Network Working Group E. Lear
Internet-Draft J. Henry
Intended status: Experimental Cisco Systems
Expires: January 9, 2020 July 08, 2019

Bandwidth Profiling Extensions for MUD
draft-lear-opsawg-mud-bw-profile-01

Abstract

Manufacturer Usage Descriptions (MUD) are a means by which devices can establish expectations about how they are intended to behave, and how the network should treat them. Earlier work focused on access control. This draft specifies a means by which manufacturers can express to deployments what form of bandwidth profile devices are expected to have with respect to specific services.

Status of This Memo

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

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

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

This Internet-Draft will expire on January 9, 2020.

Table of Contents

1. Introduction

Devices connecting to networks will often exhibit certain nominal behaviors that can be described. In addition, sometimes device require particular network behaviors such as appropriate quality-of-service treatment. Manufacturer Usage Descriptions [RFC8520] discuss how to characterize access control requirements, for instance. As just mentioned, access control requirements are not the only requirements device manufacturers may wish to specify. This memo defines an extension to the MUD YANG model by which manufacturers can characterize the traffic exchanged with a Thing, and specify how much

bandwidth is required by a device or may be expected of a device over some period of time for each given service it uses.

Network deployments may use this information in two ways:

- Provisioning of bandwidth based on device requirements;
- Facilitating proper traffic characterization and marking by the network infrastructure
- Policing of devices to not permit them to exceed design requirements. In particular, a device that is transmitting a DSCP value that exceeds the expected value, or that manifests unusual transmission patterns, should be viewed with great suspicion.

The basis of the model is that services may be identified by access-lists, and that each service can then be assigned an attendant bandwidth expectation in terms of either bits-per-second or packets-per-second. In addition, a DSCP marking can be specified.

When a service is identified by access lists, each access list is appended to the existing access list entries. N.B., as a reminder, acl names in MUD files are scoped solely to those files, and may conflict with acl names in _other_ MUD files.

1.1. Envisioned Uses

A luminaire may require a few packets per minute of a predictable payload size (e.g. keepalives), and may expect that traffic to be sent in the background, as one or more keepalive packet loss would not impede the luminaire functions. Additionally, when a virtual 'light switch' changes its state, a burst of 3 to 4 packets over a well-defined port are expected, with a QoS marking of OAM. Last, occasional firmware updates may bring an exchange of a few kilobytes marked as best effort.

A smoke detector may require at most 1 packet per second at best effort (keepalive), except when there is a problem, at which point it may send a frame upstream to a specific port and of a specified payload size, with a DSCP marking of EF.

A coffee maker may be designed never set DSCP to anything other than AF13 (even when it's empty, perish the thought), nor may it ever use more than 5 packets of 120 bytes payload per minute, even if it has a fault.

A different coffee maker may be designed to set DSCP to EF if the it has caught fire.

1.2. Limitations

Not every device can be easily profiled. Not every service on every device may be easily profiled. A manufacturer may use this extension to describe those services that _are_ easily profile, and omit services that the device offers or uses that are not easily profiled.
The local deployment is cautioned not to assume that a service not profiled is in some way anomalous, even when other services are.

1.3. What devices would use this extension?

The MUD manager remains a key component of this system. To begin with, it is the component that retrieves the MUD file, and would identify the extension. From that point, different implementation

decisions can be made. For instance, the MUD manager or associated infrastructure can retain the mapping between devices and MUD-URLs. A dispatch function could be implemented wherever that mapping is housed, such that either enforcement or monitoring functions can be invoked. Enforcement functions would almost certainly begin with some form of telemetry on access switches, routers or firewalls. That same telemetry might be exported to an IPFIX analyzer [RFC7011] that might report anomalies.

2. The ietf-mud-bw-profile model extension

To extend MUD the "qos" extension is added as an element to the "extensions" node when a MUD file is generated.

The model augmentation appears as follows:

```
module: ietf-mud-bw-profile
  augment /mud:mud/mud:to-device-policy:
    +--rw bw-params
       +--rw service* [name]
          +--rw name         string
          +--rw timeframe    uint32
          +--rw pps?         uint32
          +--rw bps?         uint64
          +--rw dscp?        inet:dscp
          +--rw aclname?     -> /acl:acls/acl/name
  augment /mud:mud/mud:from-device-policy:
    +--rw bw-params
       +--rw service* [name]
          +--rw name         string
          +--rw timeframe    uint32
          +--rw pps?         uint32
          +--rw bps?         uint64
          +--rw dscp?        inet:dscp
          +--rw aclname?     -> /acl:acls/acl/name
```

