Utility Applications of Time Sensitive Networking White Paper

Authors
Ruben Salazar
Tim Godfrey
Ludwig Winkel
Norm Finn
Clint Powell
Ben Rolfe
Maik Seewald

Trademarks and Disclaimers

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-1-5044-xxxx-x STDVAxxxxx

To order IEEE Press Publications, call 1-800-678-IEEE.
Find IEEE standards and standards-related product listings at: http://standards.ieee.org

Notice and Disclaimer of Liability
Concerning the Use of IEEE-SA Documents

This IEEE Standards Association ("IEEE-SA") publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the IEEE 802.24 activity that produced this Work. IEEE and the IEEE 802.24 members expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the IEEE 802.24 members disclaim any and all conditions relating to: results; and workmanlike effort. This IEEE 802.24 document is supplied "AS IS" and "WITH ALL FAULTS."

Although the IEEE 802.24 members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE OR IEEE 802.24 MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so. IEEE and the IEEE 802.24 members make no assurances that the use of the material contained in this work is free from patent infringement. Essential Patent Claims may exist for which no assurances have been made to the IEEE, whether by participants in this IEEE 802.24 activity or entities outside the activity. The IEEE is not responsible for identifying essential patent claims for which a license may be required, for conducting inquiries into the legal validity or scope of patents claims, or determining whether any licensing terms or conditions, if any, or any licensing agreements are reasonable or non-discriminatory. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder. The policies and procedures under which this document was created can be viewed at http://standards.ieee.org/about/sasb/iccom/.

This Work is published with the understanding that IEEE and the IEEE 802.24 members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

Contents

Utility Applications of Time Sensitive Networking White Paper

How TSN could be used in a utility operational network

In the context of this white paper, the utility is considered an entity (or entities) that manage the distribution of electricity on the transmission grid and the distribution grid. The power distribution network involves substations, and various protective and control devices that communicate over communications networks.

Low latency or “real-time” performance of the network is important for specific grid use cases and applications.

The real-time behavior of Ethernet based communication networks is defined in IEC 61784-2. There are six (plus one technology specific) consistent sets of parameters described to define the requested and achieved Real-time Ethernet behavior of end-to-end stations. For the network components, using TSN is an effort ongoing in IEC SC 65C.PT61784-6, dealing with a TSN profile for industrial automation applications.

Teleprotection

Protective relays protect electrical transmission lines against fault conditions (line down, short circuits between conductors or to ground). Simple protection schemes measure voltage and current at one end of the transmission line. Differential protection schemes determine fault conditions by measuring real-time differences in voltage and current between the ends of the line. This requires an independent communication link with very low (< 10 mS) end-to-end latency to carry the measurements between the relays at the ends of the line. The communication link latency must be highly consistent and predictable. The latency requirement is less than one cycle of the ac waveform (16.6 mS or 20 mS), because time must be allowed for the mechanical operation of the relay in the case of a fault.

The communication link connection is typically fiber, although copper circuits are also used. Power Line Carrier and point-to-point microwave are less commonly used.

Intra-substation LAN

Support for IEC 61850 Generic Object Oriented Substation Event (GOOSE) messages for controlling relays and switches within the substation. TR 61850-90-13 addresses the following:

- Type of connection – typically Ethernet (copper or fiber)
- GOOSE and MMS traffic.
- TSN could be a help on the process bus.

Shared IT/OT networks over a common medium

Operational Technology (OT) networks require a controlled, predictable latency, and freedom from dropped or lost packets. This behavior is required regardless of the loading or overloading of the Information Technology (IT) network.

How does TSN affect this? The important benefit is providing a converged multi-service architecture. Critical services can have guaranteed performance and bounded latency. This saves cost by converging several networks into one.

However, not all TSN behaviors can be built in one network component without complicating the engineering. A profile for Utilities is needed to reduce the effort of engineering. IEC TC57 is looking for such a profile and is collaborating with the IEC/IEEE 60802 joint project team. IEEE Std 802.3br provides the best basis for this instead of using only shapers.

In addition to teleprotection and SCADA, voice services from field or substation locations are also a critical application. Ensuring voice traffic is unaffected by other data flow on the common network medium is a requirement for the shared IT/OT network.

