This document is an individual contribution to the Time-Sensitive Networking Task Group of the IEEE 802.1 working group, by Tongtong Wang and Norman Finn, and is intended to further the progress of project P802.1DF. It is not an official draft of the Task or Working Group.

# P802.1DF™/Dfw0
# Draft Standard for Time-Sensitive Networking Profile for Service Provider Networks

**Abstract:** This standard defines profiles that select features, options, configurations, defaults, protocols, and procedures of bridges and end-stations defined in IEEE Std 802.1Q and IEEE Std 802.1CB that are necessary to provide Time-Sensitive Networking (TSN) quality of service features for non-fronthaul shared service provider networks. The standard also provides use cases, and informative guidance for network operators on how to configure their networks for those use cases.

**Keywords:** IEEE 802.1Q, Time-Sensitive Networking, service provider, profile, network calculus, network slicing, hard partitioning.

.

# Editors' forward

**<<Notes>>**

<<Throughout this document, all notes such as this one, presented between angle braces, are temporary notes inserted by the Editors for a variety of purposes; these notes and the Editors' Foreword will all be removed prior to publication and are not part of the normative text.>>

**<<Comments and participation in 802.1 standards development**

Comments on this draft are encouraged. **PLEASE NOTE: All issues related to IEEE standards presentation style, formatting, spelling, etc. are routinely handled between the 802.1 Editor and the IEEE Staff Editors prior to publication, after balloting and the process of achieving agreement on the technical content of the standard is complete.** Readers are urged to devote their valuable time and energy only to comments that materially affect either the technical content of the document or the clarity of that technical content. Comments should not simply state what is wrong, but also what might be done to fix the problem.

Full participation in the development of this draft requires individual attendance at IEEE 802 meetings. Information on 802.1 activities, working papers, and email distribution lists etc. can be found on the 802.1 website:

http://ieee802.org/1/

Use of the email distribution list is not presently restricted to 802.1 members, and the working group has had a policy of considering ballot comments from all who are interested and willing to contribute to the development of the draft. Individuals not attending meetings have helped to identify sources of misunderstanding and am-]biguity in past projects. Non-members are advised that the email lists exist primarily to allow the members of the working group to develop standards, and are not a general forum.

All participants in IEEE standards development have responsibilities under the IEEE patent policy and should familiarize themselves with that policy. See http://standards.ieee.org/about/sasb/patcom/materials.html.

Comments on this document may be sent to the 802.1 email exploder, to the editors, or to the Chairs of the 802.1 Working Group and Time-Sensitive Networking Task Group.

Tongtong Wang
Email: tongtong.wang@huawei.com

Norman Finn
Email: nfinn@nfinnconsulting.com

János Farkas
Chair, 802.1 Time-Sensitive Networking Task Group
Email: janos.farkas@ericsson.com

Glenn Parsons
Chair, 802.1 Working Group
Email: glenn.parsons@ericsson.com

**PLEASE NOTE: Comments whose distribution is restricted in any way cannot be con-sidered, and may not be acknowledged.** >>

**<<The draft text and accompanying information**

This document currently comprises:

—A title page for the proposed standard including an Abstract and Keywords. This title page will be retained following working group approval of this draft, i.e. prior to sponsor ballot.

—The editors’ forewords, including this text. These include an unofficial and informal appraisal of history and status, introductory notes to each draft that summarize the progress and focus of each successive draft, and requests for comments and contributions on major issues.

—IEEE boilerplate text.

—A record of participants (not included in early drafts but added prior to publication).

—The introduction to this standard.

—The proposed standard proper.

—An Annex Z comprising the editors’ discussion of issues. This annex will be deleted from the document prior to sponsor ballot.

During the early stages of draft development, 802.1 editors have a responsibility to attempt to craft technically coherent drafts from the resolutions of ballot comments and the other discussions that take place in the working group meetings. Preparation of drafts often exposes inconsistencies in editors instructions or exposes the need to make choices between approaches that were not fully apparent in the meeting. Choices and requests by the editors’ for contributions on specific issues will be found in the editors’ introductory notes to the current draft, at appropriate points in the draft, and in Annex Z. Significant discussion of more difficult topics will be found in the last of these.

The ballot comments received on each draft, and the editors’ proposed and final disposition of comments, are part of the audit trail of the development of the standard and are available, along with all the revisions of the draft on the 802.1 web site (for address see above).

>>

<< **Introductory notes to P802.1DF Draft NWF0**

Draft NWF0 was prepared by Tongtong Wang and Norman Finn to further the progress of P802.1DF. Everything in this draft can be considered a contribution to the Time-Sensitive Networking Task Group by the authors; nothing has been approved by the Task Group or Working Group.

