

Technical Disclosure Commons

Defensive Publications Series

June 2023

ENVIRONMENTAL-IMPACT EXTENSIONS FOR TRACEROUTE AND PING

Carlos M. Pignataro

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation

Pignataro, Carlos M., "ENVIRONMENTAL-IMPACT EXTENSIONS FOR TRACEROUTE AND PING", Technical Disclosure Commons, (June 15, 2023)

https://www.tdcommons.org/dpubs_series/5982



This work is licensed under a [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/).

This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

ENVIRONMENTAL-IMPACT EXTENSIONS FOR TRACEROUTE AND PING

AUTHORS:
Carlos M. Pignataro

ABSTRACT

The computer network diagnostic facilities traceroute and ping are arguably some of the most used networking troubleshooting tools. Augmenting those facilities to present environmental and sustainability data and metadata would contribute to gain visibility on “green metrics” on the Internet, an objective mentioned in the Internet Engineering Task Force (IETF) E-Impact initiative. Techniques are presented herein that support Environmental-Impact extensions (or “E-Impact” extensions for short) to both traceroute and ping. The presented extensions are backwards compatible and potentially provide per-hop (e.g., per networking topological node) power metrics, estimated greenhouse gas (GHG) emission numbers, and potentially other current or future sustainability metrics. Aspects of the presented techniques support a combination of in-packet (e.g., Internet Control Message Protocol (ICMP) extensions) plus out-of-band (e.g., out of band database lookup or application programming interface (API) calls from a host) methods that, together, yield the above-described new metrics. The presented techniques are useful not only in a transactional setting (e.g., a user desired to find some information so they issue a traceroute or a ping request) but they may also be run periodically in a mesh across the Internet or across an administrative domain to map out environmental-impact metrics, including energy usage, power and normalized power, and estimated GHG emissions.

DETAILED DESCRIPTION

The computer network diagnostic facilities traceroute, and ping are arguably two of the most widely used networking troubleshooting tools. Although ping was first implemented in 1983 and traceroute was first implemented in 1987, both facilities are still used today as much as any other day, and they are likely to be the first couple of commands that anyone would type when they suspect a network issue, when they want to test reachability, when they want to check on a delay, and when they want to explore a path.

Both traceroute and ping are so impeccable in their simplicity and efficiency that in over three decades they continue to utilize the same method and paradigm and have received only small changes and only minor improvements. For example, traceroute now has versions that support the embedding of different probe packets (for, as an example, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), or Transmission Control Protocol (TCP)). Additionally, the multi-part extensions that are described in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 4884 support the “piggybacking” (i.e., the carrying back to the originator) of metadata.

The decades of stability of traceroute and ping is one of the things that makes them so useful and without match or replacement – they are so ubiquitous and built into every stack and system in interoperable ways. However, the tools of decades ago (that are still foundational to Internet control and management) face new needs today including a hugely growing need for sustainable and environmental impact protocols, networks, and stacks. This does not only mean minimizing a negative impact on the environment due to networking technologies. It also means filling a notable gap in the tools that are available to add visibility, measure, and quantify said impact.

As Peter Drucker has stated, “you can't manage what you can't measure.” However, at the December 12, 2022, Internet Architecture Board (IAB) workshop on the Environmental Impact of Internet Applications and Systems, it was noted that it may not always be possible to obtain the necessary estimated measurements for the above-described metrics, in which case it may be necessary to infer them and in certain cases predict them.

Techniques are presented herein that support novel methods for `traceroute e-impact` as well as `ping e-impact` versions and extensions. Those versions are backwards compatible and provide per-hop estimated greenhouse gas (GHG) emission numbers (under specific conditions and context) as well as energy, power and potentially other sustainability metrics. For purposes of illustration, Figure 1, below, presents elements of an exemplary traceroute display according to the techniques presented herein.

```

cpignata@CPIGNATA-M-CMGM ~ % traceroute -eimpact -M 6 -m 8 server.example.com
traceroute to server.example.com, providing e-impact data

 6 [Est.GHG:980 g CO2e / 24h] 23-255-225-180.googlefiber.net (23.255.225.180) 12.935 ms 10.207 ms 9.724 ms
 7 [Est.GHG:1321 g CO2e / 24h] 13335.ash.equinix.com (206.126.237.30) 24.159 ms 9.994 ms 10.148 ms
 8 [Power: 4822 W] 162.70.172.2 (162.70.172.2) 12.453 ms 13.398 ms 21.317 ms
cpignata@CPIGNATA-M-CMGM ~ %

```

Figure 1: Exemplary Display

There are existing attempts at providing via traceroute other sets of information.