Field Area Network applications

Fault Location Identification and Service Restoration (FLISR) requires predictable low latency to re-route distribution power grids to isolate faulted areas and restore power to customers so quickly that they do not notice an interruption. TSN capabilities in the FAN could be used to enable FLISR to operate on shared medium networks. The same low-latency communication with a Distributed Energy Resources Management System (DERMS) will allow local DER devices to participate in the restoration. The DERMS may be located at a central location (away from the DER equipment). End-to-end connectivity between the DERMS and the DER equipment may require multiple networks, each able to support low latency applications.

The communications requirements for supporting MicroGrids have similar low-latency needs and are further extended with the need to coordinate Dynamic protection and manage the potential for reverse power flows.

Field Area Networks are typically built on wireless technologies, although there are some instances of fiber optic networks used for communications in the distribution grid. Since TSN is currently defined for wired technologies based on IEEE Std 802.1 and IEEE Std 802.3, wireless applications are not able to support TSN directly. See the following sections for further discussion of wireless use cases.

Wind Farm applications

Wind Farms may be connected into the transmission grid or distribution grid, depending on their size and scale. Although each unit requires communication for management and monitoring, grid protection algorithms are the main driver with a requirement for low-latency communications. Integrating wind resources into a distribution grid is often part of a microgrid, which brings the set of requirements mentioned above. As with microgrids, there may be situations where TSN can provide a benefit.

AR/VR application

Augmented Reality and Virtual Reality are finding increasing use in the electric industry. Utilities are finding VR technology helpful for training, and AR can be used in the field to increase worker productivity and safety by overlaying real-time metadata over equipment being installed, operated, or serviced.

Overview of TSN functionality

TSN enables low latency, and the ability to manage maximum worst-case latency, leading to the reduction or elimination of congestion loss. It is a new optimization, compared to the (typically) best-effort packet world. It is not just low latency (on average), but a bounded, deterministic worst-case latency, that enables the applications.

TSN shifts the paradigm from acting on the packet to acting when the packet says to act. Secondarily, it can provide the ability to guard against equipment failure.

Introduction: Three kinds of packet service

Best effort packet service is familiar to users of routers and bridges. It delivers most packets, most of the time, mostly in order. There are no guarantees. Certain service classes or can be given preferential treatment over other classes or flows. Performance is statistical. If one plots a histogram (Figure 1) of the probability of delivery, end-to-end latency, or variation in latency over a given time interval, one sees long, low-probability tails on every curve. [1]

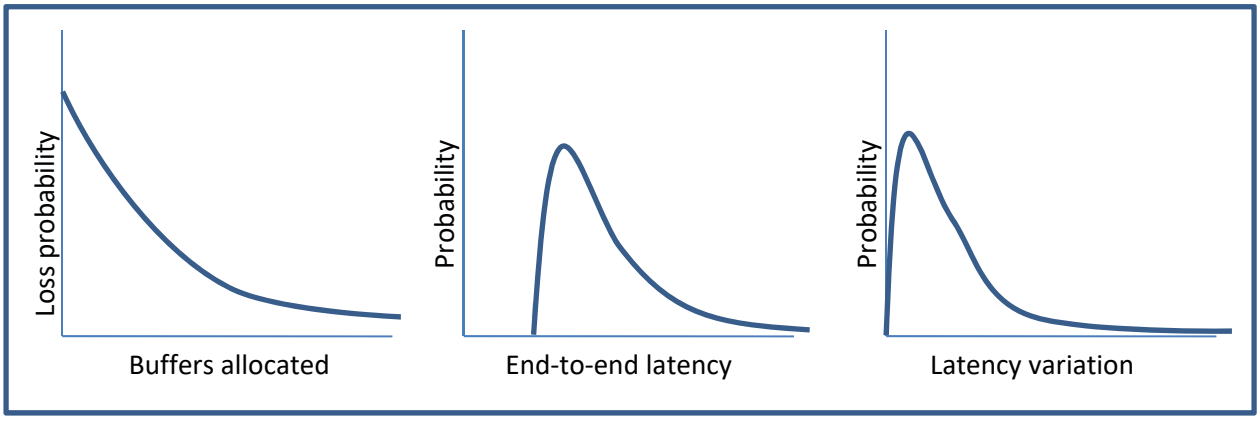

Figure 1—Best-effort packet service

Constant Bit Rate (CBR) service is typically offered by time-division multiplexing (TDM) facilities such as SDH or OTN. Latency is fixed, and jitter is essentially zero (Figure 2). The service offers connections; every packet flows end-to-end through the connection. The packet loss curve shows that CBR eliminates congestion loss, so is almost zero if the proper buffering is present. If we assume that 1+1 protection is

