Getting Ready for Energy-Efficient Networking
Internet-Draft
Intended status: Informational
Expires: 7 January 2026

R. C. Sofia
D. Ali
fortiss GmbH

6 July 2025

Energy-aware Differentiated Services (EA-DS)
draft-sofia-green-energy-aware-diffserv-00

Abstract

This document proposes to extend the Differentiated Services (DiffServ) Quality of Service (QoS) model to support energy-efficient networking. As a first draft, it discusses how such extensions could be done, bringing first examples of energy-efficiency metrics that could be applied to mark traffic, and providing routing applicability examples by interpreting existing or experimental DSCP codepoints to represent not only traditional QoS parameters (e.g., latency, jitter), but also application-level energy sensitivity. By incorporating energy metrics into traffic classification, network devices and orchestrators can make routing and resource allocation decisions that optimize both service performance and energy consumption.

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 7 January 2026.

Table of Contents

1. Introduction

Energy efficiency and sustainability are becoming design priorities in data communications, driven by the increasing complexity of ultra-dense, heterogeneous mobile network environments and the proliferation of mobile, decentralized applications. These applications often demand not only high processing power and bandwidth, but also bounded latency guarantees. At the same time, several international efforts are aligning with global net-zero objectives, investing in energy-optimized infrastructures, relying on Artificial Intelligence (AI)-based power management, renewable energy integration, and intelligent resource allocation strategies spanning both hardware and software development. As discussed in initiatives such as GREEN and the IRTF SUSTAIN research group, there is a growing need to integrate energy awareness into the broader operation of communication networks. This includes embedding energy considerations into the routing and forwarding processes, which are traditionally optimized solely for performance metrics. In this context, the present work proposes extending Quality of Service (QoS) models by incorporating energy-specific metrics as first-class parameters. Integrating energy sensitivity into QoS models offers tangible benefits across network management and operations. However, it also introduces new challenges: how to effectively express and signal energy metrics, how to gather and interpret the required telemetry, and how to manage the trade-offs between energy savings, system complexity, and performance. To address this, this draft specifically focuses on how such integration would fit the Differentiated Services (DiffServ) model as defined in [RFC2474] and [RFC2475]. The approach is to interpret existing and experimental DiffServ Code Points (DSCP) to encode both application-level QoS requirements and energy-related constraints. By doing so, network elements such as routers, switches, and orchestrators can make resource allocation and forwarding decisions that take into account energy-sensitivity parameters, such as power consumption or CO2 footprinting. This enables a more energy-efficient network behavior without compromising service-level expectations.

1.1. 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.

1.2. Problem Statement

As networks and internet applications evolve from real-time control systems to data-intensive analytics heavily involving AI workloads, the need to manage both performance and energy efficiency during networking operations, such as routing, is becoming increasingly critical. Quality of Service (QoS) models such as the Differentiated Services (DiffServ) [RFC2474][RFC2475] offer well-established frameworks for expressing and enforcing QoS application requirements in the form of latency, jitter, packet loss, among others. However, the modern shift toward decentralized architectures, such as multi-tenant, heterogeneous, and dynamic edge-cloud environments, demands a dual operational objective: maintaining service quality while minimizing energy consumption. Applications now vary not only in their strict traditional QoS constraints, but also in their energy sensitivity and adaptability. For instance, an Internet of Things (IoT) telemetry flow may tolerate delayed or batched delivery to reduce energy use, while a control loop for an industrial system may demand immediate and high-energy processing regardless of cost. In the absence of mechanisms to signal such energy-related requirements within a QoS model like DiffServ, network elements and orchestration systems lack the information needed to make coordinated decisions that optimize for both energy and performance, while meeting application-level requirements. Enabling such integration would support dynamic, intelligent traffic handling, including energy-aware routing ("green" routing), scaling of compute resources based on traffic class, or even energy-based preemption, while still respecting application-level QoS expectations. DiffServ provides a scalable approach to classifying and prioritizing traffic using Differentiated Services Code Points (DSCP). It effectively addresses performance-related service differentiation, but, similarly to other QoS models, it is agnostic to the energy consumption of the underlying infrastructure, whether in the forwarding paths or in the compute nodes executing workloads. As such, extending DiffServ to incorporate energy-awareness is a timely and necessary evolution to support sustainable, energy-efficient, and policy-aligned networking in increasingly complex and environmentally conscious operational environments.