>>

**<< Project Authorization Request, Scope, Purpose, and Five Criteria**

A PAR (Project Authorization Request) for P802.1DF was approved by the IEEE Standards Association on February 8, 2019. The following information is taken from the 802.1DF PAR and Criteria for Standards Development.

**Scope of Proposed Project:**

This standard defines profiles of IEEE Std 802.1Q and IEEE Std 802.1CB that provide Time-Sensitive Networking (TSN) quality of service features for non-fronthaul shared service provider networks. The standard also provides use cases, and informative guidance for network operators on how to configure their networks for those use cases.

**Purpose of Proposed Project:**

Service provider networks often support multiple users and applications, and can benefit from TSN Quality of Service (QoS) bridging features defined in IEEE Std 802.1Q. This standard provides guidance for configuration of QoS features to provide dependable bandwidth and bounded latency.

**Need for the Proposed Project:**

Next generation transport networks that have more stringent QoS requirements would benefit from TSN QoS features. For example, next generation mobile networks will have an order of magnitude more cells than present networks, making it essential for multiple carriers (applications/users) to share network resources of a physical infrastructure. The fronthaul use cases are already addressed by IEEE Std 802.1CM. QoS partitioning among applications or customers will enable high-value services that have stringent bandwidth and latency requirements to efficiently share the network with best effort services.

**1. IEEE 802 criteria for standards development (CSD)**

**The CSD documents an agreement between the WG and the Sponsor that provides a description of the project and the Sponsor's requirements more detailed than required in the PAR. The CSD consists of the project process requirements, 1.1, and the 5C requirements, 1.2.**

**1.1 Project process requirements**

**1.1.1 Managed objects**

**Describe the plan for developing a definition of managed objects. The plan shall specify one of the following:**

a) **The definitions will be part of this project.**

b) **The definitions will be part of a different project and provide the plan for that project or anticipated future project.**

c) **The definitions will not be developed and explain why such definitions are not needed.**

Item c) The definitions of managed objects will not be developed because the proposed standard will specify only profiles that use managed objects already defined in other IEEE 802 standards.

**1.1.2 Coexistence**

**A WG proposing a wireless project shall demonstrate coexistence through the preparation of a Coexistence Assurance (CA) document unless it is not applicable.**

a) **Will the WG create a CA document as part of the WG balloting process as described in Clause 13? (yes/no)**

b) **If not, explain why the CA document is not applicable.**

Item b). A CA document is not applicable because this is not a wireless project

**1.2 5C requirements**

**1.2.1 Broad market potential**

**Each proposed IEEE 802 LMSC standard shall have broad market potential. At a minimum, address the following areas:**

a) **Broad sets of applicability.**

b) **Multiple vendors and numerous users.**

The market for next generation service provider networks, e.g. mobile networks, will be very large. IEEE 802.1Q can provide bounded latency and zero congestion loss Quality of Service features. This makes it likely that IEEE 802 technologies can gain a significant share of the next generation service provider market.

b) A number of vendors and operators have expressed their support for a non-fronthaul service provider network profile of IEEE 802.1 Time-Sensitive Networking.

**1.2.2 Compatibility**

**Each proposed IEEE 802 LMSC standard should be in conformance with IEEE Std 802, IEEE 802.1AC, and IEEE 802.1Q. If any variances in conformance emerge, they shall be thoroughly disclosed and reviewed with IEEE 802.1 WG prior to submitting a PAR to the Sponsor.**

a) **Will the proposed standard comply with IEEE Std 802, IEEE Std 802.1AC and IEEE Std 802.1Q?**

b) **If the answer to a) is no, supply the response from the IEEE 802.1 WG.**

a) Yes, this standard will comply with IEEE Std 802, IEEE Std 802.1AC and IEEE Std 802.1Q.

b) Not applicable.

**The review and response is not required if the proposed standard is an amendment or revision to an existing standard for which it has been previously determined that compliance with the above IEEE 802 standards is not possible. In this case, the CSD statement shall state that this is the case.**

**1.2.3 Distinct Identity**

**Each proposed IEEE 802 LMSC standard shall provide evidence of a distinct identity. Identify standards and standards projects with similar scopes and for each one describe why the proposed project is substantially different.**

The proposed standard will address service provider networks other than fronthaul networks, which are already addressed by IEEE Std 802.1CM. There are no other 802 standards or approved projects that specify time-sensitive networking for non-fronthaul service provider networks.