[1] End-to-end latency and latency variation are per packet. Loss probability is highest if few buffers are allocated, but still finite with many buffers allocated.

used, packets are lost at a low rate, but in large groups, when an equipment failure is detected and an alternate path activated.

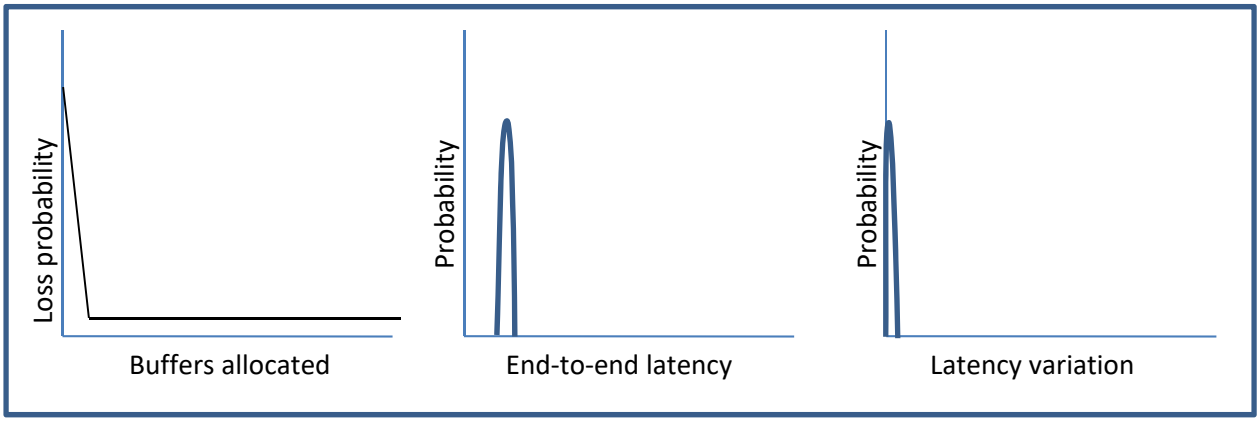

Figure 2—Constant Bit Rate packet service

Deterministic service is another kind of service that is gaining users and market attention. It is based on a best-effort packet network, but the network and an application have a contract. This contract limits the transmitter to a certain bandwidth (max packet size and max packets per time interval). The network, in return, reserves bandwidth and buffering resources for the exclusive use of these critical traffic flows. For these flows, the contracts offer bounded latency and zero congestion loss. In addition, packets belonging to a stream can be sequenced and delivered simultaneously along multiple paths, with the duplicates deleted at or near their destinations. The curves for this service are shown in Figure 3.

