Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 6, 2020

E. Lear
Cisco Systems
M. Ranganathan
NIST
July 05, 2019

Reporting MUD behavior to vendors
draft-lear-opsawg-mud-reporter-00

Abstract

As with other technology, manufacturers would like to understand how networks implementing MUD are treating devices that are providing MUD URLs and MUD files. This memo specifies an extension to MUD that permits certain behaviors to be reported.

Table of Contents

1. Introduction

Manufacturer Usage Descriptions (MUD) [RFC8520] provides a means for devices to identify what they are and what sort of network access they need. When a device with a MUD URL and a MUD file is fielded in volume, manufacturers may be curious as to whether it is getting the access it needs. There a few several reasons why a device would not be getting the access it needs. Some examples include:

- The MUD file permits access only to a controller but there is none.
- The MUD file permits access only to same-manufacturer or model but there is none.
- The MUD file permits access to a particular Internet service, but the name of that service has not been resolved (or name resolution failed).
- The administrator overrode the recommendations in the MUD file.

This memo sets out to provide manufacturers indications regarding what has happened, in a similar vein to how DMARC is usd to report message drops to messag senders [RFC7489].

In order to provide meaningful reporting, it is necessary to indicate whether or not the above abstractions are in use at a given time, and any public IP addresses that have been mapped to domain names by the local deployment. A communication method that may establish the source of the reporter is also necessary, as well as the MUD URL in use at the time of the report.

This memo specifies a YANG model for reporting and a means for transmitting the report, and appropriate extensions to the MUD file to indicate how to report and how often.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. The mud-reporter-extension model extension

We now formally define this extension. This is done in two parts. First, the extension name "reporter" is listed in the "extensions" array of the MUD file.

Second, the "mud" container is augmented with a container that points to where to report and how often.

This is done as follows:

```
module: ietf-mud-controller-candidate
  augment /mud:mud:
      +--rw reporter
          +--rw report-uri    inet:uri
          +--rw frequency?    uint32
```

Finally the logging format is defined as follows:

```
module: ietf-mud-reporter
  +--rw mud-reporter
     +--rw mudurl?       inet:uri
     +--rw mud-report* [time]
        +--rw time                 yang:timestamp
        +--rw opaqueidentifier?    string
        +--rw direction?           enumeration
        +--rw mycontrollers?       uint32
        +--rw controllers* [uri]
        |  +--rw uri          inet:uri
        |  +--rw count?       uint32
        |  +--rw ipaddress?   inet:ip-address
        +--rw samemanufacturers?   uint32
        +--rw manufacturers* [authority]
        |  +--rw authority    inet:host
        |  +--rw count?       uint32
        |  +--rw ipaddress?   inet:ip-address
        +--rw models* [uri]
        |  +--rw uri          inet:uri
        |  +--rw count?       uint32
        |  +--rw ipaddress?   inet:ip-address
        +--rw domains* [hostname]
        |  +--rw hostname        inet:host
        |  +--rw ip-addresses*   inet:ip-address
        +--rw manufacturer?        string
        +--rw model?               string
        +--rw local-networks?      boolean
        +--rw controller?          string
        +--rw drop-count?          uint32
```

2.1. The mud-reporter-extension augmentation to the MUD YANG model

```
<CODE BEGINS>file "ietf-mud-reporter-extension@2019-06-21.yang"
module ietf-mud-reporter-extension {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-mud-reporter-extension";
  prefix mud-reporter-extension;

  import ietf-mud {
    prefix "mud";
  }

  import ietf-inet-types {
    prefix "inet";
  }

  organization
```

```
      "IETF OPSAWG (Ops Area) Working Group";
    contact
      "WG Web: http://tools.ietf.org/wg/opsawg/
       WG List: opsawg@ietf.org
       Author: Eliot Lear
       lear@cisco.com
      ";
    description

      "This YANG module augments the ietf-mud model to provide for two
       optional lists to indicate that this device type may be used as
       a controller for other MUD-enabled devices.

       Copyright (c) 2019 IETF Trust and the persons identified as
       authors of the code.  All rights reserved.

       Redistribution and use in source and binary forms, with or
       without modification, is permitted pursuant to, and subject to
       the license terms contained in, the Simplified BSD License set
       forth in Section 4.c of the IETF Trust's Legal Provisions
       Relating to IETF Documents
         (https://trustee.ietf.org/license-info).

       This version of this YANG module is part of RFC XXXX
       (https://www.rfc-editor.org/info/rfcXXXX); see the RFC itself
        for full legal notices.

       The key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL
       NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'NOT RECOMMENDED',
      'MAY', and 'OPTIONAL' in this document are to be interpreted as
       described in BCP 14 (RFC 2119) (RFC 8174) when, and only when,
      they appear in all capitals, as shown here.
  ";

    revision 2019-06-21 {
      description
        "Initial proposed standard.";
      reference "RFC XXXX: Extension for MUD Reporting";
    }

    grouping mud-reporter-extension {
        description
           "Reporter information  grouping";
        container reporter {
          description "Reporter information";
          leaf report-uri {
            type inet:uri;
            description
```

```
              "Restful endpoint for reporter information.";
            }
          leaf frequency {
            type uint32
            {
              range "60..max";
            }
            default 1440;
            description
              "The minimum period of time in minutes that a deployment
               should report.";
          }
        }
    }

    augment "/mud:mud" {
      uses mud-reporter-extension;
      description
        "add reporter extension";
    }
  }
  <CODE ENDS>
```