One existing attempt encompasses in-the-wire ICMP extensions that allow a traceroute facility to display Multiprotocol Label Switching (MPLS) labels. The forwarding context of ICMP extensions showing MPLS labels, using RFC 4950, may look like the results that are shown in Figure 2, below.

```

CE-Carlos#
CE-Carlos#traceroute 6.6.6.6 source 5.5.5.5 probe 1

Type escape sequence to abort.
Tracing the route to 6.6.6.6

 1 15.1.1.1 12 msec
 2 12.1.1.2 [MPLS: Labels 201/403 Exp 0] 84 msec
 3 23.1.1.3 [MPLS: Labels 300/403 Exp 0] 92 msec
 4 46.1.1.4 [MPLS: Label 403 Exp 0] 48 msec
 5 46.1.1.6 92 msec

CE-Carlos#

CE1#traceroute 172.16.2.2 source 172.16.1.1

Type escape sequence to abort.
Tracing the route to 172.16.2.2

 1 172.16.11.2 3 msec 3 msec 3 msec
 2 10.1.111.11 [MPLS: Labels 19/24008 Exp 0] 122 msec 25 msec 19 msec
 3 10.1.211.2 [MPLS: Label 24008 Exp 0] 21 msec 16 msec 23 msec
 4 172.16.12.1 23 msec 22 msec

```

Figure 2: Existing MPLS Extensions for Traceroute -- Exemplary Display

However, in a very comprehensive traceroute implementations, traceroute-nanog, the only ICMP extensions displayed are the “MPLS label forwarding-context”, defined in the above-mentioned RFC 4950.

In other words, although there’s a baseline mechanism defined in RFC 4884, implementations only use the one specific extension defined in RFC 4950. It is also worth

noting that those are all in-the-wire metadata carried in ICMP, and then directly printed in traceroute output.

Another existing attempt encompasses out-of-band requests that glean, and print information gathered using the source Internet Protocol (IP) address of an ICMP message as the index of the information. This allows, for example, for the display of the autonomous system (AS) number that a specific hop router belongs to. This feature is advertised as performing AS path lookups for a returned addressee. An external query from the source IP address of an AS number may look like the results that are shown in Figure 3, below.

```

cpignata@CPIGNATA-M-CMGM ~ % traceroute -a -I -w 1 web27.example.com
traceroute to web27.example.com (41.203.18.62), 64 hops max, 72 byte packets
 1  [AS0] 192.168.10.1 (192.168.10.1)  5.427 ms  3.539 ms  1.762 ms
 2  [AS0] 192.168.1.1 (192.168.1.1)  3.496 ms  1.661 ms  1.552 ms
 3  [AS0] 10.26.1.218 (10.26.1.218)  6.366 ms  3.567 ms  3.537 ms
 4  * * *
 5  * * *
 6  * * *
 7  [AS16591] 23-255-225-145.fiber27.net (23.255.225.145)  16.924 ms  14.847 ms  12.893 ms
 8  * * *
 9  * * *
10  [AS46841] 100ge1-1.core1.nyc4.he.net (184.105.223.166)  25.796 ms  24.605 ms  24.701 ms
11  * [AS6939] port-channel4.core2.nyc4.he.net (184.105.64.177)  26.872 ms  24.733 ms
12  * [AS6939] port-channel11.core3.lon2.he.net (72.52.92.165)  94.241 ms *
13  [AS6939] port-channel10.core2.lon3.he.net (184.104.199.18)  97.213 ms  99.634 ms  95.087 ms
14  * * *
15  [AS46841] 100ge0-36.core2.jnb1.he.net (184.105.223.209)  261.295 ms  264.152 ms  269.487 ms
16  [AS0] xneelo-2.jinx.net.za (196.60.96.99)  262.496 ms  360.705 ms  261.059 ms
17  [AS37153] core-access-switch1.jnb1.host-h.net (197.189.193.1)  277.364 ms  263.338 ms  265.411 ms
18  [AS16637] www62.jnb2.host-h.net (41.203.18.62)  261.511 ms  259.832 ms  260.886 ms
cpignata@CPIGNATA-M-CMGM ~ %

