

Network Working Group
Internet-Draft
Intended status: Experimental
Expires: 28 October 2026

C. Pignataro
NC State University
J. Parikh
Arista Networks
R. Bonica
Juniper
M. Welzl
University of Oslo
26 April 2026

ICMP Extensions for Environmental Information
draft-pignataro-icmp-enviro-info-01

Abstract

This document defines a data structure that can be appended to selected ICMP messages. The ICMP extension defined herein can be used to gain visibility on environmental information on the internet by providing per-hop (i.e., per topological network node) power metrics and other present or future metrics around environmental information. This will contribute to achieving an objective mentioned in the IAB E-Impact workshop [RFC9547].

The techniques presented are useful not only in a transactional setting (e.g., a user-issued traceroute or a ping request), but also in a scheduled automated setting where they may be run periodically in a mesh across an administrative domain to map out environmental information.

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 28 October 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	2
2. Conventions	3
2.1. Definition of Terms	3
2.2. Requirements Language	4
3. Motivation	4
3.1. Why is ICMP suitable?	5
4. Transport Options for Environmental Information	5
5. ICMP Environmental Information Extension	6
5.1. Extension Format	6
5.2. C-Type Definition	7
6. Sub-Object Formats	11
7. Sample Use Case	12
8. Implementation Status	13
9. Security Considerations	14
10. IANA Considerations	15
11. Acknowledgements	17
12. References	17
12.1. Normative References	17
12.2. Informative References	17
Authors' Addresses	19

1. Introduction

IP devices use the Internet Control Message Protocol ICMPv4 [RFC0792] and ICMPv6 [RFC4443] to convey control information to source hosts. In particular, when an IP device receives a datagram that it cannot process, it may send an ICMP message to the datagram's originator or source. Network operators and higher-level protocols use these ICMP messages to detect and diagnose network issues.

As the world transitions towards environmental sustainability in technology, and to use metrics to make networks more efficient, both from the environmental and technological standpoint, the focus is shifting not only on creating modern technologies infused with environmental information but also on bridging gaps in the tools that are already available, to enhance visibility, measurement, and quantification of their environmental impact. Consequently, tools which have been foundational for control and management for decades now encounter new requirements including enhancing them to cater to a significantly increasing demand for monitoring the sustainability and environmental impact.

The IAB had held a workshop on "Environmental Impact of Internet Applications and Systems (eimpactws)" [IAB-EIMPACTWS], in which the need for visibility into environmental sustainability information within traditional Internet tools such as traceroute was highlighted (see WebVTT cue identifiers 139 and 140 of [IAB-EIMPACTWS-Minutes].)

This document serves that need by defining an ICMP extension object that appends environmental sustainability information to ICMP messages. Using ICMP as a medium to deliver environmental sustainability information is very apt as ICMP is one of the most used protocols for administration and troubleshooting and it works effectively not only in an automated setting, but also in an on-demand setting for different purposes and use cases.

Using the extension defined herein, a device can explicitly append these environmental sustainability information for transmission across an administrative domain:

- * Present and idle power (node level, component level)
- * Throughput (node level, component level)
- * Ecolabels and Environmentally Relevant Certifications (EERCs)

Additional environmental sustainability information, such as the following, for example, may also be specified in the future:

- * Electrical Energy Provider or Zone
- * Geolocation

2. Conventions

2.1. Definition of Terms

This document uses the following terms:

ICMP:

Generically referring to ICMPv4 [RFC0792] and ICMPv6 [RFC4443] messages.

ICMP Extension:

Extended ICMP to support multi-part messages through an ICMP extension structure, as defined in [RFC4884].

2.2. Requirements Language

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.

3. Motivation

Motivations behind this proposing the extension defined here in this document are:

(1) Native Telemetry Data Availability

Networking chips and devices increasingly measure and expose environmental information such as power draw, energy use, thermal data, and other pieces of metrics/information. Telemetry data has proven to be very important in making large scale network deployments efficient from the perspective of power consumption, cooling etc.

(2) Ubiquitous Operational Use

Classic diagnostic tools such as ping and traceroute remain the most widely used and universally available command-line utilities for network troubleshooting, commonly serving as the first step in connectivity and reachability diagnosis. Thus, building extensions on top of these tools, could prove to be relatively easy to adapt and implement.