**1.2.4 Technical Feasibility**

**Each proposed IEEE 802 LMSC standard shall provide evidence that the project is technically feasible within the time frame of the project. At a minimum, address the following items to demonstrate technical feasibility:**

a) **Demonstrated system feasibility.**

b) **Proven similar technology via testing, modeling, simulation, etc.**

a) The proposed standard will specify profiles for the use of other IEEE 802 standards for which system feasibility has been demonstrated.

b) The proposed standard will specify profiles for the use of other IEEE 802 standards for which the technology has been proven.

**1.2.5 Economic Feasibility**

**Each proposed IEEE 802 LMSC standard shall provide evidence of economic feasibility. Demonstrate, as far as can reasonably be estimated, the economic feasibility of the proposed project for its intended applications. Among the areas that may be addressed in the cost for performance analysis are the following:**

**a) Balanced costs (infrastructure versus attached stations).**

**b) Known cost factors.**

**c) Consideration of installation costs.**

**d) Consideration of operational costs (e.g., energy consumption).**

**e) Other areas, as appropriate.**

a) The well-established cost balance between infrastructure and attached stations will not be changed by the proposed standard.

b) The cost factors are known for the IEEE 802 standards that this specification references.

c) There are no incremental installation costs relative to the IEEE 802 standards that this specification references.

d) There are no incremental operational costs relative to the existing costs associated with the IEEE 802 standards that this specification references

e) No other areas have been identified.

>>

**<< IEEE boilerplate from the Word template goes here. Disclaimers, laws, copyrights, lists of participants, Introduction, etc. >>**

# Contents

<After draft body is complete, select this text and click Insert Special->Add (Table of) Contents>

# Draft Standard for Time-Sensitive Networking Profile for Service Provider Networks

## 1. Overview

### 1.1 Scope

This standard defines profiles that select features, options, configurations, defaults, protocols, and procedures of bridges and end-stations defined in IEEE Std 802.1Q and IEEE Std 802.1CB that are necessary to provide Time-Sensitive Networking (TSN) quality of service features for non-fronthaul shared service provider networks. The standard also provides use cases, and informative guidance for network operators on how to configure their networks for those use cases.

### 1.2 Purpose

This standard provides guidance for equipment vendors, designers, and operators of service provider networks that are shared by multiple users and applications, and that need the TSN Quality of Service (QoS) features offered by IEEE Std 802.1Q bridges. These networks have links with a very large bandwidth-delay product. The TSN features include dependable bandwidth and bounded latency.

### 1.3 Introduction

Service provider networks, also called carrier networks, provide connectivity between access node and content sources (usually in data centers) for multiple users and applications. While 5G new technologies come into market, URLLC (Ultra Reliable Low Latency Communication) applications (e.g. vertical applications / utility networks) bring on strict latency requirements over carrier networks.

As shown in Figure 1, a typical service provider topology is like layered ring networks with sufficient redundant connections for better reliability and load balance. Usually user end stations are connected on the access ring network and multiple access rings could be linked to one aggregation ring that has larger bandwidth links. Backbone connections to the aggregation ring are not shown.

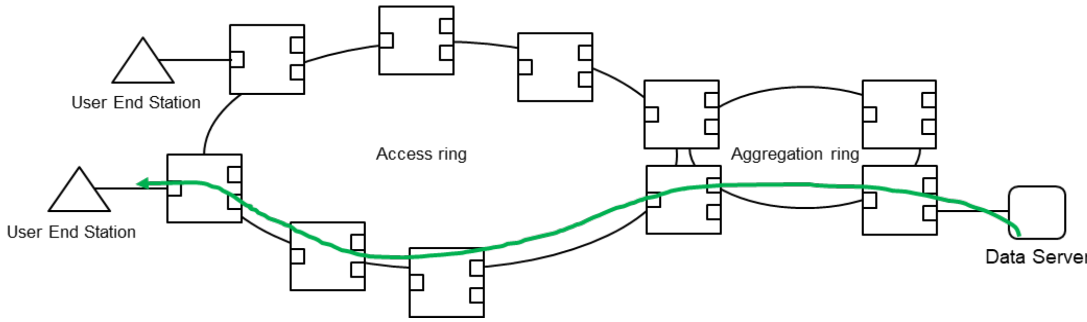


**Figure 1 Example topology of service provider networks**

To specify and explain the selection of features and options, this document:

a) Describes latency requirements for latency sensitive applications in service provider networks.
b) Describes how the operation of bridges and bridged networks affects the quality of service provided by the carrier bridged network (Clause x), provides details in the calculation of latency. (Clause …), and the potential impact of the use of flow control;
c) Specifies multiple profiles () that support the construction of bridged networks meeting latency requirements and jitter requirements.
d) Defines service provider network profile conformance requirements () for bridges meeting either profile x requirements, for end stations and for synchronization.
e) Provides a Profile Conformance Statement (PCS, Annex A) to support clear detailed statements of equipment conformance to Service provider network profile requirements.
f) Provide basic knowledge on Network Calculus to assist network latency evaluation.