```

```

cpignata@CPIGNATA-M-CMGM ~ %
cpignata@CPIGNATA-M-CMGM ~ % traceroute -a -I -w 1 w27.example.com
traceroute to w27.example.com (202.58.60.194), 64 hops max, 72 byte packets
 1  [AS0] 192.168.10.1 (192.168.10.1)  4.078 ms  1.526 ms  1.870 ms
 2  [AS0] 192.168.1.1 (192.168.1.1)  4.660 ms  2.068 ms  4.002 ms
 3  [AS0] 10.26.1.218 (10.26.1.218)  3.748 ms  3.781 ms  3.988 ms
 4  * * *
 5  * * *
 6  * * *
 7  [AS16591] 23-255-225-145.fiber27.net (23.255.225.145)  16.918 ms  14.111 ms  13.264 ms
 8  [AS0] 10g gabitethernet1-3.core1.atl1.he.net (198.32.132.75)  14.380 ms * *
 9  [AS6939] 00ge14-1.core1.dall.he.net (184.104.196.154)  57.654 ms  183.614 ms  33.083 ms
10  * [AS6939] port-channel9.core1.phx2.he.net (184.104.194.98)  185.142 ms *
11  [AS6939] 00ge11-2.core1.lax2.he.net (184.104.194.97)  243.152 ms  148.829 ms  177.220 ms
12  [AS46887] colocation-australia.as63956.any2ix.coresite.com (206.72.211.44)  183.214 ms  96.292 ms  75.714 ms
13  [AS45177] 45.112.244.198 (45.112.244.198)  237.954 ms  235.716 ms  235.811 ms
14  [AS45177] 45.112.244.197 (45.112.244.197)  243.243 ms  240.865 ms  239.061 ms
15  [AS45177] xe-5-2-3.cr1.sdc.nsw.au.coloau.net.au (103.52.116.157)  236.266 ms  235.916 ms  238.363 ms
16  [AS45177] ae2.cr2.adc.sa.au.coloau.net.au (103.52.116.150)  235.435 ms  234.397 ms  235.211 ms
17  [AS45177] 103.52.119.68 (103.52.119.68)  240.778 ms  233.852 ms  238.063 ms
18  [AS45177] 103.52.119.67 (103.52.119.67)  237.151 ms  236.490 ms  233.860 ms
19  * * *
20  * * *
21  [AS9667] 202.58.60.194 (202.58.60.194)  237.239 ms  240.696 ms  238.606 ms
cpignata@CPIGNATA-M-CMGM ~ %

```

Figure 3: Existing Traceroute display of AS information -- Exemplary Display

The above-described external query is performed within traceroute-nanog by consulting the Internet routing registry for IP to BGP origin AS mapping or through a whois search or a Réseaux IP Européens (RIPE) database inquiry.

In other words, this second attempt does not carry information on ICMP messages.

The techniques presented herein, which will be described and illustrated in detail in the following narrative, facilitate a type of output that is shown in Figure 4, below, through standard backwards-compatible traceroute and ping facilities using method extensions that are supported by the presented techniques.

```

cpignata@CPIGNATA-M-CMGM ~ % traceroute -eimpact -M 6 -m 8 server.example.com
traceroute to server.example.com, providing e-impact data

 6 [Est.GHG:980 g CO2e / 24h] 23-255-225-180.googlefiber.net (23.255.225.180) 12.935 ms 10.207 ms 9.724 ms
 7 [Est.GHG:1321 g CO2e / 24h] 13335.ash.equinix.com (206.126.237.30) 24.159 ms 9.994 ms 10.148 ms
 8 [Power: 4822 W/Day avg.] 162.70.172.2 (162.70.172.2) 12.453 ms 13.398 ms 21.317 ms
cpignata@CPIGNATA-M-CMGM ~ %
    
```

Figure 4: Exemplary Display

A discussion of the techniques presented herein may begin with the illustrative arrangement that is shown in Figure 5, below.