(3) Standardization at the Lowest Common Mechanism

We are making use of an already mature, extensible, and widely implemented foundation: RFC 4884 (Extended ICMP for Multi-Part Messages) [RFC4884]

3.1. Why is ICMP suitable?

Environmental data already exists in inventories, the novelty is surfacing it along the path of live connectivity probes (e.g., ping, traceroute, PROBE [RFC8335]) for real-time, per-hop context.

ICMP is universally implemented, stateless, and tool-agnostic enabling lightweight environmental telemetry without new protocols, APIs, or credentials.

This facilitates path-level mapping of sustainability metrics, comparable to latency or loss, across heterogeneous equipment and administrative domains.

Using ICMP as a “host” for carrying environmental information makes this retrieval method compatible with other approaches. It also complements, rather than replaces, existing methods.

4. Transport Options for Environmental Information

To achieve the goal of transporting useful environmental information across the network, there are two key considerations. First, what information is useful to convey and in what format, and second, how to transport that environmental information.

For the first task, it is critical to normalize and agree upon the information to convey and format, across potentially multiple transports.

For the second task, there is a variety of options available depending on use cases. These can be categorized based on whether the approach is distributed (i.e., any endpoint or node can request and/or receive the environmental information) or centralized (i.e., a single ‘controller’ compiles and consolidates the information.) They can also be categorized based on the networking layer used (e.g., IP, like ICMP, or applications, like SNMP). Further, an existing protocol can be extended, or a brand new protocol can potentially be created for this purpose.

This document builds upon a standardized, modular, backwards-compatible, and scale-proven ICMP extension [RFC4884]. This does not preclude the definition of other methods to transport environmental information, more fitting to other use-cases.

5. ICMP Environmental Information Extension

This section defines the Environmental Information Object, an ICMP extension object with a Class-Num (Object Class Value) of TBA that can be appended to the following messages, as per [RFC4884] and [RFC8335]:

- ```
* ICMPv4 Time Exceeded
* ICMPv4 Destination Unreachable
* ICMPv4 Parameter Problem
* ICMPv4 Extended Echo Reply [RFC8335]
* ICMPv6 Time Exceeded
* ICMPv6 Destination Unreachable
* ICMPv6 Extended Echo Reply [RFC8335]
```

The ICMP extension defined in this document MAY be appended to any of the above listed messages based on policy and following security considerations.

These extensions are preceded by an ICMP Extension Structure Header, and include an ICMP Object Header. Both are defined in [RFC4884]. The same backward compatibility issues that apply to [RFC4884] apply to this extension.

A single ICMP message can contain zero, one, or multiple instances of Environmental Information Objects. The C-Type further identifies the information fields carried.

A single instance of the Environmental Information Object can convey one of the information elements defined in Section 5.2 from each reporting node in an administrative domain.

## 5.1. Extension Format

The ICMP Environmental Information Extension has the following format.

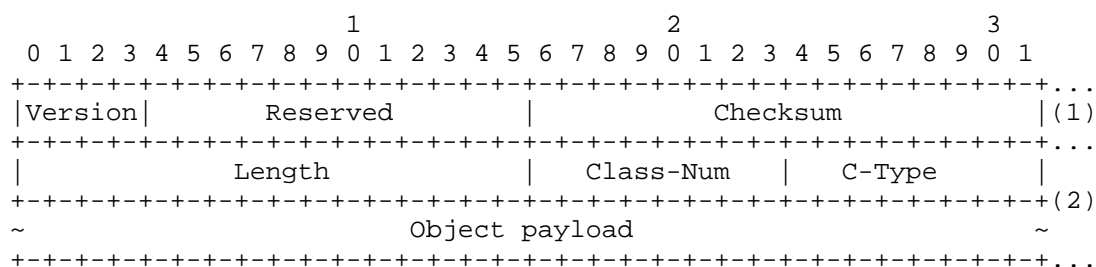


Figure 1: ICMP Environmental Information Extension Format

## (1) ICMP Extension Header

Version:

2 [RFC4884].

Reserved:

0 [RFC4884].

Checksum:

The one's complement checksum of the ICMP extension [RFC4884].

## (2) Environmental Information Object

Length:

Length of the Environmental Information object, including object header and object payload, in octets. If there is no object payload, the value of Length is 4. This is used to convey that the object is unavailable (e.g., because the requested information is not applicable for the type of component that is being queried.)

