                   Diameter Congestion and Filter Attributes

Abstract

   This document defines optional Diameter attributes that can be used
   to help manage networks that use Explicit Congestion Notification
   (ECN) or Diameter traffic filters.  These new attributes allow for
   improved data traffic identification, support of ECN, and minimal
   Diameter filter administration.

   RFC 5777 defines a Filter-Rule Attribute Value Pair (AVP) that
   accommodates extensions for classification, conditions, and actions.
   It, however, does not support traffic identification for packets
   using Explicit Congestion Notification as defined in RFC 3168 and
   does not provide specific actions when the flow(s) described by the
   Filter-Rule are congested.

   Further, a Filter-Rule can describe multiple flows but not the exact
   number of flows.  Flow count and other associated data (e.g.,
   packets) are not captured by accounting applications, leaving
   administrators without useful information regarding the effectiveness
   or appropriateness of the filter definition.

   The optional attributes defined in this document are forward and
   backwards compatible with RFC 5777.

Status of This Memo

Copyright Notice

Table of Contents

1.  Introduction

    Two optional AVPs related to Explicit Congestion Notification (ECN)
    [RFC3168] are specified in this document.  The first AVP provides
    direct support for filtering ECN-marked traffic [RFC3168] and the
    second AVP provides the ability to define alternate traffic treatment
    when congestion is experienced.

    This document also defines two optional AVPs, Flow-Count and Packet-
    Count, used for conveying flow information within the Diameter
    protocol [RFC6733].  These AVPs were found to be useful for a wide
    range of applications.  The AVPs provide a way to convey information
    of the group of flows described by the Filter-Rule, IPFilterRule, or
    other Diameter traffic filters.

    The semantics and encoding of all AVPs can be found in Section 3.

    Such AVPs are, for example, needed by some congestion-management
    functions to determine the number of flows congested or used by
    administrators to determine the impact of filter definitions.

    Additional parameters may be defined in future documents as the need
    arises.  All parameters are defined as Diameter-encoded Attribute
    Value Pairs (AVPs), which are described using a modified version of
    the Augmented Backus-Naur Form (ABNF), see [RFC6733].  The data types
    are also taken from [RFC6733].

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 RFC2119 [RFC2119].

3.  ECN-IP-Codepoint, Congestion-Treatment, and Filter Attributes

3.1.  ECN-IP-Codepoint AVP

   The ECN-IP-Codepoint AVP (AVP Code 628) is of type Enumerated and
   specifies the ECN codepoint values to match in the IP header.

```
Value | Binary | Keyword                                | References
-----------------------------------------------------------------
0     | 00     | Not-ECT (Not ECN-Capable Transport)| [RFC3168]
1     | 01     | ECT(1) (ECN-Capable Transport)     | [RFC3168]
2     | 10     | ECT(0) (ECN-Capable Transport)     | [RFC3168]
3     | 11     | CE (Congestion Experienced)        | [RFC3168]
```

   When this AVP is used for classification in the Filter-Rule, it MUST
   be part of the Classifier Grouped AVP as defined in RFC 5777.

3.2.  Congestion-Treatment AVP

   The Congestion-Treatment AVP (AVP Code 629) is of type Grouped.  It
   indicates how to treat traffic IP (5-tuple) flow(s) when congestion
   is detected.  The detection of congestion can be based on the
   reception of IP packets with the Congestion Experience (CE) codepoint
   set (see [RFC3168]) or by any other administratively defined
   criteria.

   A Filter-Rule may contain a Classifier that describes one or many
   5-tuples per RFC 5777.  This treatment applies to all packets
   associated to all 5-tuples (flows) captured by the Filter-Rule.

