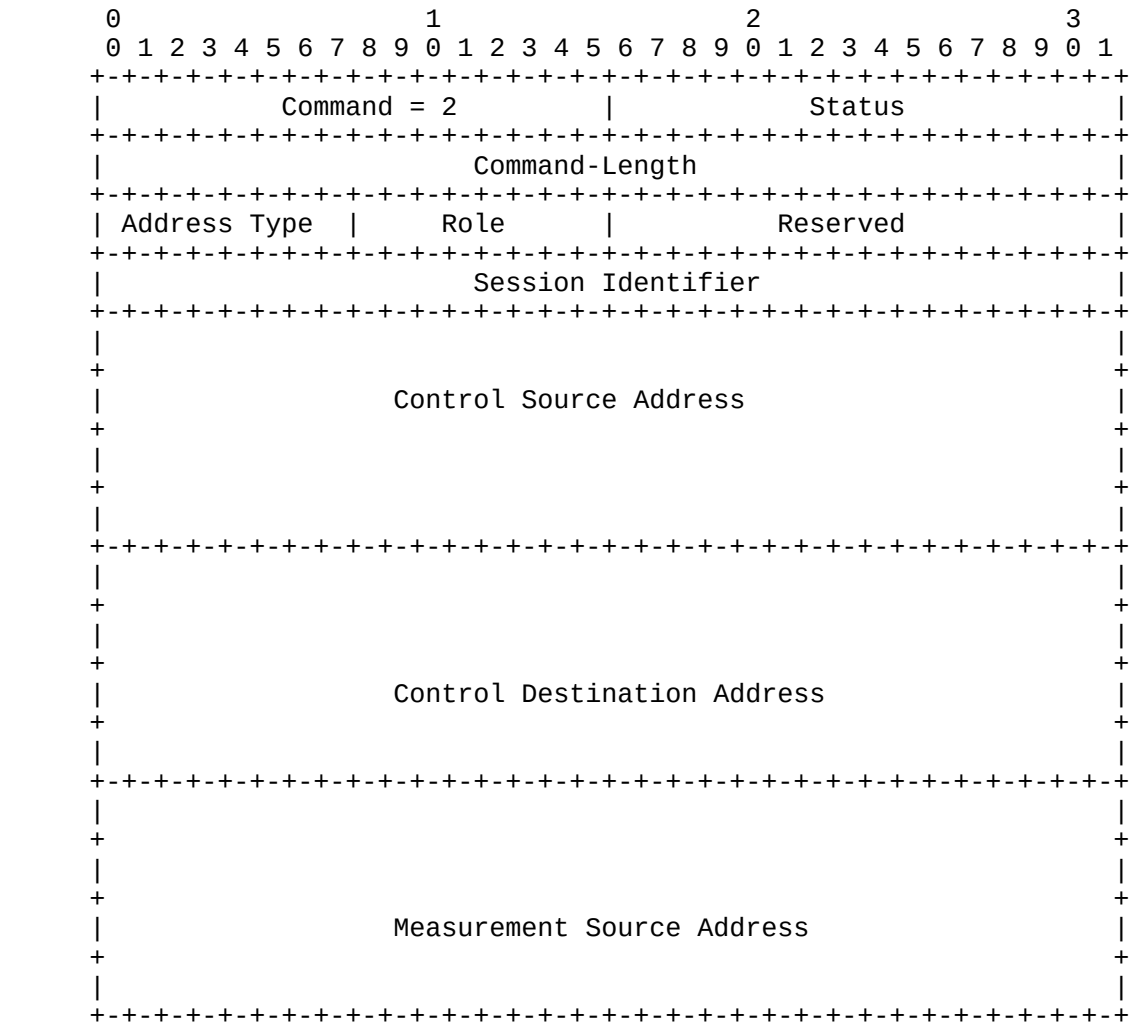


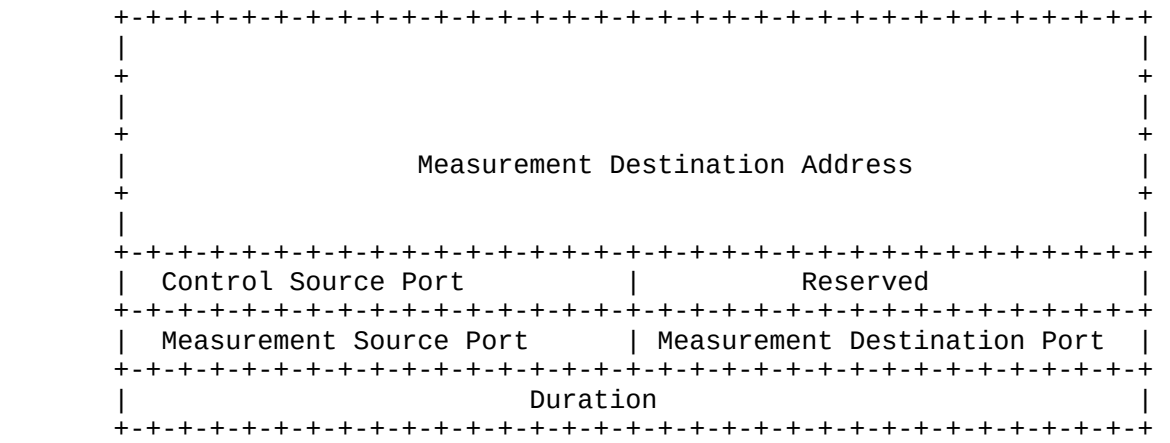
The fields for the Authentication CSLD have the following meaning:

Field	Size (bits)	Description
Command	16	Indicates the CSLD is of type Authentication.
Status	16	Not used for a request and MUST be set to 0.
Command-Length	32	Indicates the length of the CSLD in octets.
Mode	8	Indicates the type of authentication being used and is set as follows: 0 - No Authentication, 1 - SHA256 Authentication, 2 - HMAC-SHA-256
Reserved	8	This field is reserved for future extensions and MUST be set to 0.
Key ID	16	Indicates the index number of the shared secret to be used for authenticating the Control-Request message.
Random Number	128	This field is to be unique over the shared-secret life and is used to make it difficult to predict the shared secret via multiple packet captures. The value is reflected in a response message. This field MAY be used when security is of concern and is useful to prevent dictionary attacks. When not being used, it should be set to all 0's
Message Authentication Digest	256	Contains the message authentication digest and is computed over the entire control packet, including this field set to all 0s.

3.1.1.2.2. UDP-Measurement CSLD

The UDP-Measurement CSLD indicates the Measurement-Type to be used during the Measurement Phase and specifies the addresses and UDP port to be opened as well as the duration that the port has to be kept open for the Measurement Phase. The format of the CSLD is as follows:





Note: Duration is specified in milliseconds.

The fields in the UDP-Measurement CSLD have the following meaning:

Field	Size (bits)	Description
Command	16	Indicates that the CSLD is to simulate UDP traffic measurements.
Status	16	Not used for a request and MUST be set to 0.
Command-Length	32	Indicates the length of the CSLD in octets.
Address Type	8	Indicates the address type and is set to one of the values in the "Cisco SLA Protocol Address Family Registry": 2 - IPv4 addresses, 3 - IPv6 addresses.
Role	8	Indicates the role of the endpoint receiving the Control message and is set as follows: 1 - Responder.
Reserved	16	Reserved and MUST be set to 0.