# 2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 802, IEEE Standard for Local and Metropolitan Area Networks—Overview and Architecture.4, 5

IEEE Std 802.1Q, IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks.

IEEE Std 802.1CB, IEEE Standard for Local and Metropolitan Area Networks—Frame Replication and Elimination for Reliability

IEEE Std 802.1DC, IEEE Standard for Local and Metropolitan Area Networks—Quality of Service Provision by Network Systems

IEEE Std 802.3, IEEE Standard for Ethernet.

IEEE Std 802.3br, IEEE Standard for Ethernet—Amendment 5: Specification and Management Parameters for Interspersing Express Traffic.

IETF RFC xx05, (draft-ietf-detnet-ip-over-tsn) DetNet Data Plane: IP over IEEE 802.1 Time Sensitive Networking (TSN).

IETF RFC xx07, (draft-ietf-detnet-mpls-over-tsn) DetNet Data Plane: MPLS over IEEE 802.1 Time Sensitive Networking (TSN).

IETF RFC xx09, (draft-ietf-detnet-tsn-vpn-over-mpls) DetNet Data Plane: IEEE 802.1 Time Sensitive Networking over MPLS.

# 3. Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.[1]

This standard makes use of the following terms defined in IEEE Std 802:

— bridge
— end station
— Ethernet
— forwarding
— frame
— Local Area Network (LAN)

This standard makes use of the following terms defined in IEEE Std 802.1Q:

— bridged network
— latency
— port
— priority-tagged frame
— traffic class
— untagged frame
— Virtual Local Area Network (VLAN)
— VLAN Bridge
— VLAN-tagged frame

The following terms are specific to this standard:

[1]*IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

# 4. Abbreviations

ATS – Asynchronous Traffic Shaping

CBS – Credit Based Shaper

DetNet – IETF Deterministic Networking

GBR – Guarantee Bit Rate

IETF – Internet Engineering Task Force

MPLS – Multi-Protocol Label Switching

QoS – Quality of Service

RFC – Request for Comments

TAS – Time Aware Shaper

# 5. Conformance

A claim of conformance to this standard is a claim that the behavior of an implementation of a bridge (5.3, 5.4) or of an end station (5.5, 5.6) meets the mandatory requirements of this standard and may support options identified in this standard.

<< Editor's note: This profile will distinguish between an end station, on the one hand, and a router, label switch, or other network device defined by IETF, on the other, in order to link our standard to the relevant RFCs from the IETF DetNet Working Group. It is possible that this will result in a third requirement clause. >>

## 5.1 Requirements terminology

For consistency with existing IEEE and IEEE 802.1 standards, requirements placed upon conformant implementations of this standard are expressed using the following terminology:

- g) *Shall* is used for mandatory requirements;
- h) *May* is used to describe implementation or administrative choices ("may" means "is permitted to," and hence, "may" and "may not" mean precisely the same thing);
- i) *Should* is used for recommended choices (the behaviors described by "should" and "should not" are both permissible but not equally desirable choices).

The Profile Conformance Statement (PCS) proformas (see Annex A) reflect the occurrences of the words "shall," "may," and "should" within the standard.

The standard avoids needless repetition and apparent duplication of its formal requirements by using *is*, *is not*, *are*, and *are not* for definitions and the logical consequences of conformant behavior. Behavior that is permitted but is neither always required nor directly controlled by an implementer or administrator, or whose conformance requirement is detailed elsewhere, is described by *can*. Behavior that never occurs in a conformant implementation or system of conformant implementations is described by *cannot*. The word *allow* is used as a replacement for the phrase "Support the ability for," and the word *capability* means "can be configured to."

## 5.2 Profile Conformance Statement (PCS)

The supplier of an implementation that is claimed to conform to this standard shall provide the information necessary to identify both the supplier and the implementation, and shall complete a copy of the PCS proforma provided in Annex A.