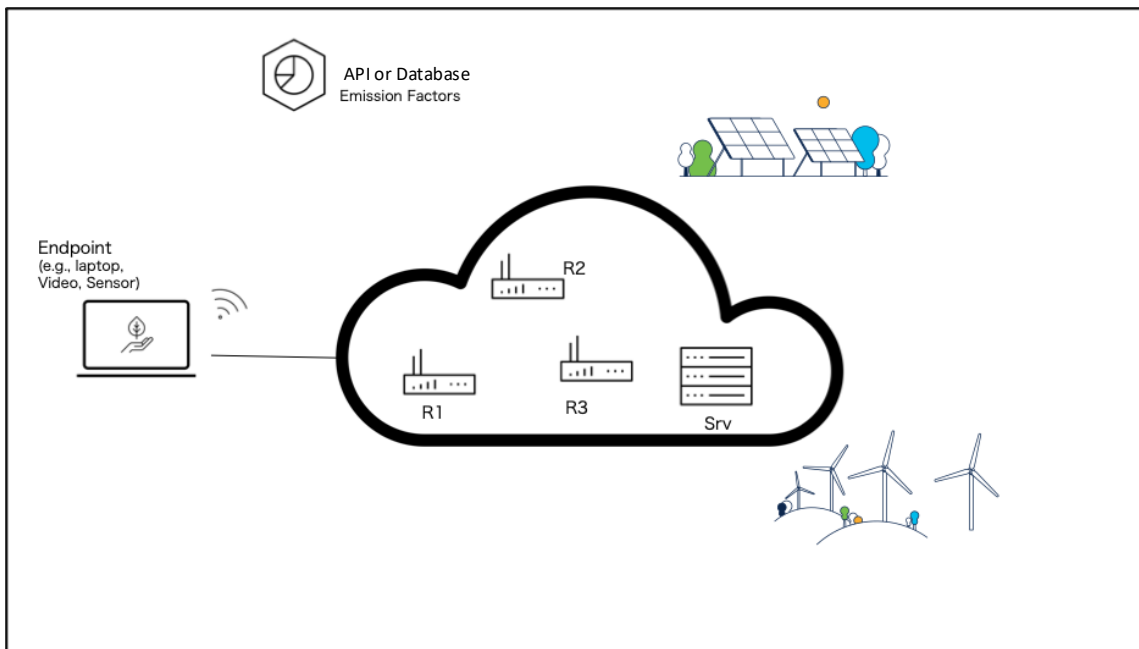


Figure 5: Illustrative Arrangement

Figure 5, above, depicts a computer network comprising Routers R1, R2, and R3 and a set of servers that reside in Srv. The network also includes an endpoint such as a laptop (or a thermostat, etc.) that originates a traceroute command and a remote database (of, for example, emission factors or carbon intensity) that may be queried through application programming interfaces (APIs). Additionally, the figure shows how energy may be produced through a diverse set of sources.

Using the arrangement that was shown in Figure 5, above, a first step according to the techniques presented herein may be understood through Figure 6, below.

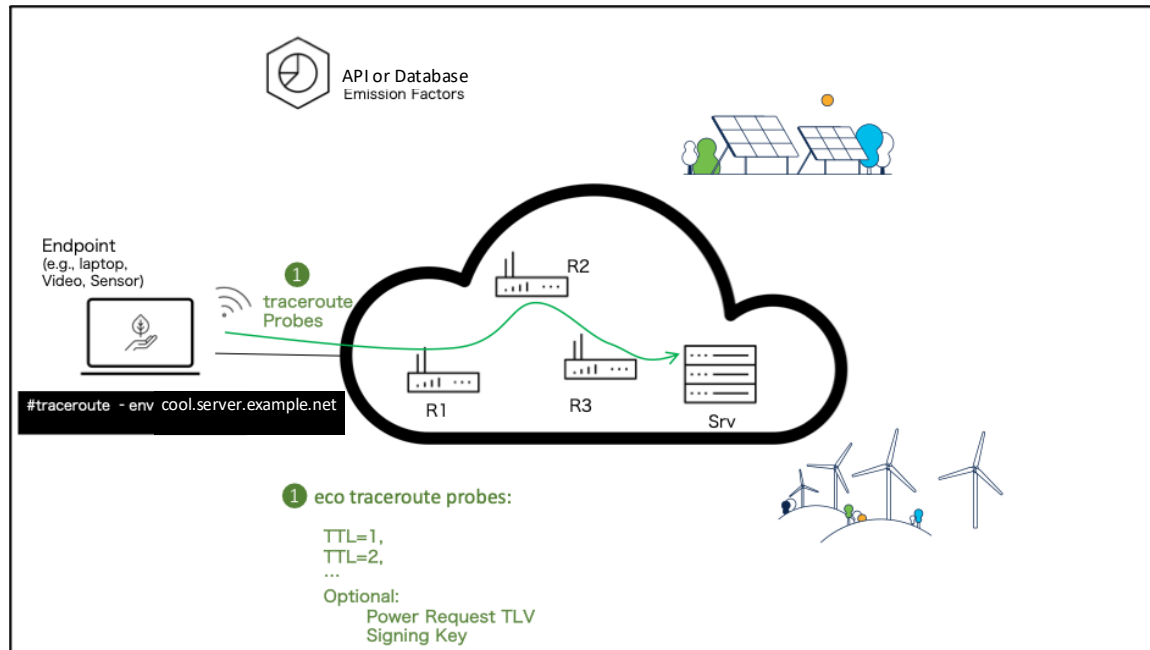


Figure 6: First Step – Traceroute Command

As shown in Figure 6, above, during a first step an endpoint executes a traceroute command requesting Environmental-impact and sustainability extended data. The request includes a set of probes on the traceroute request packet and the incrementing of a time to live (TTL) or hop limit (HL) value to elicit a response in successive hops. It is important to note that this represents a traditional traceroute approach.