2.1. The mud-qos YANG model

```
<CODE BEGINS>file "ietf-mud-bw-profile@2019-07-08.yang"
module ietf-mud-bw-profile {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-mud-bw-profile";
  prefix mud-qos;

  import ietf-access-control-list {
    prefix acl;
  }
  import ietf-inet-types {
```

```
    prefix inet;
  }
  import ietf-mud {
    prefix mud;
  }

  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: Jerome Henry
     jerhenry@cisco.com
    ";
  description

    "This YANG module augments the ietf-mud model to provide the
     network with some understanding as to the QoS requirements and
     anticipated behavior of a device.

     The to-device-policy and from-device-policy containers are
     augmented with one additional container, which expresses how many
     packets per second a device is expected to transmit, how much
     bandwidth it is expected to use, and what QoS is required, and
     how much bandwidth is to be expected to be prioritized.  An
     access-list is further specified to indicate how QoS should be
     marked on ingress and egress.

     Copyright (c) 2016,2017,2018 IETF Trust and the persons
     identified as the document authors.  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
     (http://trustee.ietf.org/license-info).
     This version of this YANG module is part of RFC XXXX; see
     the RFC itself for full legal notices.";

  revision 2019-07-08 {
    description
      "Initial proposed standard.";
    reference "RFC XXXX: Bandwidth Descriptions for MUD
Specification";
  }

  grouping mud-bw-params {
```

```
     description
       "QoS and Bandwidth additions for MUD";
     container bw-params {
       description
         "Expected Bandwidth to/from device";
       list service {
         key "name";
         description
           "a list of services that are being described.";
         leaf name {
           type string;
           description
             "Service Name";
         }
         leaf timeframe {
           type uint32;
           mandatory true;
           description
             "the period of time in seconds one
              expects a service to burst at described rates";
         }
         leaf pps {
           type uint32;
           description
             "number of packets per second to be expected.";
         }
         leaf bps {
           type uint64;
           description
             "number of bits per second to be expected.";
         }
         leaf dscp {
           type inet:dscp;
           description
             "The DSCP that packets for this service should
              treated with.  N.B., just because the manufacturer
              wants this, doesn't mean it will get it.  However,
              manufacturers who do set the DSCP value in their
              packets SHOULD indicate that in this description.

              This field differs from the dscp field in the matches
              portion of the access-list in that here the field is
              populated when the manufacturer states what the nominal
              value of the DSCP field MAY be, and how much bandwidth
              can be used when it is set.  Note that it is possible
              that the same service may use multiple DSCP values,
              depending on the circumstances.  In this case, service
              entry MUST be made.";
```

```
        }
        leaf aclname {
          type leafref {
            path "/acl:acls/acl:acl/acl:name";
          }
          description
            "The name of the ACL that will match packets
             for a given service.";
        }
      }
    }
  }

  augment "/mud:mud/mud:to-device-policy" {
    description
      "add inbound QoS parameters";
    uses mud-bw-params;
  }
  augment "/mud:mud/mud:from-device-policy" {
    description
      "add outbound QoS parameters";
    uses mud-bw-params;
  }
}
<CODE ENDS>
```

3. Examples

TBD

4. Security Considerations

4.1. Manufacturer Attempts to Exhaust Available Bandwidth

An attacking manufacturer claims a device would require substantial bandwidth or QoS for use. This attack would be effected when a device is installed into a local deployment and its MUD file interpreted. The impact of a device demanding excessive bandwidth could be overprovisioning of the network or denial of service to other uses.

This attack is remediated by a human being reviewing the bandwidth consumption projections suggested by the MUD file when they are in some way beyond the norm for any device being installed.

4.2. Device lies about what it is to get more bandwidth

If the device is emitting a MUD-URL via insecure, it is possible for an attacker to modify it. Devices emitting such URLs should already receive additional scrutiny from administrators as they are onboarded. This mechanism SHOULD NOT be used to admit devices into privileged queues without them having been securely admitted to the network, through means such as IEEE 802.1X.

5. IANA Considerations

The IANA is requested to add "qos" to the MUD extensions registry as follows:

Extension Name: MUD
Standard reference: This document

6. References

6.1. Normative References

[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>.

6.2. Informative References

[RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <https://www.rfc-editor.org/info/rfc7011>.

Appendix A. Changes from Earlier Versions

Draft -01:

- Very modest changes.

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

Jerome Henry
Cisco Systems
170 W. Tasman Dr.
San Jose, CA 95134
United States

Email: ofriel@cisco.com