Session Identifier	32	Carries a session identifier that is a locally significant unique value to the originator of the message. MUST be 0 when not specified.
Control Source Address	128	Set to the address from which the Sender initiates Control messages. For IPv4 addresses, only the first 32 bits are filled and the remaining bits MUST be set to 0.
Control Destination Address	128	Set to the address on the Responder where the Control message will be sent. For IPv4 addresses, only the first 32 bits are filled and the remaining bits MUST be set to 0.
Measurement Source Address	128	Set to the address of the Sender from where the measurement packets will originate. For IPv4 addresses, only the first 32 bits are filled and the remaining bits MUST be set to 0.
Measurement Destination Address	128	Set to the address on the Responder towards which the measurement packets will be sent and is a way to identify an ingress interface on the Responder. For IPv4 addresses, only the first 32 bits are filled and the remaining bits MUST be set to 0.
Control Source Port	16	Indicates the port on the Sender from which the Control message is sent. If not set, the value should be derived from the incoming packet.
Reserved	16	Reserved Field, MUST be set to 0.
Measurement Source Port	16	Indicates the UDP Port on the Sender from which the measurement packets will be sent.
Measurement Destination Port	16	Indicates the UDP Port on the Responder towards which the measurement packets will be sent.

| --- | --- | --- |
| Duration | 32 | This is the duration in milliseconds that the port needs to be kept open for accepting Measurement Phase messages. Measurement messages received after the duration MUST be ignored. |

Note: The source addresses are only indicative of identity of the originator and cannot be used as a destination address for responses in a NAT environment.

3.1.2. Control-Response Message

In response to the Control-Request message, the network element designated the Responder sends back a Control-Response message that reflects the Command-Header with an updated Status field and includes the two CSLD sections that also carry updated Status fields. Hence, the format is identical to the Control-Request message as described above.

The following table shows the supported values of the Status fields:

Status Value	Description
0	Success
1	Fail - catch all
2	Authentication Failure
3	Format error - sent when any CSLD type is not recognized or any part of a CSLD has a value that is not recognized
4	Port in use - the UDP/TCP port is already being used by some other application and cannot be reserved
5+	Future extension and experimental values; refer to the "Cisco SLA Protocol Status Types Registry" in the Considerations section (Section 6).

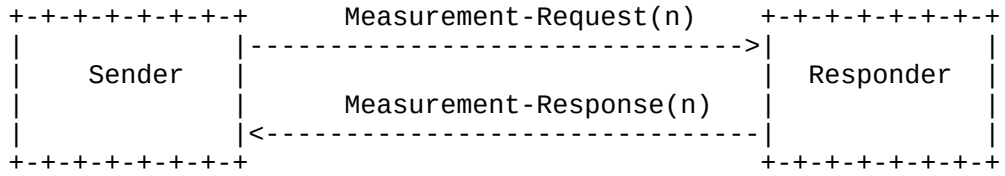
The Status field values are applicable to both Command-Header and CSLD sections. In a Command-Header, the Status field indicates Success only if all the CSLD sections have their Status set to

Success. The Command-Header Status field is set to non-zero otherwise. The Status field in a Command-Header SHOULD only make use of status values 0 through 3, whereas CSLDs can also make use of other status values as applicable. Future extensions MAY extend these values as appropriate.