   If the Congestion-Treatment AVP is absent, the treatment of the
   congested traffic is left to the discretion of the node performing
   quality-of-service (QoS) treatment.

```
             Congestion-Treatment ::= < AVP Header: 629 >
                      { Treatment-Action }
                      [ QoS-Profile-Template ]
                      [ QoS-Parameters ]
                  * [ AVP ]
```

   Treatment-Action, QoS-Profile-Template, and QoS-Parameters are
   defined in RFC 5777.  The Congestion-Treatment AVP is an action and
   MUST be an attribute of the Filter-Rule Grouped AVP as defined in RFC
   5777.

3.3.  Flow-Count AVP

   The Flow-Count AVP (AVP Code 630) is of type Unsigned64.

   It indicates the number of protocol-specific flows.  The protocol is
   determined by the filter (e.g., IPFilterRule, Filter-Id, etc.).

3.4.  Packet-Count AVP

   The Packet-Count AVP (AVP Code 631) is of type Unsigned64.

   It indicates the number of protocol-specific packets.  The protocol
   is determined by the filter (e.g., IPFilterRule, Filter-Id, etc.).

4.  IANA Considerations

4.1.  AVP Codes

   IANA allocated AVP codes in the IANA-controlled namespace registry
   specified in Section 11.1.1 of [RFC6733] for the following AVPs that
   are defined in this document.

   +---------------------------------------------------------------+
   |                              AVP    Section                    |
   |AVP                           Code   Defined  Data Type         |
   +---------------------------------------------------------------+
   |ECN-IP-Codepoint              628    3.1      Enumerated        |
   |Congestion-Treatment          629    3.2      Grouped           |
   |Flow-Count                    630    3.3      Unsigned64        |
   |Packet-Count                  631    3.4      Unsigned64        |
   +---------------------------------------------------------------+

5.  Examples

   The following examples illustrate the use of the AVPs defined in this
   document.

5.1.  Classifier Example

   The Classifier AVP (AVP Code 511) specified in RFC 5777 is a grouped
   AVP that consists of a set of attributes that specify how to match a
   packet.  The addition of the ECN-IP-Codepoint is shown here.

```
      Classifier ::= < AVP Header: 511 >
                   { Classifier-ID }
                   [ Protocol ]
                   [ Direction ]
                   [ ECN-IP-Codepoint ]
                 * [ From-Spec ]
                 * [ To-Spec ]
                 * [ Diffserv-Code-Point ]
                   [ Fragmentation-Flag ]
                 * [ IP-Option ]
                 * [ TCP-Option ]
                   [ TCP-Flags ]
                 * [ ICMP-Type ]
                 * [ ETH-Option ]
                 * [ AVP ]
```

   Setting the ECN-IP-Codepoint value to 'CE' would permit the capture
   of CE flags in the Flow.

   Another Classifier with the ECN-IP-Codepoint value of 'ECT' could be
   specified and, when coupled with the Flow-Count AVP, reports the
   number of ECT-capable flows.

5.2.  Diameter Credit Control (CC) with Congestion Information

   Diameter nodes using Credit Control can use the Congestion-Treatment
   AVP to trigger specific actions when congestion occurs.  This is
   similar to the Excess-Treatment Action.  The ability to detect when
   congestion occurs is specific to the AVPs in the Filter-Rule and
   Diameter Client and is no different than how 'Excess' can be
   determined for Excess-Treatment.  If conditions associated with
   Excess-Treatment [RFC5777] or Congestion-Treatment have occurred,
   Diameter Clients may autonomously send Credit-Control Requests (CCRs)
   during the Service Delivery session as interim events.  This is shown
   in Figure 1.

```
                         Service Element
         End User         (CC Client)                      CC Server
            |                 |                                |
            |(1) Service Request|                             |
            |------------------>|                             |
            |                 |(2) CCR (Initial,              |
            |                 |    QoS-Resources(QoS-Desired)) |
            |                 |------------------------------->|
            |                 |(3) CCA (Granted-Units,        |
            |                 |    QoS-Resources(QoS-Authorized))|
            |                 |<-------------------------------|
            |(4) Service Delivery|                            |
            |<----------------->|                             |
            |           (5) Congestion Detected               |
            |           (6) Congestion Treatment Occurs        |
            |                 |(7) CCR (Termination, Used-Units,|
            |                 |    Flow-Count, Packet-Count,   |
            |                 |    QoS-Resources(QoS-Delivered))|
            |                 |------------------------------->|
            |                 |(8) CCA                         |
            |                 |<-------------------------------|
            |                 |                                |
            |                 |                                |
            |(9) End of Service|                              |
            |------------------>|                             |
            |                 |(10)CCR (Termination, Used-Units,|
            |                 |    Flow-Count, Packet-Count,   |
            |                 |    QoS-Resources(QoS-Delivered))|
            |                 |------------------------------->|
            |                 |(11) CCA                        |
            |                 |<-------------------------------|
```