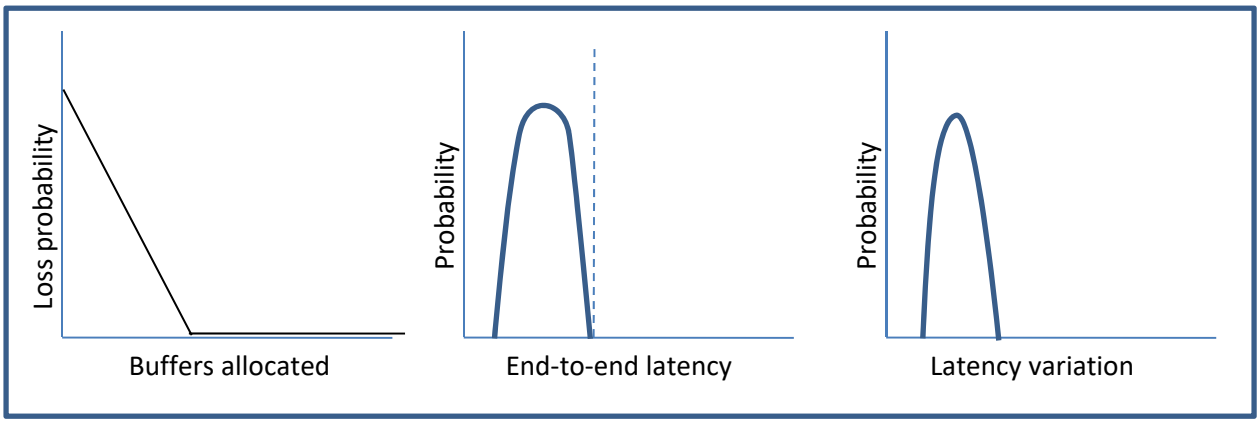

Figure 3—Deterministic packet service

The biggest differences between Figure 2 and Figure 3 is that the latency and latency variation curves have a larger range, though they are still bounded. The packet loss curve for Deterministic service has a much lower tail than the CBR curve, because Deterministic Networking uses a different protection scheme (see Packet Replication and Elimination) than the 1+1 protection usually employed in CBR. (Both services could employ either protection scheme, in which case they can have the same packet loss curve.)

Some applications are a natural fit to Constant Bit Rate (CBR) service. The original CBR services, telephony and telegraphy, are obvious examples. Some applications are a natural fit to best-effort packet service. Web browsing is typical of this usage.

Best effort services are much cheaper to deploy than CBR, and work reasonably well, even for the original CBR applications such as voice. The volume of internet traffic vastly exceeds that of voice, so best-effort has become the dominant form of digital communication.

Some applications, however, have never been able to use best-effort service. Examples are industrial control (including electrical transmission teleprotection), audio and video production, and automobile control. When these industries moved from mechanical or analog technologies to digital technologies in the 1980s, best-effort packet technologies, including Ethernet, were not suitable, so these industries had to invent special-purpose digital systems. The problem with Ethernet included its high cost, compared to special-purpose digital connections, and its inherent unpredictability. Collision detection and retransmission algorithms were not suitable for physical control systems.

Networking technology is now at the point where best-effort networking equipment can, at a modest expense, supply Deterministic services (in addition to normal best-effort services) that meet the needs of many applications that formerly required either CBR service or special-purpose digital connections. Because of the huge increase in the demand for networking, Ethernet is now cheaper than special-purpose digital connections, so there is significant incentive for these industrial and control applications to migrate to Ethernet.

Essential Features of Deterministic Networks

Deterministic Networking is a feature supplied by a network that is primarily a best-effort packet network consisting of bridges, routers, and/or MPLS label switches. The Deterministic quality of service is supplied to flows designated as being critical to a real-time application. Other than the bandwidth required for the critical traffic, the quality of the network as observed by best-effort traffic is typically not affected by the critical traffic.

The essential features of Deterministic networks are as follows:

a) Time synchronization. All network devices and hosts can synchronize their internal clocks to an accuracy between 1 µs and 10 ns. Synchronization is accomplished using some variant of the IEEE 1588 Precision Time Protocol. Most, though not all, Deterministic networking applications require that the end stations be synchronized in time. Some queuing algorithms require that the network nodes be synchronized, and some do not.
b) Contracts between transmitters and the network: Every critical flow is the subject of a contract arranged between the transmitter of the flow and the network. This enables Deterministic networks to provide the following:
    1) Bounded latency and zero congestion loss. Congestion loss, the statistical overflowing of an output buffer in a network node, is the principle cause of packet loss in a best-effort network. By pacing the delivery of packets and allocating sufficient buffer space for critical flows, congestion is eliminated. Therefore, any given critical flow can be promised a maximum latency for delivering its packet end-to-end through the network.
    2) Ultra-reliable packet delivery. Having eliminated congestion loss, the next most important cause of packet loss is equipment failure. Deterministic networks can send multiple copies of a sequence-numbered data stream over multiple paths, and eliminate the duplicates at or near the destinations. There is no cycle of failure detection and recovery–every packet

duplicated and taken to or near its destinations, so a single random event or a single equipment failure does not cause the loss of even one packet.