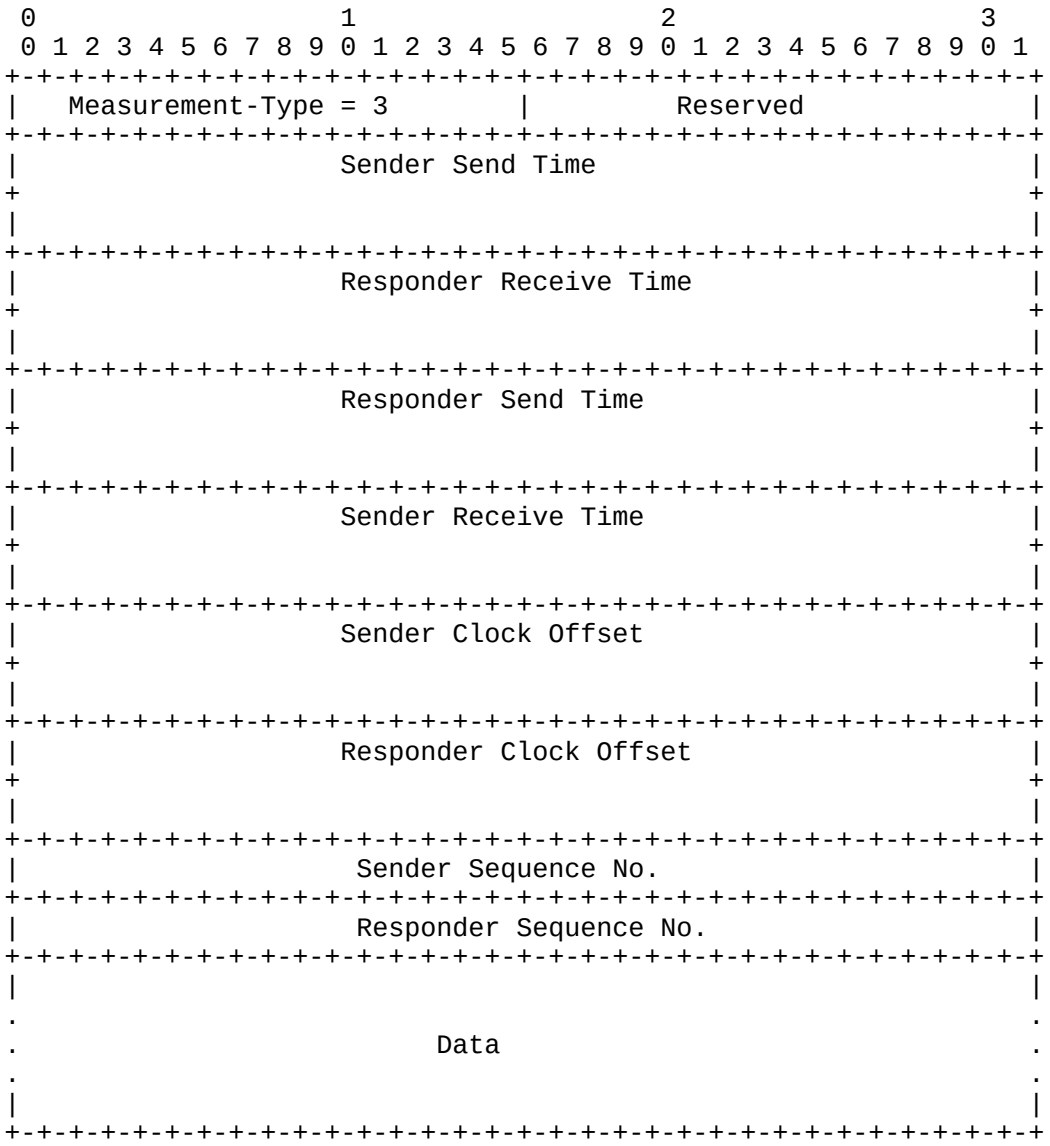
The Control-Response message, aside from updating the Status fields, SHOULD also update the Sent Timestamp (if used) in the Command-Header and the Message Authentication Digest in the Authentication CSLD. The Message Authentication Digest is computed in the same way as the Control-Request message. The Random Number field MUST be reflected without modification. The Session Identifier MAY be updated to reflect a locally significant unique value; it MUST be 0 if not specified.

3.2. Measurement Phase

Upon receiving the Control-Response message with the Status set to Success, the second phase of the protocol, the Measurement Phase, is initiated. In all other cases when the Status is not set to Success, no measurement traffic is initiated. In the Measurement Phase, the Sender sends a stream of measurement messages. The measurement message stream consists of packets or frames that are spaced a configured number of milliseconds apart.



The format of the measurement messages as defined by this document for UDP-Measurements is as shown below and is the same for the exchange in both directions. That is, the format is the same when sent from the Sender to the Responder and when sent back from the Responder to the Sender with the only difference being the update of those fields that are designated with the Responder prefix; all other fields MUST remain unchanged.