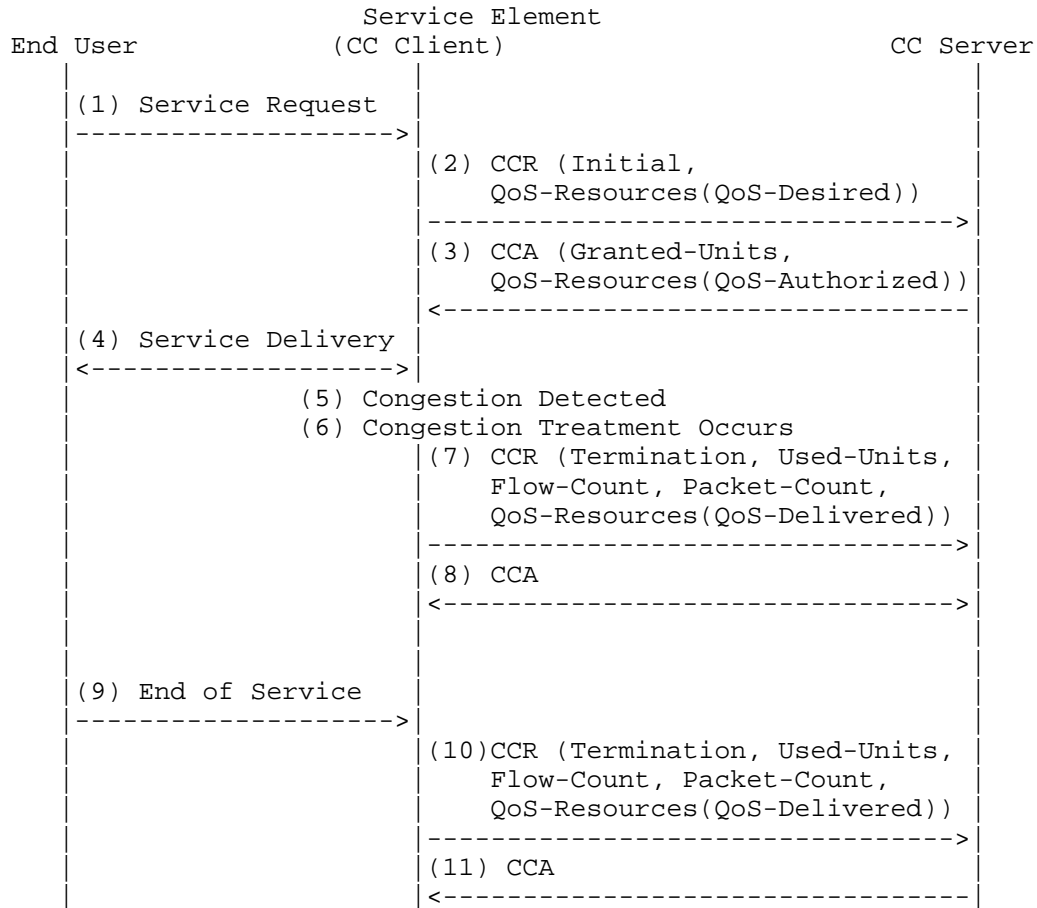                  Figure 1: Example of a Diameter Credit Control with
                             Congestion Information

   The 'Used-Service-Units' described in RFC 5777 examples is
   customarily a Service-Units, Time-Units, or Byte-Count AVP.  This is
   insufficient to represent network state and does not differentiate
   between throughput and good-put (good or quality throughput) even
   though the filters may imply good or poor throughput.