Class-Num:

TBA (Environmental Information)

C-Type:

C-Type as explained in Section 5.2.

Object Payload:

As defined by each C-Type.

While there is a single ICMP Extension Header, there could be multiple Environmental Information Objects.

## 5.2. C-Type Definition

The 8-bit C-Type defined in the Section 8 of [RFC4884] allows to carry different information elements within this Class-Num (TBA). The techniques herein defined can be used with any specific environmental sustainability metric in use, present or future.

The ICMP Environmental Information Extension Object header has the following format:

| 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 |              |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Length |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   | Class-Num=TBA |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   | C-Type=1-255 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Figure 2: Environmental Information Extension Object Header

The following C-Type values are currently defined.

#### 1. Node Power Draw Sub-Object

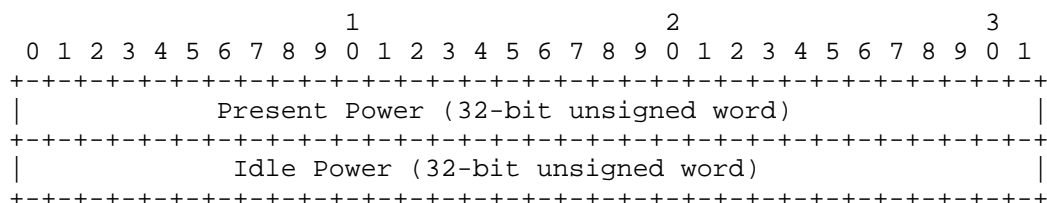


Figure 3: Node Power Draw Sub-Object

A Class-Num of TBA and a C-Type of 1 are specified.

The Length is 12 if the object contains this payload. A Length value of 4 indicates that it is unavailable.

The Present Power is the node-level power being presently drawn, which is a magnitude that may be directly displayed, and is expressed in Watts (W). A value of 0 indicates that the Present Power is not available. The Idle Power is the node-level power when the node is idle. A value of 0 indicates that the Idle Power is not available.

#### 2. Node Throughput Sub-Object

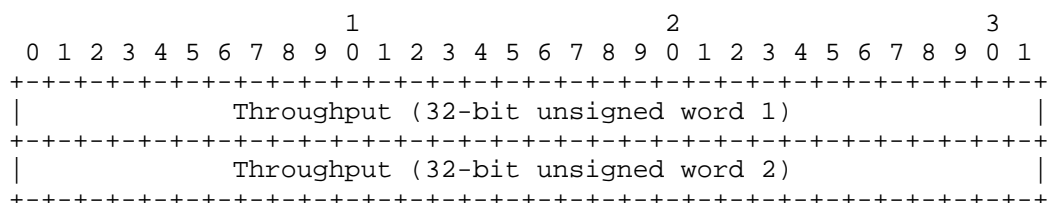


Figure 4: Node Throughput Sub-Object

A Class-Num of TBA and a C-Type of 2 are specified.

The Length is 12 if the object contains this payload. A Length value of 4 indicates that it is unavailable.



The returned value is the node-level present throughput, which is a magnitude that may be directly displayed, and is expressed in bits-per-second (bps). This allows the recipient of the ICMP message to determine a relationship between power and traffic load.

There's an in-depth discussion on why we have chosen a 64-bit object type in Section 6.

### 3. Ecolabels and Environmentally Relevant Certification (EERC) Sub-Object

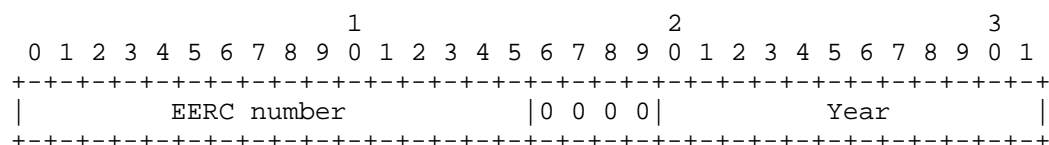


Figure 5: EERC Sub-Object

A Class-Num of TBA and a C-Type of 3 are specified.

The Length is 8 if the object contains this payload. A Length value of 4 indicates that it is unavailable.

The returned value references an Ecolabels and Environmentally Relevant Certification (EERC) number. The following EERC numbers are defined by the present specification:

1. ISO 14001:2015 [EERC-ISO14001\_2015]
2. TCO Certified [EERC-TCO]
3. Energy-efficient ethernet [EERC-EEE]

The "Year" field must contain the year in which the certificate was issued, or 0 to indicate "unknown" or "not specified".