3) Flexibility. New contracts can be made and old ones revoked. As critical flows come and go, the proper functioning of all critical flows is maintained at all times.

c) Coexistence with best-effort services. Unless the demands of the critical flows consume too much[2] of a particular resource, such as the bandwidth of a particular link, the critical traffic can be paced so that the customary best-effort Quality of Service practices such as priority scheduling, hierarchical QoS, weighted fair queuing, random early discard, etc., still function in their usual manner, except that the bandwidth available to these capabilities reduced by the critical traffic.

The reader should note that item b)3) above, flexibility, is the most radical change to existing paradigms for supporting real-time applications over best-effort networks. All other alternatives to Deterministic Networking require network simulation, prototyping, and/or run-time testing to determine whether a change to the critical flows can or cannot be supported. Changes can only be made to such real-time networks when the applications are down. Deterministic networks can be built to support a dynamic environment.

In a sense, Deterministic Networking (DetNet) is just one more QoS offered by a best-effort network. The DetNet service provides an absolute upper bound on end-to-end latency, and at some cost in buffer space and timers, can provide a lower bound, as well. It also provides, as a natural consequence, zero packet loss due to output port congestion. The DetNet service is most useful where much of the traffic over the network as a whole is best-effort, but there is a significant component of DetNet traffic, perhaps even a majority of DetNet traffic in some parts of the network.

Understand IEC 61850 activities and relationships

IEC TC57 WG 10 (Power system IED communication and associated data models) has started to work on the Technical Report IEC 61850-90-13—Deterministic Networking Technologies (in IEC 61850 networks). The scope comprises use cases, potential improvements, key challenges, technology considerations (TSN, IETF DetNet), profile definitions, and compatibility aspects. The set of IEEE 802.1 TSN standards (profile) is in discussion and not completely decided yet. The use cases and applications are structured and mapped to the following two core domains: substation automation (Station and Process Bus) and WAN-based applications such as tele-protection and DER (Distributed Energy Resources). For substation automation networks, TSN will be considered as one solution to meet functional and non-functional requirements. The following features of TSN are especially interesting for applications and networks based on IEC 61850:

- Bounded latency
- Low bounded jitter
- Zero congestion loss
- A converged network architecture

The use of TSN-technologies comprising these key features will help to reduce the overprovisioning of network bandwidth as an approach currently used to assure delivery of critical traffic by preventing

[2] “Too much” has no fixed definition. IEEE Std 802.1 has used 75% as a design goal for the upper limit to the proportion of traffic that is Deterministic.

network congestion. According to the network architecture recommendation in IEC 61850, a substation network is partitioned into a Station and Process Bus. The Process Bus connects the IED's (Intelligent Electronic Devices) on the level of the primary equipment, typically to Merging Units (MUs). The deterministic behavior of TSN can help to foster the adoption and deployment of the Process Bus. Furthermore, non-functional requirements such as manageability, usability, and flexibility are addressed in the Technical Report (TR) as well as network security consideration. While the first three bullet points provide excellent support to meet functional requirements for critical protection and control applications, the converged network architecture enables a multi-service architecture. A multi-service architecture allows critical traffic on the same physical network with best-effort services such as network and security configuration, engineering, and monitoring. This approach is a requirement specified by utilities in order to make networking more efficient. Security monitoring as defined in IEC 62351-7 would especially benefit from the multi-service capabilities. The subsequent bullets list other important benefits and improvements:

- A tight integration with substation engineering tools to allow network configuration based on intent which hides complexity and is less prone to errors.
- High flexibility regarding the network topology and the concatenated redundancy requirements (seamless redundancy is achievable for individual streams over meshed-networks).
- Robust network security capabilities enhancing network access control, filtering, traffic segmentation, and visibility into the network. Immunity to best effort Denial of Service (DoS) attacks is implicit.
- Multi-service capabilities to allow Synchro-phasor traffic over the Station Bus and combined GOOSE and Sampled Value (SV) messages over Process Bus.