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
Measurement-Type = 3
Reserved
Sender Send Time
Responder Receive Time
Responder Send Time
Sender Receive Time
Sender Clock Offset
Responder Clock Offset
Sender Sequence No.
Responder Sequence No.
Data

The fields for the UDP-Measurement Measurement-Request have the following meaning:

Field	Size (bits)	Description
Measurement-Type	16	Carries the type of measurement being performed; 1 - Reserved, 2 - Reserved, 3 - UDP-Measurement
Reserved	16	Reserved field and MUST be set to 0.
Sender Send Time	64	Carries the timestamp when the measurement message was submitted for transmission by the Sender.
Responder Receive Time	64	Carries the timestamp when the measurement message was received by the Responder.
Responder Send Time	64	Carries the timestamp when the measurement message was submitted for transmission by the Responder. It MUST be 0 in the Sender-to-Responder direction.
Sender Receive Time	64	Carries the timestamp when the Sender received the measurement message. It MUST be 0 in both directions on the wire and is filled on the Sender side as soon as the measurement message is received.
Sender Clock Offset	64	Gives an estimate of the Sender clock skew measured in seconds and fractional seconds.
Responder Clock Offset	64	Gives an estimate of the Responder clock skew measured in seconds and fractional seconds.
Sender Sequence Number	32	The sequence number of the measurement message on the Sender side. This field is monotonically increasing and MAY wrap around.

Responder Sequence Number	32	The sequence number of the measurement message on the Responder side. This field is monotonically increasing and MAY wrap around.
Data	32 bit aligned	This field is used to pad up to the configured request data size. The minimum size for this field SHOULD be 64 octets.

Note: All timestamps have the default format as described in RFC 5905 [RFC5905] and is as follows: the first 32 bits represent the unsigned integer number of seconds elapsed since 0 h on 1 January 1900; the next 32 bits represent the fractional part of a second thereof. The timestamp definition is also similar to that described in RFC 4656 [RFC4656].

In addition, the timestamp format used can be as described for the low-order 64 bits of the IEEE 1588-2008 (1588v2) Precision Time Protocol timestamp format [IEEE1588]. This truncated format consists of a 32-bit seconds field followed by a 32-bit nanoseconds field, and is the same as the IEEE 1588v1 timestamp format. This timestamp definition is similar to the default timestamp specified in RFC 6374 [RFC6374]

Implementations MUST use only one of the two formats. The chosen format is negotiated out-of-band between the endpoints or defaults to the format as defined in RFC 5905. [RFC5905]

4. Implementation Notes

Responder implementations SHOULD support simultaneous measurements destined to a single port either from the same or a different Sender. For different measurement instances that originate from the same Sender, there MUST be a clear method for the Responder to distinguish the traffic, for example, per a unique 5-tuple of protocol, source address, source port, destination address, and destination port.

A Control-Request that is received for the same Measurement-Type request as identified by the 5-tuples, for instance, SHOULD result in the resetting of the duration timer as well as the Responder sequence number.

A Control Phase followed by the Measurement Phase can be repeated in order to have a continuous measurement over the entire lifetime of a device.

The Authentication CSLD MUST always be included. The Random Number field is used to prevent dictionary attacks and is to be set to a random value in environments where security is a concern.

An implementation MUST include the Random Number and Message Authentication fields when the mode is non-zero. The fields MAY be included when the mode is set to 'No Authentication'; when present, they MUST be set to 0. For the SHA256 authenticator mode, the shared secret is prepended to the Control message and the authentication algorithm is then run over the complete data including the shared secret. The SHA256 mode is included for ease of implementation, and use of the HMAC variant is strongly recommended for stronger security.

If the UDP port indicated in the UDP-Measurement CSLD is busy, the Responder MAY suggest an alternative port, in which case the Status of the UDP-Measurement CSLD MUST be set to Success. The Sender MAY set a value of 0 in the field, in which case the Responder MAY choose to open a port and send that back along with the Status set to Success. It should be noted that this behavior has security ramifications and the port needs to be chosen very carefully by the Responder.