2.2. The Reporter record format

```
   <CODE BEGINS>file "ietf-mud-reporter@2019-06-21.yang"
   module ietf-mud-reporter {
     yang-version 1.1;
     namespace "urn:ietf:params:xml:ns:yang:ietf-mud-reporter";
     prefix mud-reporter;

     import ietf-inet-types {
       prefix inet;
     }
     import ietf-yang-types {
       prefix yang;
     }

     organization
       "IETF OPSAWG (Ops Area) Working Group";
     contact
       "WG Web: http://tools.ietf.org/wg/opsawg/
        WG List: opsawg@ietf.org
        Author: Eliot Lear
        lear@cisco.com
       ";
     description
       "This YANG module specifies the reporting format for MUD managers
```

```
        to use when they are reporting to manufacturers.

        Copyright (c) 2019 IETF Trust and the persons identified as
        authors of the code.  All rights reserved.

        Redistribution and use in source and binary forms, with or
        without modification, is permitted pursuant to, and subject to
        the license terms contained in, the Simplified BSD License set
        forth in Section 4.c of the IETF Trust's Legal Provisions
        Relating to IETF Documents
          (https://trustee.ietf.org/license-info).

        This version of this YANG module is part of RFC XXXX
        (https://www.rfc-editor.org/info/rfcXXXX); see the RFC itself
         for full legal notices.

        The key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL
        NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'NOT RECOMMENDED',
        'MAY', and 'OPTIONAL' in this document are to be interpreted as
        described in BCP 14 (RFC 2119) (RFC 8174) when, and only when,
        they appear in all capitals, as shown here.
      ";

    revision 2019-06-21 {
      description
        "Initial proposed standard.";
      reference
        "RFC XXXX: Extension for MUD Reporting";
    }

    container mud-reporter {
      uses mud-reporter-grouping;
      description "Reporter Information.";
    }

    grouping mud-reporter-grouping   {

      description
        "MUD reporter container.";
      leaf mudurl {
        type inet:uri;
        description
          "The MUD-URL for which the report is being sent.";
      }
      list mud-report {
        key "time";
        description
          "individual records.";
```

```
        leaf time {
          type yang:timestamp;
          description
            "when this happened.";
        }
        leaf opaqueidentifier {
          type string;
          description
            "This is an identifier that maps to a particular
             device.  Its value MUST NOT be mappable back to
             any identifying information about the device.  It
             may be a suitable hash, such as SHA256.";
        }
        leaf direction {
          type enumeration {
            enum to-device {
              description
                "packet was traveling toward the device";
            }
            enum from-device {
              description
                "packet was traveling away from the device";
            }
          }
          description
            "which way packet is going";
        }
        leaf mycontrollers {
          type uint32;
          description
            "how many entries for my-controller.";
        }
        list controllers {
          key "uri";
          description
            "list of controllers and how many there were.";
          leaf uri {
            type inet:uri;
            description
              "the class URI of this controller";
          }
          leaf count {
            type uint32;
            description
              "number of devices serving this class.";
          }
          leaf ipaddress {
            type inet:ip-address;
```

```
            description
              "IP address of the controller.  Note that the MUD
               reporter MUST NOT transmit this contents of this
               node to the manufacturer.";
          }
        }
        leaf samemanufacturers {
          type uint32;
          description
            "number of devices matching same
             manufacturer.";
        }
        list manufacturers {
          key "authority";
          description
            "list of models and how many there were.";
          leaf authority {
            type inet:host;
            description
              "the manufacturer domain";
          }
          leaf count {
            type uint32;
            description
              "number of devices serving this class.";
          }
          leaf ipaddress {
            type inet:ip-address;
            description
              "IP address of the controller.  Note that the MUD
               reporter MUST NOT transmit this contents of this
               node to the manufacturer.";
          }
        }
        list models {
          key "uri";
          description
            "list of models and how many there were.";
          leaf uri {
            type inet:uri;
            description
              "the URI of this model";
          }
          leaf count {
            type uint32;
            description
              "number of devices serving this class.";
          }
```

```
          leaf ipaddress {
            type inet:ip-address;
            description
              "IP address of the controller.  Note that the MUD
               reporter MUST NOT transmit this contents of this
               node to the manufacturer.";
          }
        }
        list domains {
          key "hostname";
          description
            "list of hosts, and ip addresses if known.";
          leaf hostname {
            type inet:host;
            description
              "the host listed";
          }
          leaf-list ip-addresses {
            type inet:ip-address;
            description
              "ipv4 or v6 address mapping for this host if
               known.";
          }
        }
        uses class-drop-count;
      }
    }

    grouping class-drop-count {
      description
        "Destination fields of acl violating  packet are classfied.";
      leaf manufacturer {
        type string;
        description
          "manufacturer name";
      }
      leaf model {
        type string;
        description
          "model name";
      }
      leaf local-networks {
        type boolean;
        description
          "this packet matches the local networks
           classification";
      }
      leaf controller {
```

```
        type string;
        description
          "controller name";
      }
      leaf drop-count {
        type uint32;
        description
          "number of packets dropped for this classification";
      }
    }
  }
```