According to one approach of the techniques presented herein, although this is not the default, the request packet itself can encode an entreat for sustainability data along with a signature and authentication.

The techniques presented herein also support the case where a request for power and sustainability data in a probe packet is processed on an error condition. The specific mechanism and encoding is less relevant provided that one is agreed upon, and one possible approach is discussed in the IETF Internet-Draft draft-shen-udp-traceroute-ext-01 titled “UDP Traceroute Message Extension.”

For a traceroute facility, as packets begin expiring, they will elicit back an ICMP response. For a ping facility, as the probe Echo-Request packet reaches the destination it will elicit an Echo-Reply. The ping format may follow that of the network diagnostic tool PROBE as described in RFC 8335.

In both cases, the ICMP response that is returned may encode any extra sustainability metadata information as prescribed by RFC 4884. Figure 7, below, depicts elements of this activity.

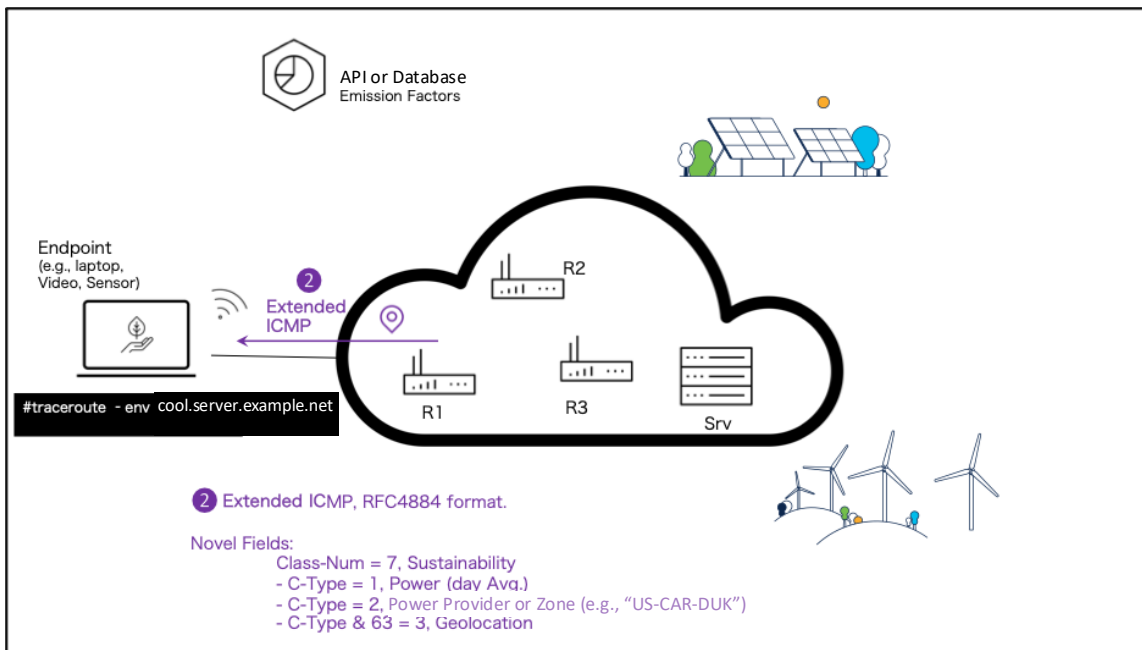


Figure 7: First Step – Extended-ICMP Traceroute Results

Each hop may respond with an ICMP message which piggy-backs sustainability information. Figure 7, above, shows elements of an extended ICMP response. A Class-Num of TBD (e.g., 7) is selected as the Internet Assigned Numbers Authority (IANA) identifies that value as unassigned. This Class-Num needs to be assigned by IANA following the registry allocation rules. Thus, within a Class-Num of TBD (e.g., 7 for e-impact and sustainability) an entire octet of fields is available to be managed as a registry.

This concept is one of encoding and piggy-backing non-forwarding information (i.e., information that is not related to the forwarding of a packet such as encapsulation, label, interface, next hop, etc.) in an error response (or an echo response) is new for e-

impact metrics and is one of the capabilities that is supported by the techniques presented herein.