### 4. Component-level Power Draw Sub-Object

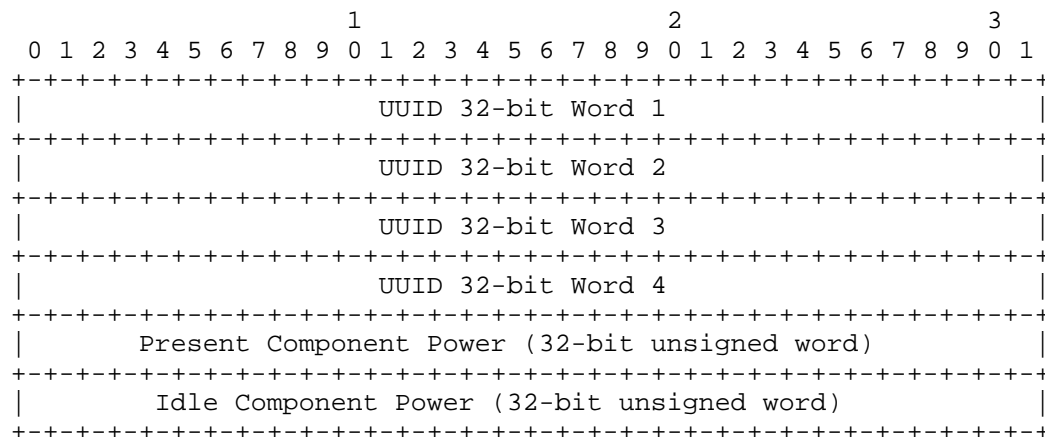


Figure 6: Component-level Power Draw Sub-Object

A Class-Num of TBA and a C-Type of 4 are specified.

The Length is 4 plus 24 times the number of elements included. A Length value of 4 indicates that this object is unavailable.

The returned value is one or more instances of component-level power drawn metrics. Each instance is a set comprised by a UUID [RFC4122] uniquely identifying the component, and the Present Component Power and Idle Component Power fields. The Present Component Power is the component-level power being presently drawn, which is a magnitude that may be directly displayed, and is expressed in Watts (W). A value of 0 indicates that the Present Component Power is not available. The Idle Component Power is the component-level power when the component is idle. A value of 0 indicates that the Idle Component Power is not available.

## 5. Component-level Throughput Sub-Object

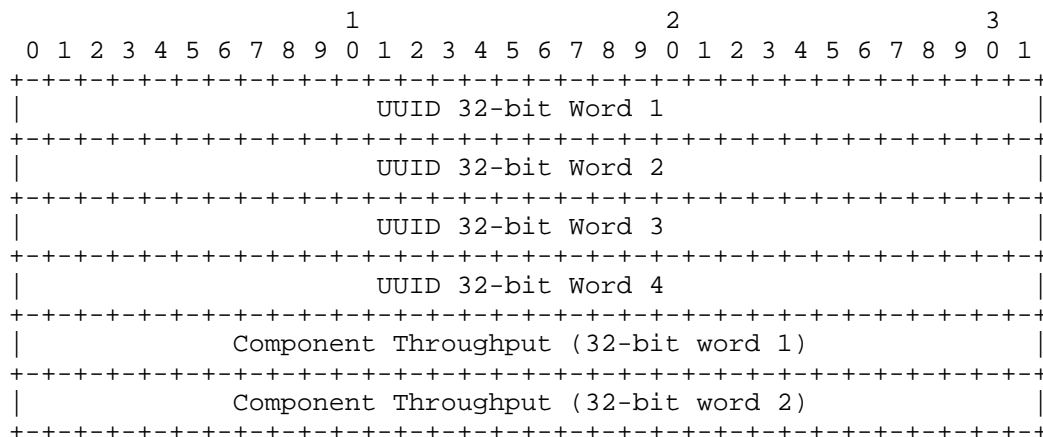


Figure 7: Component-level Throughput Sub-Object

A Class-Num of TBA and a C-Type of 5 are specified.

The Length is 4 plus 24 times the number of elements included. A Length value of 4 indicates that this object is unavailable.

The returned value is one or more instances of component-level throughput. Each instance is a set comprised by a UUID uniquely identifying the component, and the actual throughput of said component in bits-per-second (bps). This allows the recipient of the ICMP message to determine a relationship between power and traffic load.