## 5.3 Bridge requirements

## 5.4 Bridge options

## 5.5 End station requirements

## 5.6 End station options

# 6. Service provider networks

<< Editor's Note: This clause is a suggestion based on the presentation Suggestions for Service Provider Networks. http://www.ieee802.org/1/files/public/docs2019/df-wangtt-SP-prof-outline-0519.pdf

This clause will list a few representative use cases for service provider networks, and classify them from requirement perspective,

1. Bounded latency
2. Bounded jitter
    a. Isolation
    b. Slicing
3. Reliability

\>>

Possible emerging applications on 5G carrier networks are discussed in 3GPP TS 23.501 [B1], and summarized into three types of services shown in Table 1. Bandwidth sensitive services have strict requirement on average bandwidth and loose constraints on latency, while connection services just require message delivery from time to time. A new type of service is the delay critical service, that is the subject of this standard.

| Service Catalog | Examples | Packet delay budget | Packet loss rate | Default Max Data Burst |
|---|---|---|---|---|
| Bandwidth Sensitive Services (GBR) | Conservational Voice | 100ms | $10^{-2}$ | N/A |
| | Conversational Video (live streaming) | 150ms | $10^{-3}$ | N/A |
| | Real Time Gaming | 50ms | $10^{-3}$ | N/A |
| Connection Services (Non-GBR) | Buffered Streaming Video | 300ms | $10^{-6}$ | N/A |
| Latency Sensitive Services (Delay Critical) | Intelligent Transport Systems | 30ms | $10^{-5}$ | 1354 bytes |
| | Smart Grid Tele-protection | 5ms | $10^{-5}$ | 255 bytes |

**Table 1 Typical services in 5G carrier networks**

## 6.1 Causes of packet loss

The most common causes of packet loss can be classified, for our purposes, as:

a) Congestion: lack of buffer space for a particular frame in some network node.
b) Equipment failure: The loss of a wire or a node in the network causes some number of packets to be lost until either the failure can be corrected, or following packets can be re-routed.
c) Interference: Electromagnetic events can cause some number of packets to be lost, or received with checksum errors that cause them to be discarded.
d) Random: Random thermal or quantum mechanical events in physical interfaces or buffer memory can cause the loss of a packet, typically due to a checksum error.

## 6.2 Causes of excessive latency

The most common causes of delivery latency in excess of requirements can be classified, for our purposes, as:

a) Physical: The path of the Stream through the network can involve too many hops and/or traverse links that are too long, or have a low transmission rate.
b) Interference from other flows also requiring low latency.

High latency for a stream is seldom a goal for a network, simply because higher latency equates to additional storage for holding the packets. However, eliminating packet loss due to congestion can

## 6.3 Bandwidth sensitive services

Bandwidth sensitive services such as conversational voice usually have relaxed delay requirements over a carrier network. Currently, all such packets traverse IP DiffServ networks (Differentiated Services, [B7], [B8], [B9]) using QoS methods like strict priority, weighted round robin, etc. Since carrier networks usually have large bandwidth and are utilized in as balanced a manner as possible, traffic congestion rarely happens to high priority data streams. Bandwidth sensitive applications get satisfactory performance as long as adequate throughput and buffering capabilities are reserved and provided in time.

<<Editor Note: Consider to provide guideline on bandwidth analysis over carrier networks>>

## 6.4 Latency sensitive services

Latency sensitive services put more stringent requirements on end-to-end latency over a carrier network; any packet arriving later than a certain deadline (the tolerable deadline) is regarded as a failure of packet delivery. An example of the latency sensitive service is the smart grid tele-protection application, which requires 5 ms end-to-end latency over carrier networks with 99.999% reliability [B1].

It is important to note the difference between minimum average latency and an assurance of a finite worst-case latency. In general, the best possible average latency is obtained using simple, strict priority-based forwarding. The average latency for packets of a highest-prirotiy Stream can be very near the minimum latency. However, the worst-case latency for any given packet is generally many times larger than that minimum. Packets delivered late are equivalent to packets lost. The techniques called out in the present standard (see 6.5) are concerned with providing a finite worst-case latency. When this can be achieved, zero congestion loss is a pleasant byproduct.

<<Editor's Note: Consider to provide detailed latency evaluation method and compare multiple TSN techniques in Profiles section.>>

## 6.5 Providing the services

There are five basic data plane techniques for providing the services described in Clause 6:

a) **FRER:** Frame Replication and Elimination for Reliability.
b) **CBS:** Credit-based shaper, defined as Enhancements for Time-Sensitive Streams in 8.6.8.2 of IEEE Std 802.1Q-2018.
c) **ATS:** Per-Stream flow policing, using IEEE Std 802.1Qcr Asynchronous Traffic Shaping (ATS) and/or IETF IntServ ([B2], [B3], [B4], [B5], [B6]).
d) **Scheduled Traffic:** Timed transmission windows, using 8.6.8.4 in IEEE Std 802.1Q-2018.
e) **CQF:** Time-synchronized flow windows, using Annex T in IEEE Std 802.1Q-2018 Cyclic Queuing and Forwarding.

f) **Preemption:** Frame preemption, using 6.7.2 in IEEE Std 802.1Q-2018 and clause 99 in IEEE Std 802.3-2018.