The next portion of the narrative discusses some of the information that may be encoded in a reply, according to the techniques presented herein, and various ways in which that information may be utilized.

With an 8-bit C-Type value, there are potentially 256 information elements and pieces of metadata, within this Class-Num, to carry different pieces of information. This is of paramount importance on this paper, since metrics are usually changing, and in particular, specific useful e-impact metrics are being discussed. With a new field, particularly multidisciplinary, there's an asymptote of establishing useful metrics, after various are tried and argued. The techniques herein defined can be used with any specific e-impact metric in use, current or future. Further, by this paper listing exemplary metrics, it makes no implication of support of one over another.

A first piece of information encompasses a measure of power consumption on the device that is sourcing an ICMP message. This can be a device-level power number. Figure 8, below, presents elements of an ICMP Extension Object that may be employed.

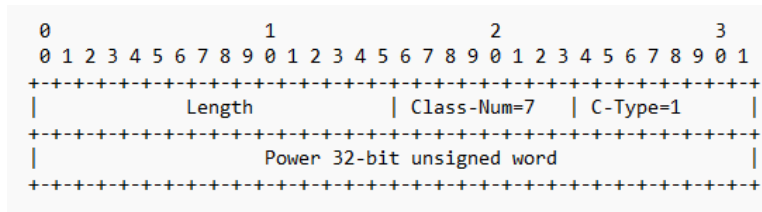


Figure 8: ICMP Extension Object – Power Consumption (e.g., day average)

As depicted in Figure 8, above, a Class-Num of 7 (TBD, exemplary for sustainability) and a C-Type of 1 (for average daily power) are specified. The returned power metric is something that may be directly displayed. Having a traceroute or ping facility that prints a per-hop power metrics is useful and is one of the capabilities that is supported by the techniques presented herein.

It is important to note that there are various metrics that can be used. These potentially include ratios such as Energy per data transmitted, Average daily Power normalized to (i.e., divided by) maximum switching capacity of the node, Kw / Gbps

without including optics, etc. Without taking position on merits or usefulness of any of these metrics, these methods allow for carrying any and all of them.

A second piece of information encompasses quantities that, indirectly, support the calculation of the “green-ness of power,” such as emission factors or carbon intensity. These are quantities that a networking node would likely not know. To acquire them, the techniques presented herein support obtaining a quantity that may be used for a second-order query to dynamically obtain such ever-changing emission factors.

A first approach to the above process involves encoding an Electrical Power Provider, Geographical Area, or Zone that may be mapped to a power provider or an area. Figure 9, below, presents elements of a partial data frame that may be employed.

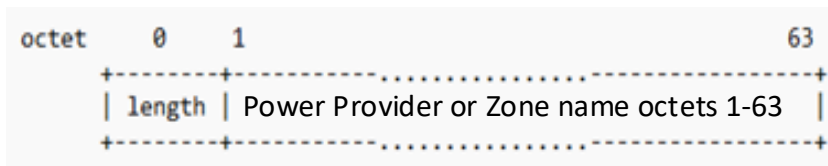


Figure 9: Data Frame – Electricity Power Provider or Zone

While not explicitly depicted in Figure 9, above, a Class-Num of TBC (7 exemplary for sustainability) and a C-Type of 2 (for an Electricity Power-Zone) are specified. Additionally, as shown in the figure, the name of a Power Provider or Zone (such as, for example, “US-CAL-EXAMPLE”) is also specified. A database (co-located or remote) or API call to a Web-service can query an Electrical Power Provider or Power Zone.

A second approach to the above process is easier and involves providing, within the ICMP extensions, geolocation coordinates which may then be mapped to an energy provider or to a specific emission factor. Figure 10, below, presents elements of an ICMP Extension Object that may be employed.

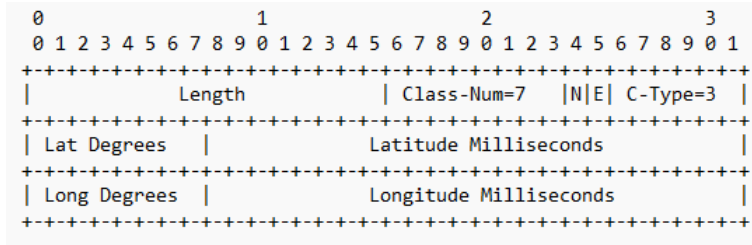


Figure 10: ICMP Extension Object – Geolocation Coordinates

As depicted in Figure 10, above, a Class-Num of TBC (e.g., 7 for sustainability) and a C-Type of 3 (using the binary mask of 00111111 with a logical AND, for geolocation) are specified.