1.3. Scope and Applicability

The energy-aware discussion on extensions to DiffServ proposed in this document is applicable in environments where fine-grained policy enforcement, traffic classification, and telemetry-driven routing or scheduling are operationally feasible. The work is primarily applicable to multi-tenant federated edge-cloud environments where energy-sensitive networking policies are relevant. These include:

* Cloud-edge computing infrastructures, especially those integrating AI workloads or energy-constrained nodes.

* Industrial IoT environments, where specific classes of traffic (e.g., control loops vs. telemetry) exhibit distinct energy and latency requirements.

* Software-defined WANs (SD-WANs) deployments, where centralized controllers manage QoS and routing policies.

* Federated edge-cloud platforms, such as those based on CODECO, where energy efficiency is a key orchestration objective.

These scenarios typically involve DSCP marking and enforcement at ingress points, real-time or periodic energy/load telemetry collection, and centralized or distributed routing logic. The proposed approach assumes that DSCP markings are respected across the path and that telemetry is exposed with sufficient granularity, with attention to privacy

1.4. Definitions

Latency:
: (also known as bounded latency) refers to the end-to-end transmission delay between a sender and a receiver when a traffic flow is initiated by an application. By definition, latency corresponds to the time interval between the sending of the first packet of a flow from a source to a destination and the time at which the last packet of that flow is received

Node energy, n_e(i)
: is the amount of energy (typically measured in Joules or Watts over time) consumed by a node to host, process, and serve workloads, including compute, memory, storage, and network interface activity.

Node load
: CPU, memory, or I/O resource usage that may affect dynamic energy consumption and thermal management.

Link energy, l_e(i,j)
: The amount of energy (typically measured in milliJoules per bit (mJ/bit) or Watts) consumed by the transmission of data across a network connection between two nodes, including switches, routers, and network interface cards (NICs) involved in the path.

Link load, l(i,j)
: The current traffic load (e.g., as a percentage of link capacity), which can affect both latency and energy cost.

Energy sensitivity
: A qualitative or quantitative indication of how tolerant a given application or flow is to variations in energy consumption (e.g., delay to save power, or no tolerance at all).

2. Energy-awareness and Node, Link, Path Telemetry Considerations

To enable energy-aware routing and resource management, network elements MUST have access to timely, accurate telemetry about the energy consumption and utilization characteristics of both nodes and links. This information allows the control or data plane to make informed decisions about path selection and traffic treatment based not only on traditional QoS metrics (e.g., delay, jitter, loss), but also on energy-related factors. To enforce energy-aware policies, networking nodes MUST expose telemetry on:

* Node energy.

* Node usage

* Link energy.

* Link usage

Network nodes MAY also expose telemetry on other parameters such as:

* Node power state transition (e.g., idle, transmit, receive modes).

* Other energy related metrics, such as CO2 footprint.

A combined path energy cost can be computed by aggregating both node and link energy metrics along a given forwarding path. Formulations of some of these metrics can be found in related initiatives. As a representative example, this work references node and link energy/load metrics used in the CODECO edge-cloud container orchestration framework [codeco]. While CODECO offers a practical implementation of energy metric collection and usage, the definitions and methods presented here are not exclusive to CODECO and can be generalized to other orchestration or telemetry frameworks. Hence, the metrics defined in CODECO deliverable D10 [codeco_d10] offer a compute- and network-oriented view of energy metrics and can serve as a useful reference for exploring how similar principles might be applied to DiffServ-based QoS extensions. These metrics are illustrative and not prescriptive, and alternative formulations or telemetry models

may be equally valid. Such telemetry can serve as input for policy engines or SDN controllers in future DiffServ extensions. In particular, the CODECO framework defines:

* Node energy as n_e(i): Per-node energy over time, aggregated from system sensors.