There are other potential data plane techniques that are **not** addressed by the present standard:

g) Cut-through forwarding: The transmission of a frame is initiated before the last bit of the frame has been received and the checksum examined for errors. This document assumes store-and-forward operation.
h) Overprovisioning/prioritization: One builds a network that has significantly more physical link bandwidth that is required by the critical data, with network nodes that have a large amount of buffer space. Critical data is given the highest priority in the network, perhaps even higher than network control traffic. This works, but only when the critical traffic is a very small proportion of the total.
i) Isolation: A network is constructed for the exclusive use of one or a small number of critical applications, and this network is physically isolated from other networks.
j) Weighted fair queuing (WFQ) and other prioritization schemes: Bandwidth and resources can be allocated to be statistically fair among critical flows to minimize the impact they have on each other. This is a perfectly viable and a common technique, but has insufficiently low latency and packet loss characteristics for the present standard.
k) Congestion detection: This technique typically causes a flow that is experiencing congestion to slow down. This is not applicable for the present standard, because the applications of interest, here, typically cannot slow down the real-time physical world to accommodate the network's current load.
l) Congestion avoidance: Routes flows over less-congested network paths. This can work at the time a flow is established, but afterwards, its efficacy declines.

### 6.5.1 Frame Replication and Elimination for Reliability

Frame Replication and Elimination for Reliability (FRER) is described in IEEE Std 802.1CB. See clause 7 in IEEE Std 802.1CB-2017 for an overview of the technique. The packet replication and packet elimination techniques described in 3.2.2.2 in IETF RFC 8655 [B13] are a generalization of IEEE Std 802.1CB FRER.

FRER is aimed at packet loss due to equipment failure (point b) in 6.1) or interference (point c) in 6.1).[2] Packets in a stream are sequence numbered, then replicated, and flow along two (or more) paths to a point nearer the destination. At that point, the paths are combined into a single Stream, again. There, packet sequence numbers are compared continuously, and the duplicates eliminated. For FRER to be useful, the cost of losing packets while the network recovers from a failure must be greater than the cost of doubling the bandwidth used by the critical, replicated, Streams.

### 6.5.2 Credit-Based Shaper

The use of CBS does not provide 100% assurance against frame loss due to congestion. CBS throttles the transmission of a class of Streams (up to 7 classes per port) to the sum of the bandwidth of those Streams, at every hop along the path through the network. This throttling can prevent momentary bursts of critical data, caused by recent interference upstream, from combining to overflow the buffer capacity of a downstream node, and thus cause congestion loss (point a) in 6.1).

Assuming that a given network port has so few critical streams that each can be assigned its own one of the seven traffic classes, any given traffic class, and so any given shaper, supports more than one Stream. Interference between Streams sharing a traffic class can, in some cases, cause congestion loss. CBS has been found, in practice, to provide better packet loss characteristics than other common methods, e.g. Weighted

[2] In rare environments, where congestion loss is eliminated (by other methods), and equipment failure and interference are very rare, FRER can improve packet loss due to random events (point d) in 6.1).

Fair Queuing, but it is not perfect. It is, however, relatively cheap to implement, because it has one shaper per traffic class, instead of one per Stream.

### 6.5.3 Asynchronous Traffic Shaping

Asynchronous Traffic Shaping (ATS) is described in clause 8.6.11 of IEEE Std 802.1Qcr-2020[3]. With ATS, each Stream gets its own state machine for regulating the flow of that Stream through the network node. When ATS is implemented, an off-line network management system can compute the worst-case latency for any packet belonging to a Stream, and can compute the amount of per-Stream and/or per-class buffering needed at every hop along the path in order to assure that packet loss due to congestion (point a) in 6.1) is mathematically impossible.

### 6.5.4 Scheduled Traffic

Etc. More difficult to configure. Also solves the congestion problem.

## 6.6 Cyclic Queuing and Forwarding

Requires time synchronization. Limited flexibility. But, zero per-hop state. Solves congestion/worst-case latency problem.