It is important to note in the above that two bits are borrowed from the C-Type field, which is in the context of the Class-Num. Thus, C-Type values of binary XX000011 are for geolocation.

The above-described borrowed bits may be used to support two indicators – an N-bit (which when set indicates that the provided latitude is north relative to the equator and if clear indicates that the latitude is south of the equator) and an E-bit (which when set indicates that the provided longitude is east of the prime meridian and if clear indicates that the longitude is west of the prime meridian).

As shown in Figure 10, above, a Lat Degrees field contains an unsigned 8-bit integer with a range of 0 – 90 degrees north or south of the equator (i.e., the northern or southern hemisphere, respectively). A Latitude Milliseconds field then contains an unsigned 24-bit integer with a range of 0 – 3,599,999 (i.e., less than 60 minutes). Similarly, a Long Degrees field contains an unsigned 8-bit integer with a range of 0 – 180 degrees east or west of the prime meridian. A Longitude Milliseconds field contains an unsigned 24-bit integer with a range of 0 – 3,599,999 (i.e., less than 60 minutes).

The techniques presented herein support the novel approach of responding in a networking tool with a proxy for emission factors or carbon intensity through location details.

Using either geolocation or location zone information (as described and illustrated above) it is possible to obtain (through Web Service APIs or through local or remote static databases) a value for emission factors. An example of source of emission factors is the

“GHG Emission Factors Hub” at the U.S. Environmental Protection Agency (EPA), reachable at <https://www.epa.gov/climateleadership/ghg-emission-factors-hub>. Figure 11, below, depicts elements of this activity.

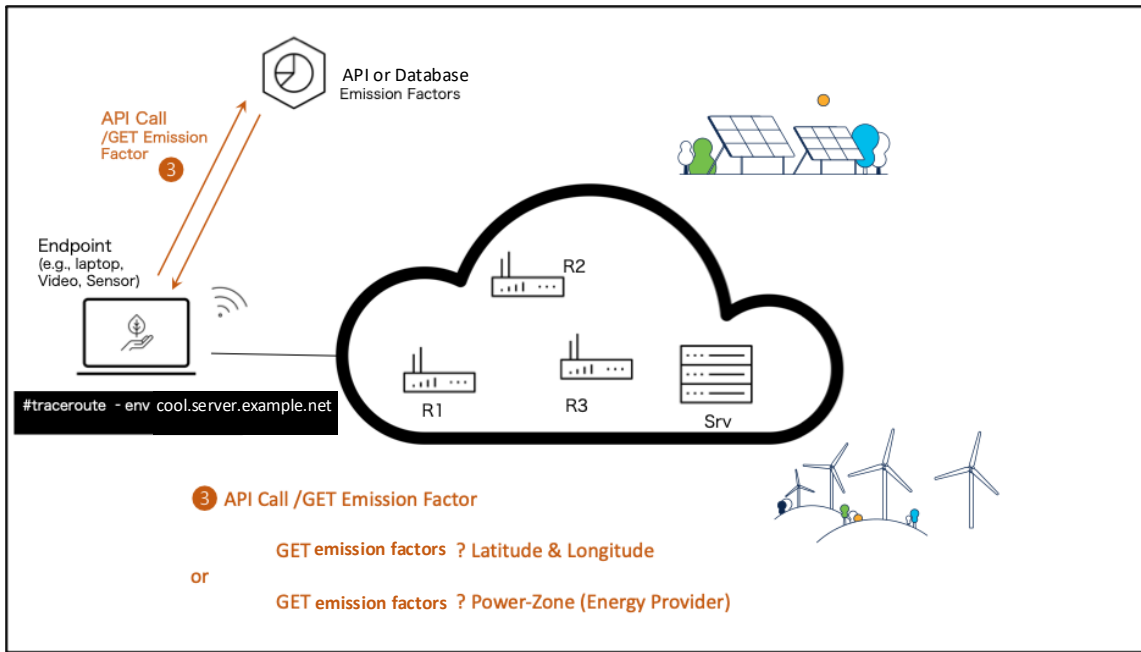


Figure 11: Carbon Intensity

Figure 11 shows a specific API call to get emission factors, which is advantageous to get real-time numbers (as for example differentiating electricity production during day or at night).