Another important aspect is guidance how to achieve co-existence and interoperability with existing technologies such as PTP (IEC 61850-9-3 Profile), PRP, and HSR. This encompasses potential impact on applications, the requirement to define migration paths and to outline support for brownfield installations. The latter point addresses the fact that today's Digital Protections Devices/IEDs do not implement a TSN-enabled network stack in order to function as a listener or talker, using the notion of TSN. On the other hand, IEDs typically have a long life-cycle (15 years and longer) and there will be a need to integrate them into a TSN-enabled network. A gateway approach addressing the specifics of IEC 61850 messages such as GOOSE and Sampled Values (SV) is in consideration. A final objective is to address new use cases and opportunities derived from the capabilities of deterministic networking.

Based on the requirements, the task force responsible for IEC 61850-90-13 is asked to coordinate the work with other working groups in IEC TC 57 (Power systems management and associated information exchange) as well as with IEC SC65C, WG 15 (High Availability Networks). Furthermore, there is close collaboration with the efforts in IEC/IEEE 60802 working on the TSN-profile for Industrial Automation. One objective is to harmonize both profiles as much as possible.

IEC 61850 is based on a layered model. The communication stack is decoupled. The layering is defined in IEC 61850-7. The layered system architecture of IEC 61850 decouples application model and services from the communication stack. This allows change to the network stack, the definition of new communication profiles, and facilitates the integration and use of the TSN-profile.

Various grid applications are based on IEC 61850. The standard series specifies the essential requirements and interfaces for these applications as well as the recommendations for a network architecture. Typical grid applications are substation automation and control (e.g., distance protection, overcurrent protection), metering, alarm and event handling, distribution automation, tele-control (SCADA), condition monitoring, synchro-phasor applications, to name a few. The core use cases

comprise substation automation systems, substation to substation, and substation to control center installations.

Time synchronization

The TSN standards assume usage of a time synchronization protocol that provides the same time to nodes in the TSN network, within a known precision and accuracy. There are a variety of uses for synchronized time, but with respect to TSN specifically, synchronized time is related to the TSN goal of providing bounded latency.

IEEE Std 1588 profiles

For packet-switched networks, one of the most commonly used standards for time synchronization is IEEE Std 1588, which specifies the Precision Time Protocol (PTP). IEEE Std 1588 specifies a variety of features for synchronization of time. For a given application, usage of PTP features will vary based on the size of the network, topology, assumptions regarding the support of PTP in all nodes, and so on. Due to this variation in needs, most PTP features are specified as optional in IEEE Std 1588. In order to accommodate the requirements of different applications, IEEE Std 1588 specifies the concept of a PTP profile. A PTP profile document specifies the set of PTP features that are required for a given application. Since the PTP profile narrows the set of features to a specific set, the PTP profile typically serves as the specification that determines interoperability from one company's product to another company's product.

As part of the family of TSN standards, the IEEE 802.1 Working Group has specified a PTP profile: IEEE Std 802.1AS. The PTP profile of IEEE Std 802.1AS applies to a LAN in which all nodes support the IEEE 802.1AS PTP profile with hardware-level timestamping. Although IEEE Std 802.1AS provides a high degree of accuracy and precision, its PTP profile does not necessarily fit all applications.

The family of TSN standards supports use of any standard for time synchronization, including any PTP profile. For example, the TSN standard for scheduled traffic (IEEE Std 802.1Qbv-2015) depends on synchronized time, but any PTP profile can be used (IEEE Std 802.1AS is not required).

Utility standardization organizations have specified PTP profiles for their applications, including IEEE Std C37.238, and IEC 62439-3 (PRP-HSR). These PTP profiles provide an excellent fit for utility applications, and either PTP profile can be used with the TSN family of standards.

Usage of synchronized time

The following lists provide example use cases for synchronized time. Each use case is an example only, and is not required in order to use TSN standards.

Application (i.e., in end nodes of network)

Timestamp of input:

This refers to measuring physical input data along with a synchronized timestamp of the measurement, and encoding both data and timestamp in a message sent over the network, for correlation and/or analysis in the receiver. Today's synchrophasor measurements are one example. TSN standards are not necessarily applicable to this example.

Timestamp to apply output data:

This refers to a TSN talker that sends data in a message to multiple TSN listeners, and the message contains a synchronized timestamp that specifies when the data is to be applied to a physical output. For example, professional audio applications use this technique to ensure that audio data is output to multiple speakers in a synchronized manner. The TSN latency bound is used to determine the timestamp for output.