## 6.7 Preemption

Non-critical traffic and perhaps, all traffic but the most critical traffic, can be preemptable. This lessens the impact of the critical traffic on the best-effort traffic. Unless there is only one critical Stream, it offers no improvement to the guaranteed worst-cast latency critical traffic; the packets cannot all preempt each other.

[3] IEEE Std 802.1Qcr will be incorporated into the next edition of IEEE Std 802.1Q following the 2019 edition of that standard.

# 7. Profiles

## 7.1 Introduction

<< Editor's Note: Suggested profiles would include:

a)

>>

## 7.2 Base Profile

<< Editor's Note: with existing TSN techniques, considering CBS, ATS, TAS, Paternoster, Strict Priority etc. >>

# 8. Interface with DetNet

## 8.1 Introduction

The Deterministic Networking Working Group (DetNet, https://datatracker.ietf.org/wg/detnet/documents/) of the Internet Engineering Task Force (IETF) has worked closely with the IEEE 802.1 Time-Sensitive Networking Task Group, by means of common participation by individuals, to generate documents that provide very similar services, for IETF routers and label switches, that TSN provides for bridged LANs. Participants have endeavored to make the TSN and DetNet documents consistent and compatible. To date, DetNet has published a number of RFCs. The one most relevant to the present IEEE standard include:

a) RFC 8557, Deterministic Networking Problem Statement;
a) RFC 8578, Deterministic Networking Use Cases;
b) RFC 8655, Deterministic Networking Architecture;
c) RFC xx01, (draft-ietf-detnet-data-plane-framework) DetNet Data Plane Framework;
d) RFC xx02, (draft-ietf-detnet-flow-information-model) DetNet Flow Information Model;
e) RFC xx03, (draft-ietf-detnet-ip) DetNet Data Plane: IP;
f) RFC xx04, (draft-ietf-detnet-ip-over-mpls) DetNet Data Plane: IP over MPLS;
g) RFC xx05, (draft-ietf-detnet-ip-over-tsn) DetNet Data Plane: IP over IEEE 802.1 Time Sensitive Networking (TSN);
h) RFC xx06, (draft-ietf-detnet-mpls) DetNet Data Plane: MPLS;
i) RFC xx07, (draft-ietf-detnet-mpls-over-tsn) DetNet Data Plane: MPLS over IEEE 802.1 Time Sensitive Networking (TSN);
j) RFC xx08, (draft-ietf-detnet-mpls-over-udp-ip) DetNet Data Plane: MPLS over UDP/IP;
k) RFC xx09, (draft-ietf-detnet-tsn-vpn-over-mpls) DetNet Data Plane: IEEE 802.1 Time Sensitive Networking over MPLS;
l) RFC xx10, (draft-ietf-detnet-yang) Deterministic Networking (DetNet) Configuration YANG Model;

<< Editor's note: We expect the referenced IETF drafts, above, to achieve RFC status by the time the present draft standard is published. We expect only RFCs to be referenced in the published IEEE standard. >>

Section 10 of RFC 8578, use cases, gives the particular example of applying DetNet to provide network slicing capability for a 5G bearer network. (See RFC 8578 for the definitions of these terms.)

## 8.2 Data plane

If a network compliant to the present standard is intended to transport DetNet traffic, or if traffic in a compliant network is to be transported over an IP or MPLS network, then it shall conform to the relevant IETF standards, including RFC xx05, RFC xx07, and/or RFC xx09.

## 8.3 Control plane

<< Editor's note: At this writing, the IETF DetNet Working Group has not made sufficient progress on the control plane (e.g. resource reservation and fixed path establishment) for the present draft to make normative references. In the opinion of the author, the issue is more narrowing down choices than designing new protocols. It is possible that there is a need to augment some IETF protocol(s) to support the Paternoster algorithm, but that algorithm has not been standardized in either IEEE or IETF, yet. There is also the possibility of implementing RAP in a router or label

switch. This has not been sufficiently explored to determine whether it is a viable idea or not. As a consequence, this section will likely point the reader to the DetNet Working Group for further information. >>

# Annex A

(informative)

# PCS Proforma—TSN for Service Provider Networks Profiles

.