* Link energy, l_e(i,j): Dynamic energy cost for traffic across interface j of node i, derived from interface statistics and probing.

* Node usage: % of CPU available derived from interface statistics and probing.

* Link usage, l: traffic across interface j of node i, derived from interface statistics and probing.

3. Energy-aware DSCP Mapping

The DSCP field provides a 6-bit space in the IP header used to classify traffic into Per-Hop Behaviors (PHBs), as defined in [RFC2474] and further elaborated in [RFC4594]. This document proposes extending the semantics of selected DSCP values to encode energy sensitivity, in addition to traditional QoS dimensions such as latency, jitter, and packet loss. Table 1 provides a representative mapping of DSCP values to energy-aware service classes. Where possible, this mapping is aligned with the traffic classes and PHBs defined in RFC 4594, ensuring backward compatibility and operational consistency. Additionally, a subset of experimental DSCP values (from the local/experimental range) is introduced to support emerging use cases in energy-aware networking environments. Each DSCP class in the table is annotated with an intended energy sensitivity, an example use case, and a recommended policy behavior. These annotations are illustrative and meant to guide implementations that wish to leverage DiffServ for integrated energy and performance-aware traffic treatment. Experimental DSCP values (e.g., 0x2E, 0x1A, 0x0A) are intended for closed or federated environments where domain-wide agreement on codepoint interpretation is feasible. These enable finer-grained control over routing or resource scheduling policies that optimize for energy efficiency alongside service quality.

DSCP Value	PHB Name	RFC 4594 Traffic Class	Energy Sensitivity	Example Usage	Example Recommended Behaviour
46	EF	Real-Time Interactive	Ignore	VoIP, industrial	Route via path with lowest

				control	latency and jitter; energy cost not considered
34	AF41	Broadcast Video	Moderate	Real-time HD video	Prefer low-latency and low-loss paths with moderate energy awareness
26	AF31	Multimedia Conferencing	Moderate	Interactive conferencing	Route via medium-energy, lightly loaded paths to balance latency and energy-efficiency
18	AF21	High Throughput Data	High	AI/ML batch jobs, smart uploads	Prefer energy-efficient routes even if slightly higher delay; include load balancing
10	AF11	Low-Latency Data	High	Firmware updates, telemetry sync	Select underutilized, low-energy paths, tolerate variable latency
8	CS1	Background Data	Very High	Backups, logs, cold storage	Route via lowest-energy, longest-delay paths; preemptable traffic
0	BE	Best Effort	Max energy savings	Non-critical data transfer	Allow opportunistic routing; energy-efficiency maximized, no performance

					guarantee
0x2E	EXP	Experimental Use (High Priority)	Low	Secure, energy-sensitivity critical flows	Route through secure but energy-aware paths; monitored for telemetry feedback
0x1A	EXP	Experimental Balanced Load	Moderate	Distributed compute jobs	Trade-off between energy cost and congestion across nodes and links
0x0A	EXP	Experimental Energy Saver	Very High	Delay-tolerant batch processing	Explicitly prefer energy-minimizing paths; opportunistic or deferred routing

Table 1: Energy-aware DSCP Mapping Aligned with RFC 4594

4. Routing Behaviour

Network elements and orchestrators MAY implement routing and scheduling decisions that consider both the DSCP value (as a proxy for energy sensitivity) and real-time energy metrics collected from network nodes and links. A few examples based on the Figure 1 topology:

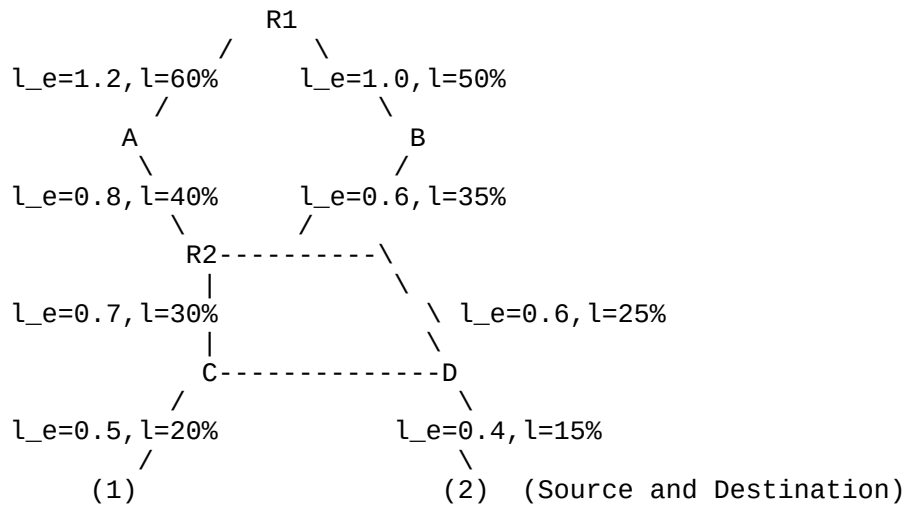

Figure 1: Example topology with link and node Energy/Load Metrics.

Where:

* (1) Source node.

* (2) Destination node

* R1, R2 routers

* A, B, C, D: Intermediate access routers/edge nodes

Between nodes, each link has the following costs:

* e = energy per bit (in mJ/bit).

* l = current load (in % usage)

4.1. Example: Minimize Link Energy

The aim is to define a policy that always selects links with lowest energy, independently of node energy or load. Here, delay-tolerant or low-priority traffic WOULD be routed via links that overall provide the minimum cumulative energy cost, independently of the node location, number of hops, or total latency.

* Selected path: 1 -- C --D --2

* Link Costs:

* 1--C: 0.5, C--D: 0.4, D--2: 0.4 = 1.3 mJ/bit total link energy
* Alternative Path (e.g., via R1): much higher link energy (1.2+1.0)
* DSCP: CS1 (8) or BE (0)
* Traffic example: Background data sync, logs

4.2. Example: Lowest Total Energy (Links and Nodes)

The aim is to define a policy that results in the selection of routes with both total lowest cumulative energy, and low utilization, considering both link and node load.

* Candidate Path: 1 --C --R2 --B --2
* Link energy: 0.5 + 0.7 + 0.6 + 0.6 = 2.4
* Node energy: C (0.6) + R2 (0.9) + B (1.0) = 2.5
* Total = 4.9 mJ/bit
* Alternative path via R1 has total energy = 6.0+ mJ/bit
* DSCP: AF31 (26) or AF21 (18)
* Traffic example: Analytics, smart batching apps

4.3. Example: Lowest Energy-Load Preference

The aim of this policy would be to consider a combination of energy and load, to ensure that traffic WOULD be routed over nodes that can offer the path with low energy and also low usage:

* Candidate Path: 1 --C --R2 --D --2
* Load: C -- 20%, R2 -- 30%, D -- 15%, links -- 25-30%
* Energy: C + R2 + D = 0.6 + 0.9 + 0.5 = 2.0 mJ (nodes)
* Links 2.0 mJ --Total 4.0 mJ
* DSCP: AF11 (10) or Experimental (0x30)
* Traffic Type: Opportunistic jobs like firmware updates or distributed computations where network and compute utilization should be minimized.

4.4. Example: No energy-awareness Preference

In this example, the DSCP marking would allow routers to ignore any energy preference, ensuring a traditional expedited treatment.