<CODE ENDS>

3. RESTful interface at the collector

```
<CODE BEGINS>file "ietf-mud-reporter-collector@2019-06-21.yang"
module ietf-mud-reporter-collector {
   yang-version 1.1;
   namespace "urn:ietf:params:xml:ns:yang:ietf-mud-reporter-collector";
   prefix "mud-collector";

   import ietf-mud-reporter {
        prefix "reporter";
    }
  organization
    "IETF OPSAWG (Ops Area) Working Group";
  contact
    "WG Web: http://tools.ietf.org/wg/opsawg/
     WG List: opsawg@ietf.org
     Author: Eliot Lear
     lear@cisco.com
     Author: Mudumbai Ranganathan
     mranga@nist.gov
    ";
  description
    "This YANG module specifies the reporting format for MUD managers
     to use when they are reporting to manufacturers.

     Copyright (c) 2019 IETF Trust and the persons identified as
     authors of the code.  All rights reserved.

     Redistribution and use in source and binary forms, with or
     without modification, is permitted pursuant to, and subject to
     the license terms contained in, the Simplified BSD License set
     forth in Section 4.c of the IETF Trust's Legal Provisions
     Relating to IETF Documents
       (https://trustee.ietf.org/license-info).
```

```
      This version of this YANG module is part of RFC XXXX
      (https://www.rfc-editor.org/info/rfcXXXX); see the RFC itself
       for full legal notices.

      The key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL
      NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'NOT RECOMMENDED',
      'MAY', and 'OPTIONAL' in this document are to be interpreted as
      described in BCP 14 (RFC 2119) (RFC 8174) when, and only when,
      they appear in all capitals, as shown here.
    ";
  revision 2019-06-21 {
    description
      "Initial proposed standard.";
    reference
      "RFC XXXX: Extension for MUD Reporting";
  }
    rpc post-mud-report {
      description
         "Rpc interface that must be supported by collection point.";
      input {
        container mud-report {
          uses  reporter:mud-reporter-grouping;
          description "MUD report";
        }
      }
    }
}

<CODE ENDS>
```

4. Examples

TBD

5. Privacy Considerations

Using this reporting mechanisms does not reveal internal IP addresses. Instead, it simply indicates whether a given abstraction is in use, and how many instances there are. What is revealed to the manufacturer is that one or more devices reporting a particular MUD-URL is located at a particular deployment. In addition, as of this draft, reportable events include only administratively dropped packets, and the times they were dropped.

In order to report the sorts of errors discussed in this memo, a deployment must determine which packets from a given device have either been or would be dropped due to an administrative filter rule.

6. Security Considerations

All security considerations of [RFC8520] apply equally to this extension. In addition, some care should be given to claims that a device is permitted to be a controller in any given circumstances. Complete automation requires far more context than is currently specified here. Some form of confirmation or selection is required by an administrator. This memo simply makes it easier for administrator to identify candidates for controller selection.

IANA Considerations ==========

The IANA is requested to add "controller-candidate" to the MUD extensions registry as follows:

Extension Name: reporter
Standard reference: This document

7. References

7.1. Normative References

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

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <https://www.rfc-editor.org/info/rfc6991>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8520] Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", RFC 8520, DOI 10.17487/RFC8520, March 2019, <https://www.rfc-editor.org/info/rfc8520>.

7.2. Informative References

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/info/rfc7489>.

Appendix A. Changes from Earlier Versions

Draft -00:

- Initial revision

Authors' Addresses

Eliot Lear
Cisco Systems
Richtistrasse 7
Wallisellen CH-8304
Switzerland

Phone: +41 44 878 9200
Email: lear@cisco.com

Mudumbai Ranganathan
NIST
100 Bureau Dr.
Gaithersburg
U.S.A

Phone: +1 301 975 2857
Email: mranga@nist.gov