There's an in-depth discussion on why we have chosen a 64-bit object type in Section 6.

## 6. Sub-Object Formats

As discussed in Section 5.2, we have chosen 64-bit sub-objects to accommodate the present trends of the industry with respect to high density ports/components and nodes. Organizations now have components/interfaces/line cards with 100/400/800Gbps throughput and nodes with a combined throughput exceeding 10Tbps. This cannot be represented in a field which is only 32-bit long. A 32-bit field can only represent a max throughput of 4Gbps ( $2^{32}$  bps). To address this, we define a "wider" 64-bit Sub-Object format.

We could have defined both the "wide" (64-bit) and "short" (32-bit) variants and leave it up to the device (node) to choose one over the other based on the size requirements of the data; this could make the final packet space efficient, but it would be harder to implement, as

a node would have to make an extra check to decide what kind to choose from (wide or short). Hence, for the ease of implementation, we have decided to just define a 64-bit sub-object where we need one, and skip defining a 32-bit sub-object for information like throughput, etc.

## 7. Sample Use Case

The ICMP extension defined in this memo can be used to get environmental information, either via a "transactional" or a "scheduled automated" fashion, inside an administrative domain. This section presents a sample "transactional" use case of how these pieces of information could be displayed to a user. Since both traceroute and ping utilities are based on ICMP, we will use traceroute as an example.

The flavor of traceroute that has been shown here supports the ICMP extensions and is capable of conveying to the end user the environmental information in the extensions, along with the nodes that the original datagram visited on its way to the destination. This traceroute is also backwards-compatible, i.e., it can also work well with those nodes which do not support these ICMP extensions.

A user at a host with an IP address 198.51.100.27 executes a traceroute to 192.0.2.1 and the Figure 8 shows how the user can be presented with these different pieces of information:

```

> traceroute 192.0.2.1
Tracing route to 192.0.2.1 over a maximum of 30 hops

 1 3 ms 1 ms 2 ms 203.0.113.118
 Present Power(Node=160W,Fan=7W)
 Idle Power(Node=152W,Fan=7W,Chassis=10W)
 Throughput(53687091200bps)
 EERC(ISO 14001:2015, Energy-efficient ethernet)

 2 12 ms 9 ms 9 ms 192.0.2.9
 Present Power(Node=163W,Fan=8W,Chassis=11W)
 Throughput(55834574848bps)
 EERC(ISO 14001:2015)

 3 12 ms 9 ms 9 ms 192.0.2.17

 4 7 ms 4 ms 7 ms 192.0.2.122
 Idle Power(Node=150W,Chassis=9W)
 Throughput(51539607552bps)
 EERC(ISO 14001:2015, Energy-efficient ethernet)

 5 4 ms 3 ms 3 ms 192.0.2.1

Trace complete.

```

Figure 8: Environmental-Information Infused Traceroute

Many use cases are possible on the basis of the ICMP extensions defined in this memo; it is up to the user to decide how frequently queries are issued, when and how these metrics are reported, or which policy will guide such decisions.

## 8. Implementation Status

There is interest in the 'green networking community' to have a lightweight mechanism to provide environmental sustainability information. We are aware of a couple of implementations.

1. William Hawkins III, from the University of Cincinnati, has led an implementation called "greenmatter", found at <https://github.com/cerfcast/greenmatter>, that responds to ICMP Extended Echo Messages with Environmental Information.
2. A second implementation, which is a Python-based sender and a receiver, led by Jainam Parikh, found at <https://github.com/jmparikh/green-extension-poc>, that responds to ICMP Extended Echo Messages with Environmental Information, with an Extended Echo Reply.

- \* Receiver (receiver.py) — waits for incoming data. Requires two arguments: (0 or 1)
  - probeFlag: Tells the receiver to include the Interface Identification Object [RFC8335] in the response or not
  - greenFlag: Tells the receiver to include the Environmental Information Object (this document) in the response or not
- \* Sender (sender.py) — connects to the receiver and sends data. Simply sends an ICMP Extended Echo Request to the receiver.py

## 9. Security Considerations

The security considerations of [RFC4884] and of [RFC8335] apply to these extensions.

Upon receipt of an ICMP message, application software must check it for syntactic correctness. The extension checksum **MUST** be verified. Care should be taken, as improperly specified length attributes and other syntax problems may result in buffer overruns.