* Path Selected: 1 --C --R2 --A --R1 --B --2
* DSCP Mapping: EF (DSCP 46)
* Traffic Type: Real-time voice/video or control systems

5. Telemetry and Probing for Energy-aware Routing Considerations

Energy-aware service differentiation requires accurate, real-time insights into the state of the network, particularly with respect to energy consumption and resource load. Such insights can be gathered through two primary telemetry mechanisms: passive or active (in-band) probing.

5.1. Passive Probing

Passive probing refers to the collection of performance and usage metrics by observing ongoing traffic without modifying it. Common methods include flow monitoring (e.g., NetFlow, IPFIX), SNMP-based counters, interface statistics, and network tap-based analytics. Passive probing is advantageous due to its low intrusiveness, wide support in existing infrastructure, and suitability for long-term trend analysis. However, it typically lacks real-time granularity, does not reflect per-packet variation, and often provides limited insight into specific in-network behavior such as queuing delay or microbursts. Passive probing is beneficial to bring a fine-grained perspective on energy sensitivity based on:

* Interface energy counters (if supported by hardware)
* Node CPU/memory utilization
* Link usage

5.2. Active Probing

Active probing (or in-band telemetry) involves the use of explicit probes or modifications to data-plane packets to embed monitoring information. This includes:

* In-situ Operations, Administration, and Maintenance (IOAM) [RFC9197]

* In-band Network Telemetry (INT) using programmable data planes (e.g., P4)

* Application-layer probes for measuring latency and loss

* Synthetic probing (e.g., ping, traceroute with extensions)

Active probing allows for per-hop, per-packet collection of:

* Processing delay

* Queue depth

* Path-level latency and jitter

* Node and link identifiers

* (Optionally) energy cost annotations per segment

This level of visibility is especially valuable for adaptive, energy-aware routing decisions. For example, flows marked with energy-sensitive DSCP values may be routed dynamically based on the measured per-path energy profile, using IOAM metadata. However, in the context of edge-cloud multi-tenant, federated environments, active probing may increase the overall operational inherent to deploying a monitoring architecture across mobile, heterogeneous large-scale edge-cloud environments.

5.3. Hybrid Approaches

In practice, energy-sensitive service differentiation may benefit from a combination of passive and active mechanisms. Passive metrics can provide baseline load and energy cost estimates, while active probing offers precision feedback for high-priority or adaptive flows. Control planes (e.g., SDN controllers or orchestrators) can use telemetry to:

* Select energy-efficient paths for DSCP classes that tolerate delay

* Adjust queue policies or scheduling weights in real-time

* Trigger re-marking or flow deferral when energy thresholds are reached

Probing systems MUST ensure time-synchronization and data fidelity if they are used for per-hop energy optimization. Energy-related telemetry formats and reporting intervals SHOULD be aligned with flow-level characteristics to avoid overreaction or instability.

6. IANA Considerations

This document does not request IANA action but suggests using DSCP values in the experimental or local-use ranges for energy-aware extensions.

7. Security Considerations

Energy-aware Differentiated Services introduce several new potential attack vectors and privacy implications beyond those already present in traditional DiffServ and QoS mechanisms.

7.1. DSCP Misuse and Traffic Reclassification

This work proposes to rely on experimental DSCP values to signal energy sensitivity and influence routing and scheduling decisions. Malicious or misconfigured endpoints could falsely mark traffic to gain preferential treatment, such as being routed through energy-saving paths or low-congestion nodes. To mitigate this, networks SHOULD:

* Enforce DSCP re-marking at domain ingress (e.g., at provider or enterprise edges)

* Authenticate or validate traffic classification based on application profiles or identity

* Restrict high-sensitivity DSCP values (e.g., EF or experimental green classes) to trusted endpoints

7.2. Control Plane Manipulation

Energy-aware routing relies on telemetry and policy interpretation at centralized or distributed control planes. Attackers who gain access to these systems could manipulate:

* Energy metrics to bias routing

* Load reports to induce congestion

* Path computation engines to direct traffic inefficiently or disrupt service

Control planes MUST be protected using standard practices:

* Mutual authentication between controllers and forwarding devices

* Role-based access control (RBAC) for orchestration systems

* Secure telemetry channels (e.g., TLS, IPsec)

7.3. Privacy Preservation

Probing mechanisms, in particular active probing, may expose internal node performance, energy use, and utilization patterns. This can leak information about the network's architecture, topology, or workload behaviour. Networks SHOULD:

* Limit the telemetry scope (e.g., aggregate rather than per-packet reporting)

* Apply encryption or anonymization where telemetry crosses trust boundaries

* Use access controls for telemetry consumers and collectors

7.4. Energy Specific Threats

Manipulating energy-related behavior may not only degrade QoS but also undermine broader sustainability goals. Attackers may attempt to:

* Overload energy-efficient paths to force fallback to high-consumption infrastructure

* Create asymmetric energy drain in multi-tenant environments

* Starve critical energy-aware flows by congesting green paths

Such threats can be mitigated by:

* Incorporating energy fairness into policy logic

* Monitoring for unusual shifts in energy path usage

* Reserving minimum energy budgets for critical DSCP classes

7.5. Inter-domain Trust and Policy Consistency

In multi-domain deployments (e.g., federated edge-cloud or SD-WAN), DSCP interpretations and energy policies may vary across domains. Without consistent trust models, forwarding domains may ignore, alter, or misinterpret DSCP markings. To prevent this:

* Domains SHOULD negotiate DSCP-to-policy mappings where possible

* Border routers MUST apply local enforcement and telemetry filtering

* DSCP field usage SHOULD be aligned with IANA and IETF-recommended classes

8. References

8.1. 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>.

[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>.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, DOI 10.17487/RFC2474, December 1998, <https://www.rfc-editor.org/info/rfc2474>.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, DOI 10.17487/RFC2475, December 1998, <https://www.rfc-editor.org/info/rfc2475>.

[RFC4594] Babiarz, J., Chan, K., and F. Baker, "Configuration Guidelines for DiffServ Service Classes", RFC 4594, DOI 10.17487/RFC4594, August 2006, <https://www.rfc-editor.org/info/rfc4594>.

[RFC9197] Brockners, F., Ed., Bhandari, S., Ed., and T. Mizrahi, Ed., "Data Fields for In Situ Operations, Administration, and Maintenance (IOAM)", RFC 9197, DOI 10.17487/RFC9197, May 2022, <https://www.rfc-editor.org/info/rfc9197>.

8.2. Informative References

[codeco] C. Sofia et al., R., ""A Framework for Cognitive, Decentralized Container Orchestration," inProc. IEEE Access, vol. 12, pp. 79978-80008, 2024, doi: 10.1109/ ACCESS.2024.3406861.", 2024.

[codeco_d10]
C. Sofia et al., R., ""CODECO Deliverable D10 - Technological Guidelines, Reference Architecture, and Open-source Ecosystem Design.https://doi.org/10.5281/zenodo.12819444", 2024.

Acknowledgements

This work has been funded by The European Commission in the context of the Horizon Europe CODECO project under grant number 101092696, and by SGC, Grant agreement nr: M-0626, project SemComIIoT. We thank the following colleagues for their discussions concerning network probing and exposure as well as application workload scheduling aspects:

* Alberto del Rio, Universidad Politecnica de Madrid, for contributions for active probing.

* Kaikang Huang, fortiss, for contributions on energy-efficient network telemetry and probing

* Tina Samizadeh, fortiss, for contributions on scheduling benchmarking

* Alejandro Muniz, Telefonica, for contributions on network exposure

* Luis Miguel Contreras Murillo, Telefonica, for contributions on network exposure

Authors' Addresses

Rute C. Sofia
fortiss GmbH
Guerickestr. 25
80805 Munich
Germany
Email: sofia@fortiss.org
URI: www.rutesofia.com

Dalal Ali
fortiss GmbH
Guerickestr. 25
80805 Munich
Germany
Email: ali@fortiss.org