The measurement stream typically consists of packets or frames with a periodic inter-packet distribution. The Sender need not wait for a Measurement-Response packet to arrive before sending another Measurement-Request packet; in many cases, it will not be possible to wait in order to maintain the desired inter-packet distribution.

The default format for all timestamps is as specified in RFC 5905 [RFC5905].

All messages and fields within a message are assumed to be in network order. In addition, all data fields are unsigned unless mentioned otherwise.

5. Extensions

This section describes how the protocol can be extended to allow for additional functionality, such as new types of measurements.

In order to allow for new types of measurements, additional Measurement-Type CSLDs can be defined to be carried within the Control-Request and Control-Response messages in place of the UDP-Measurement CSLD defined in this document. The meaning and precise format of such a CSLD needs to be defined in a separate specification. Such a specification will also need to describe the appropriate formats for the messages in the Measurement Phase.

In addition, the protocol can be extended by adding support for new values to registries defined in this document.

6. IANA Considerations

The registries defined below are needed for the extensibility of the protocol. In the registries, the terms 'Private Use' and 'Experimental Use' have the same meaning as described in RFC 5226 [RFC5226].

Furthermore, for the following registries, the ranges designated "Unassigned" are governed by the policy 'RFC Required' as described in RFC 5226 [RFC5226].

Cisco SLA Protocol Version Number Registry

Version	Description
0	Reserved
1	Reserved
2	Version 2
3 - 200	Unassigned
201 - 225	Private Use
226 - 255	Experimental Use

The version number should be changed only when the structure of the Command messages is different from the basic Command-Header and CSLD structure described in this document.

Cisco SLA Protocol CSLD Command Registry

CSLD Type	Description
0	Reserved
1	Authentication CSLD
2	UDP-Measurement
3 - 52	Reserved
53 - 10239	Unassigned
10240 - 20479	Private Use
20480 - 65535	Experimental Use

It is envisioned that future documents will provide their own Measurement-Type number and format of the Data portion.

Cisco SLA Protocol Authenticator Modes Registry

Mode	Description
0	No Authentication
1	SHA256
2	HMAC-SHA-256
3 - 200	Unassigned
201 - 225	Private Use
226 - 255	Experimental Use

Cisco SLA Protocol Roles Registry

Role	Description
0	Reserved
1	Sender
2	Responder
3 - 200	Unassigned
201 - 225	Private Use
226 - 255	Experimental Use

Cisco SLA Protocol Measurement Type Registry

Measurement Type	Description
0	Reserved
1	Reserved
2	Reserved
3	UDP
4 - 52	Reserved
53-10239	Unassigned
10240 - 20479	Private Use
20480 - 65535	Experimental Use

The following registry is also needed for the extensibility of the protocol. However, the range designated "Unassigned" is governed by the policy 'First Come First Served' as described in RFC 5226 [RFC5226].

Cisco SLA Protocol Status Types Registry

Status	Description
0	Success
1	Fail - catch all
2	Authentication failure
3	Format error - sent when any CSLD type is not recognized or any part of a CSLD has a value that is not recognized
4	Port in use - the UDP/TCP port is already being used by some other application and cannot be reserved
5 - 40959	Unassigned
40960 - 65535	Experimental Use

Finally, the following registry is also needed for the extensibility of the protocol. However, the range designated "Unassigned" is governed by the policy 'Specification Required' as described in RFC 5226 [RFC5226].

Cisco SLA Protocol Address Family Registry

Address Type	Description
0	Reserved
1	Reserved
2	IPv4
3	IPv6
4 - 200	Unassigned
201 - 225	Private Use
226 - 255	Experimental Use

7. Security Considerations

7.1. Message Authentication

When the mode for the Authentication CSLD is set to 1, the Message Authentication Digest is generated using the SHA256 algorithm and is to be calculated over the entire packet including the Message Authentication Digest field, which MUST be set to all 0s.

When the mode for the Authentication CSLD is set to 2, the Message Authentication Digest is generated using the HMAC-SHA-256 algorithm as described in RFC 4868 [RFC4868] and is to be calculated over the entire packet including the Message Authentication Digest field, which MUST be set to all 0s.