This document does not define the conditions under which a router sends an ICMP message. Therefore, it does not expose routers to any new denial-of-service attacks. Routers may need to limit the rate at which ICMP messages are sent.

The extensions defined in this document allows a router to append environmental sustainability information to multi-part ICMP messages, and therefore can provide the user of the traceroute and ping applications with additional information.

The intended field of use for the extensions defined in this document is administrative debugging and troubleshooting and operational facilities. The extensions herein defined supply additional information in ICMP responses. These mechanisms are not initially intended for other uses.

Some of the additional information provided, as e.g., power draw information, have privacy considerations. For example, behavioral considerations of the devices, or estimating other node and network attributes from the power or energy data. Other things like identification of the node, deducing node usage patterns are some more privacy concerns that can be related to the information.

Keeping these considerations in mind, we limited the scope of the transportation of the environmental information to a single administrative domain (AD). But, based on [RFC8799], limiting a protocol's functionality doesn't mean that it will be secure. So, this particular document, which defines "a modified ICMP message with

environmental information", can be classified as a FAIL-OPEN protocol [I-D.wkumari-intarea-safe-limited-domains]. That is, the interfaces of administrative domain border nodes, facing towards the open internet, can be configured such that they avoid leaking messages with extensions containing environmental information, out of the AD. To allow general ICMP messages, an administrator can configure those outward facing interfaces to not block/drop the entire message but only strip off the extension objects and only forward the ICMP message if it is destined to go out of the AD.

When environmental information are limited to the same AD, it can be considered that they can be generated from a valid source and will have integrity.

High-fidelity reporting of power draw for the targeted node's memory, cache, hardware security module, or other sensitive component could allow an attacker to perform a remote side-channel attack (i.e., using differential power analysis) during cryptographic operations. This attack would allow the adversary to extract the network node's secret key(s) or other sensitive data. There are a couple of ways of mitigating this type of attack; exclude power metrics for components that process sensitive data or provide countermeasures that introduce noise in the reported power metrics (e.g., software that demarcates sensitive data which signals the processing hardware to treat this data with algorithmic noise). The latter technique is an area of ongoing research at the time of this writing.

Finally, this document does not specify an authentication mechanism for the extension that it defines. Application developers should be aware of various ICMP attacks [RFC5927].

## 10. IANA Considerations

IANA is requested to assign the following object Class-num in the ICMP Extension Object Classes and Class Sub-types registry [IANA-ICMP-Extended]:

| Class Value | Class name                       | Reference     |
|-------------|----------------------------------|---------------|
| TBA         | Environmental Information Object | This document |

Table 1: Class-num for Environmental Information Extensions

IANA is requested to establish a registry for the corresponding class sub-type (C-Type) space, as follows:

| C-Type Value | Description                                                 | Reference     |
|--------------|-------------------------------------------------------------|---------------|
| 0            | Reserved                                                    | This document |
| 1            | Node Power Draw                                             | This document |
| 2            | Node Throughput                                             | This document |
| 3            | Ecolabels and Environmentally Relevant Certification (EERC) | This document |
| 4            | Component-level Power Draw                                  | This document |
| 5            | Component-level Throughput                                  | This document |
| 6-246        | Unassigned                                                  |               |
| 247-255      | Reserved for Experimentation                                | This document |

Table 2: C-Types for Environmental Information Extensions

C-Type values are assignable on a first-come-first-serve (FCFS) basis.

IANA is requested to establish a registry for Ecolabels and Environmentally Relevant Certification (EERC) numbers (C-Type 2), as follows:

| Number      | Name                         | Reference     |
|-------------|------------------------------|---------------|
| 0           | Reserved                     |               |
| 1           | ISO 14001:2015               | This document |
| 2           | TCO Certified                | This document |
| 3           | Energy-efficient ethernet    | This document |
| 4-65527     | Unassigned                   |               |
| 65528-65535 | Reserved for Experimentation | This document |

Table 3: EERC numbers



EERC numbers are assignable on a first-come-first-serve (FCFS) basis, and require a citation to the definition of the certification.

## 11. Acknowledgements

We are very grateful to Jari Arkko for his support, thorough review, and a useful set of comments and suggestions. We are also appreciative of the feedback, input, and interest from participants of the eimpact 2024 Interim meeting.