   Flow-Count and Packet-Count AVPs defined in this document could be
   sent with a CCR when the triggering event is related to Congestion-
   Treatment.  This provides the CC Server with a better view of the
   type of congested traffic for improved decision making and charging.
   Sending such AVPs under any condition permits rudimentary traffic
   profiling regardless of network conditions.  For instance, low byte
   counts per packet is indicative of web traffic and high byte counts

   per packet with a small number of flows may be indicative of video
   traffic.  Enriched reporting described here provides relief from Deep
   Packet Inspection load and loss of information as traffic becomes
   increasingly encrypted.

   Some services, e.g., streaming services, limit the number of flows,
   Flow-Count, as opposed to other units, i.e. Byte-Count.  In such a
   case, the Flow-Count AVP may be used in place of Service-Units.

6.  Security Considerations

   This document describes an extension of RFC 5777 that introduces a
   new filter parameter applied to ECN as defined by [RFC3168].  It also
   defines a new Grouped AVP that expresses what action to take should
   congestion be detected.  The Grouped AVP reuses attributes defined in
   RFC 5777.  As these are extensions to RFC 5777, they do not raise new
   security concerns.

   The Flow-Count and Packet-Count AVPs can be provided in conjunction
   with customary AVPs, e.g., Bytes, Time, Service units, during
   accounting activities as described in the base protocol [RFC6733] or
   other Diameter applications.  These new AVPs provide more information
   that can be privacy sensitive.  The privacy sensitivity is directly
   related to traffic captured by filters and associated reports.
   Narrow filtering, which creates the highest level of privacy
   sensitivity, is too resource intensive to be widely applied on large
   networks.  Paradoxically, improving reporting information lessens the
   depth of inspection required to characterize traffic for many
   congestion management activities as noted in Section 5.2.

   If an administrator can provide congestion actions without the need
   to report them to a Diameter application, they should use the
   Congestion-Treatment AVP, which also reduces Diameter traffic during
   congestion events.

   The Security Considerations of the Diameter protocol itself have been
   discussed in RFC 6733 [RFC6733].  Use of the AVPs defined in this
   document MUST take into consideration the security issues and
   requirements of the Diameter base protocol.

7.  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,
              <http://www.rfc-editor.org/info/rfc2119>.

   [RFC3168]  Ramakrishnan, K., Floyd, S., and D. Black, "The Addition
              of Explicit Congestion Notification (ECN) to IP",
              RFC 3168, DOI 10.17487/RFC3168, September 2001,
              <http://www.rfc-editor.org/info/rfc3168>.

   [RFC6733]  Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn,
              Ed., "Diameter Base Protocol", RFC 6733,
              DOI 10.17487/RFC6733, October 2012,
              <http://www.rfc-editor.org/info/rfc6733>.

   [RFC5777]  Korhonen, J., Tschofenig, H., Arumaithurai, M., Jones, M.,
              Ed., and A. Lior, "Traffic Classification and Quality of
              Service (QoS) Attributes for Diameter", RFC 5777,
              DOI 10.17487/RFC5777, February 2010,
              <http://www.rfc-editor.org/info/rfc5777>.

Acknowledgements

Authors' Addresses

   Lyle Bertz
   Sprint
   6220 Sprint Parkway
   Overland Park, KS 66251
   United States

   Email: lyleb551144@gmail.com


   Serge Manning
   Sprint
   6220 Sprint Parkway
   Overland Park, KS 66251
   United States

   Email: sergem913@gmail.com


   Brent Hirschman

   Email: Brent.Hirschman@gmail.com