When the mode field is set to 0, the Random Number and the Message Authentication Digest fields MAY be included; when present, they MUST be set to all 0s.

7.2. IPsec Considerations

It is RECOMMENDED that IPsec be employed to afford better security. IPsec provides enhanced privacy as well as an automated key-distribution mechanism. The recommendations below are similar to those in Section 2 of RFC 3579 [RFC3579].

7.2.1. Control Traffic

For Senders implementing this specification, the IPsec policy would be "Initiate IPsec, from me to any, destination port UDP 1167". This causes the Sender to initiate IPsec when sending control traffic to any Responder. If some Responders contacted by the Sender do not support IPsec, then a more granular policy will be required, such as "Initiate IPsec, from me to IPsec-Capable-Responder, destination port UDP 1167".

For Responders implementing this specification, the IPsec policy would be "Require IPsec, from any to me, destination port UDP 1167". This causes the Responder to require use of IPsec. If some Sender does not support IPsec, then a more granular policy will be required: "Require IPsec, from IPsec-Capable-Sender to me".

7.2.2. Measurement Traffic

As the Control Phase occurs before the Measurement Phase, it should be possible to build an IPsec Security Association once a successful Control-Response is received.

For Senders implementing this specification, the IPsec policy would be "Initiate IPsec, from me to negotiated address, destination is negotiated port". This causes the Sender to initiate IPsec when sending measurement traffic to the Responder. If some Responders contacted by the Sender do not support IPsec, then a more granular policy will be required, such as "Initiate IPsec, from me to IPsec-Capable-Responder, destination is negotiated port".

For Responders implementing this specification, the IPsec policy would be "Require IPsec, from negotiated address to me, destination is negotiated port". This causes the Responder to require use of IPsec. If some Sender does not support IPsec, then a more granular policy will be required: "Require IPsec, from IPsec-Capable-Sender to me, destination is negotiated port".

7.3. Replay Protection

For the Control messages, the originator of the message MAY choose to include a current value in the Sent Timestamp field indicating the time the message was submitted for transmission; otherwise, it MUST be set to 0. The receiver of the message MAY choose to validate it if the timestamp is within an acceptable range. The measurement traffic described in this document contains a timestamp to indicate the sent time and hence no new field is required.

8. Acknowledgements

The authors wish to acknowledge the contributions of several key people who contributed to the current form of the document: Hanlin Fang, David Wang, Anantha Ramaiah, Max Pritikin, Malini Vijayamohan, and Susan Boyle.

9. References

9.1. Normative References

[IEEE1588] IEEE, "1588-2008 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", March 2008.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, May 2007.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, June 2010.

9.2. Informative References

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", RFC 4656, September 2006.

[RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, October 2008.

[RFC6374] Frost, D. and S. Bryant, "Packet Loss and Delay Measurement for MPLS Networks", RFC 6374, September 2011.

Authors' Addresses

Murtaza S. Chiba
Cisco Systems
170 West Tasman Drive
San Jose, 95134
USA

Phone: 1-408-526-4000
EMail: mchiba@cisco.com

Alexander Clemm
Cisco Systems
170 West Tasman Drive
San Jose, 95134
USA

Phone: 1-408-526-4000
EMail: alex@cisco.com

Steven Medley
Cisco Systems
170 West Tasman Drive
San Jose, 95134
USA

Phone: 1-408-526-4000
EMail: stmedley@cisco.com

Joseph Salowey
Cisco Systems
170 West Tasman Drive
San Jose, 95134
USA

Phone: 1-408-526-4000
EMail: jsalowey@cisco.com

Sudhir Thombare
Cisco Systems
170 West Tasman Drive
San Jose, 95134
USA

Phone: 1-408-526-4000
EMail: thombare@cisco.com

Eshwar Yedavalli
Cisco Systems
170 West Tasman Drive
San Jose, 95134
USA

Phone: 1-408-526-4000
EMail: eshwar@cisco.com