An exemplary Webservice API call can look like this, in which for a given location by latitude and longitude coordinates, the user obtains a value of “342”:

```
carlos@server ~ % curl -- request GET \
--url'https://webservice.greenness.example.org/emission-
factors/latest?lat=35.79158&lon=-78.7811' \
-header 'X- KEY: myverydifficultsecretauthenticationtoken' --silent |
jq .EmissionFactors
342
carlos@server ~ %
```

That said, any way to glean the emission factors that is not carried in the packet itself (e.g., checking locally a downloaded version of the EPA database) will suffice.

Employing the GHG protocol standard formulas and continuing with the example that was presented above, it is possible to finally calculate an estimate of the GHG measures and display the full traceroute output.

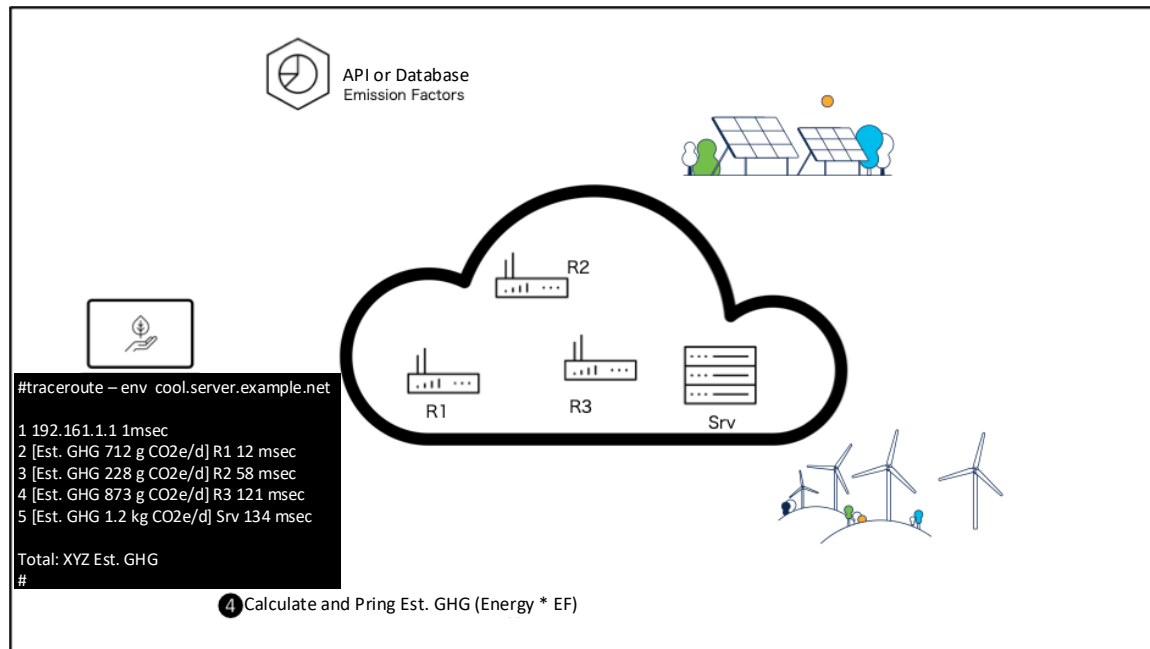


Figure 12: Illustrative Environmental-Impact Traceroute Output

As shown in Figure 12, above, the traceroute output, as augmented according to the techniques presented herein as described and illustrated above, comprises:

```
#traceroute -env cool.server
1 192.168.1.1 1msec
2 [Est. GHG 712 g CO2e/d] R1 12 msec
3 [Est. GHG 228 g CO2e/d] R2 58 msec
4 [Est. GHG 873 g CO2e/d] R3 121 msec
5 [Est. GHG 1.2 kg CO2e/d] Srv 134 msec

Total: XYZ Est. GHG
#
```

Importantly, as described and illustrated in the above narrative, the techniques presented herein support a combination of in-the-wire methods plus out-of-band methods

to bring together a direct metric (i.e., power consumption) and an indirect metric (i.e., location details being used to develop an emission factor).

In summary, techniques have been presented that E-Impact extensions to both traceroute and ping. The presented extensions are backwards compatible and provide per-hop estimated GHG emission numbers as well as power and potentially other sustainability metrics. Aspects of the presented techniques support a combination of in-packet (e.g., ICMP extensions) plus out-of-band (e.g., database lookup or API calls from the originating host) methods that, together, yield the above-described new metrics. The presented techniques are useful not only in a transactional setting (e.g., a user needs to find some information so they issue a traceroute or a ping request) but they may also be run periodically in a mesh across the Internet or across an administrative domain to map out estimated GHG emissions.