# Annex B

(informative)

# A concept for network calculus

<< Editor's Note: Basis of Network Calculus will be introduced briefly. Also considering re-visit latency evaluation for existing TSN techniques, like CBS, TAS, etc. Probably leads to maintenance for 802.1Q-2018 with update on latency analysis >>

## Latency analysis based on Network Calculus (Informative)

<< Editor's Note: This clause may set an example on how to use profiles defined in this standard to setup a network to satisfy a certain use cases, such as smart grid or Cloud VR applications. >>
<< Editor's Note: briefly introduce Network Calculus methodology with examples. Illustrate how to use Network calculus to analyze delay on single node and cascaded networks.>>

Network calculus theory emerged during 1990s as a latency evaluation theory for quality of service analysis of packet switching networks, it is originally focus on performance analysis for IntServ model over IP network. Data arrivals at a networked system are modelled by upper envelope functions. Minimum service guarantees that are provided by systems, such as a router, a scheduler, or a link, are characterized by service curves. Based on these concepts, network calculus offers convolution forms that enable worst case performance bounds evaluation including backlog and delay. Any number of bridged system in series can be transformed into a single equivalent system by convolution operation and obtain end-to-end performance.

## A.1 Arrival curves

Flows can be described by arrival functions F(t) that are given as the cumulated number of bits seen in an interval[0,t]. Arrival curves are defined to give an upper bound on the arrival functions, where

$\alpha(t2\text{-}t1) = F(t2) - F(t1)$;

Token bucket based arrival curve is usually featured like in equation, $\alpha(t) = b + rt$, where b is burst size, r is data rate;

<< Editor's Note: diagram of token bucket arrival curves will be helpful in this section. >>

## A.2 Service curves

The service offered by the scheduler on an output port can be characterized by a minimum service curve, denoted by $\beta(t)$. A common service curve is described as rate-latency service curve that includes a rate R and a latency T. Service curves of the rate-latency type can be implemented by Priority Queuing (PQ) , Generalized Processor Sharing (GPS) , Weighted Fair Queuing (WFQ), and further with TSN schedulers, where bandwidth resource R is assigned to selected traffic. However, in aggregated scheduling networks resources are provisioned on an aggregate basis.

<< Editor's Note: Consider a separate section to talk about aggregating mode. >>

# Annex C

(informative)

# Network slicing

<< Editor's Note: Network slicing is essentially related to latency/jitter/reliability performance, TSN techniques provide different features and help implement network slicing over service provider networks. >>

# Annex D

(informative)

# Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] 3GPP TS 23.501 “System Architecture for the 5G System” V16.3.0.

[B2] IETF RFC 1633, “Integrated Services in the Internet Architecture: an Overview”.

[B3] IETF RFC 2211, “Specification of the Controlled-Load Network Element Service”.

[B4] IETF RFC 2212, “Specification of Guaranteed Quality of Service”.

[B5] IETF RFC 2215, “General Characterization Parameters for Integrated Service Network Elements”.

[B6] IETF RFC 2205, “Resource ReSerVation Protocol (RSVP) ”.

[B7] IETF RFC 2474, 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>.

[B8] IETF RFC 2475, Black, D., Wang, Z., Carlson, M., Weiss, W., Davies, E., and Blake, S., “An Architecture for Differentiated Services”, RFC2475, DOI 10.17487/RFC2475, December 1998, <https://rfc-editor.org/rfc/rfc2475.txt>.

[B9] IETF RFC 4594, “Configuration Guidelines for DiffServ Service Classes”.

[B10] IETF RFC 8100, “Diffserv-Interconnection Classes and Practice”.

[B11] IETF RFC 8578, “Deterministic Networking Use Cases”.

[B12] IETF RFC 8557, “Deterministic Networking Problem Statement”.

[B13] IETF RFC 8655, “Deterministic Networking Architecture”.

[B14] IETF RFC xx01, (draft-ietf-detnet-data-plane-framework) “DetNet Data Plane Framework”.

[B15] IETF RFC xx02, (draft-ietf-detnet-flow-information-model) “DetNet Flow Information Model”.

[B16] IETF RFC xx03, (draft-ietf-detnet-ip) “DetNet Data Plane: IP”.

[B17] IETF RFC xx04, (draft-ietf-detnet-ip-over-mpls) “DetNet Data Plane: IP over MPLS”.

[B18] IETF RFC xx06, (draft-ietf-detnet-mpls) “DetNet Data Plane: MPLS”.

[B19] IETF RFC xx08, (draft-ietf-detnet-mpls-over-udp-ip) “DetNet Data Plane: MPLS over UDP/IP”.

[B20] IETF RFC xx10, (draft-ietf-detnet-yang) “Deterministic Networking (DetNet) Configuration YANG Model”.

<< Editor’s note: We expect the referenced IETF drafts, above, to achieve RFC status by the time the present draft standard is published. We expect only RFCs to be referenced in the published IEEE standard. >>

# Annex Z

(informative)

# Issues