Thank you to Shawn Emery for providing very useful feedback and suggestions, and to William Hawkins III for a thorough review and sharing some fixes, as well as for the first implementation of this Internet-Draft, adding environmental information to ICMP messages.

## 12. References

### 12.1. 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>>.
- [RFC4884] Bonica, R., Gan, D., Tappan, D., and C. Pignataro, "Extended ICMP to Support Multi-Part Messages", RFC 4884, DOI 10.17487/RFC4884, April 2007, <<https://www.rfc-editor.org/info/rfc4884>>.
- [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>>.
- [RFC8335] Bonica, R., Thomas, R., Linkova, J., Lenart, C., and M. Boucadair, "PROBE: A Utility for Probing Interfaces", RFC 8335, DOI 10.17487/RFC8335, February 2018, <<https://www.rfc-editor.org/info/rfc8335>>.

### 12.2. Informative References

- [EERC-EEE] "IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 3: CSMA/CD Access Method and Physical Layer Specifications Amendment 5: Media Access Control Parameters, Physical Layers, and Management Parameters for Energy-Efficient Ethernet", IEEE Std 802.3az-2010 (Amendment to IEEE Std 802.3-2008), 27 October 2010, <<https://standards.ieee.org/ieee/802.3az/4270/>>.

[EERC-ISO14001\_2015]

"ISO 14001:2015 Environmental management systems. Requirements with guidance for use", September 2015, <<https://www.iso.org/standard/60857.html>>.

[EERC-TCO] "TCO Certified", <<https://tcocertified.com/>>.

[I-D.wkumari-intarea-safe-limited-domains]

Kumari, W. A., Alston, A., Vyncke, E., and S. Krishnan, "Safe(r) Limited Domains", Work in Progress, Internet-Draft, draft-wkumari-intarea-safe-limited-domains-00, 19 January 2024, <<https://datatracker.ietf.org/doc/html/draft-wkumari-intarea-safe-limited-domains-00>>.

[IAB-EIMPACTWS]

"IAB workshop on Environmental Impact of Internet Applications and Systems (eimpactws)", December 2022, <<https://datatracker.ietf.org/group/eimpactws/>>.

[IAB-EIMPACTWS-Minutes]

"Minutes for the IAB E-Impact Workshop Session 4: Next Steps", eimpactws Session 4, 12 December 2022, <<https://datatracker.ietf.org/doc/minutes-interim-2022-eimpactws-04-202212121400/>>.

[IANA-ICMP-Extended]

"Internet Control Message Protocol (ICMP) Parameters, ICMP Extension Object Classes and Class Sub-types", <<https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml#icmp-parameters-ext-classes>>.

[RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, DOI 10.17487/RFC0792, September 1981, <<https://www.rfc-editor.org/info/rfc792>>.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <<https://www.rfc-editor.org/info/rfc4122>>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <<https://www.rfc-editor.org/info/rfc4443>>.

- [RFC5927] Gont, F., "ICMP Attacks against TCP", RFC 5927, DOI 10.17487/RFC5927, July 2010, <<https://www.rfc-editor.org/info/rfc5927>>.
- [RFC8799] Carpenter, B. and B. Liu, "Limited Domains and Internet Protocols", RFC 8799, DOI 10.17487/RFC8799, July 2020, <<https://www.rfc-editor.org/info/rfc8799>>.
- [RFC9547] Arkko, J., Perkins, C. S., and S. Krishnan, "Report from the IAB Workshop on Environmental Impact of Internet Applications and Systems, 2022", RFC 9547, DOI 10.17487/RFC9547, February 2024, <<https://www.rfc-editor.org/info/rfc9547>>.

## Authors' Addresses

Carlos Pignataro  
North Carolina State University  
United States of America  
Email: [cpignata@gmail.com](mailto:cpignata@gmail.com), [cmpignat@ncsu.edu](mailto:cmpignat@ncsu.edu)

Jainam Parikh  
Arista Networks  
5453 Great America Parkway  
Santa Clara, 95035  
United States of America  
Email: [jainam@parikhgroup.net](mailto:jainam@parikhgroup.net)

Ron Bonica  
Juniper Networks  
United States of America  
Email: [rbonica@juniper.net](mailto:rbonica@juniper.net)

Michael Welzl  
University of Oslo  
Norway  
Email: [michawe@ifi.uio.no](mailto:michawe@ifi.uio.no)