Timestamp to detect stale data:

For some closed-loop control applications, data that is received late (i.e., after latency bound) is not usable. Although TSN can guarantee bounded latency for a normal configuration, there is always the possibility of a flawed configuration or a software bug. In order to validate TSN latency, the TSN talker can include a timestamp in the message that corresponds to the time of transmit. The TSN listener takes a timestamp when the message is received, and if the difference between transmit and receive time exceeds the latency bound, the listener can discard the data and take appropriate action for mitigation of the fault.

Scheduling of application code:

For closed-loop control applications in which inputs, outputs, and/or control algorithms are located in different nodes of the network, scheduling of application code helps to reduce the loop rate down to the fastest possible. Although scheduling of application code is not directly related to TSN, it does work well with certain TSN standards such as scheduled traffic.

Interior network (i.e., bridges and routers)

Scheduled traffic:

IEEE Std 802.1Qbv-2015 specifies use of synchronized time to open/close gates for each traffic class of a bridge/router. This prevents lower-priority traffic (i.e., best-effort) from interfering with TSN traffic. As with scheduling of application code, scheduled traffic provides the lowest latency bound, but when latency requirements are not tight, alternative TSN traffic standards can be used. When scheduled traffic is used, the TSN standard for traffic policing (IEEE Std 802.1Qci-2017) provides features to police the scheduled traffic to help detect faulty or malicious equipment.

Cyclic queuing and forwarding:

IEEE Std 802.1Qch-2017 specifies use of synchronized time in bridges and routers to provide a cycle-per-hop bound for latency. The bounded latency is higher than scheduled traffic, but the standard is simple to configure and use.

Relationship to IETF DETNET

The work of the IETF DETNET working group targets the same network “quality of service” (QoS) properties as TSN, namely bounded, deterministic worst-case latency that enables certain classes of applications. However, the IETF work will apply these properties to network operation at layer 3, which is the traditional purview of the IETF. The key goal of the IETF DETNET work is to utilize the common

themes of congestion control and traffic scheduling to offer bounded latency to applications with these requirements. As a layer 3 protocol, DETNET works over a routed network.[3]

Wired vs. Wireless

In addition to the common obstacles to bounded latency faced by wired networks (congestion control, resource reservation), wireless networks have additional challenges managing latency that are not faced by wired topologies, including:

- RF interference: Even if the issues of congestion control and resource reservation are solved, local RF interference can cause packets to be lost and/or require packets to be re-transmitted, causing increased latency.
- Bandwidth: Many wireless mesh networks (IEEE 802.15.4, LPWANs, etc.) have limited bandwidth, and operate at speeds in kilobits-per-second, as opposed to megabits-per-second or higher.
- Resource constraints: On wireless mesh networks, network devices will be constrained in their resources and have limited buffer space to manage congestion control.
- Mobility: For wireless networks supporting mobility, the potential for variances in RF interference are higher than wireless topologies that with fixed node location and no mobility support.
- Low-Power: In some wireless mesh topologies, there are battery-powered devices that need to limit their packet transmission rates and active duty cycle, which adds additional latency.

The wireless standards in IEEE 802 do not currently support TSN in the manner of IEEE Std 802.1 and IEEE Std 802.3. Use cases with requirements for bounded latency are accommodated through network design, frequency planning, and use of QoS. Future amendments to IEEE 802 Wireless standards could provide the functionality needed to support TSN and the IEEE 802.1 TSN standards. The examples described previously (Fault Location, Isolation, and Service Restoration or FLISR, and Microgrid control) are currently the most latency sensitive distribution grid applications. In 2018 and 2019, the IEEE 802.11 working group conducted the Real Time Applications Topic Information Group (TIG), which explored low latency for IEEE 802.11. The TIG completed in March 2019 and published a report.[4] The TIG's findings in low-latency applications and requirements will continue in the IEEE 802.11be Extremely High Throughput (EHT) task group. The IEEE 802.1 TSN architecture and features are referenced, and will be considered and potentially incorporated in the EHT amendment, with the necessary adaptations for the wireless medium.

[3] https://tools.ietf.org/id/draft-ietf-detnet-architecture-05.html.

[4] IEEE 802.11 Real Time Applications TIG Report is available at https://mentor.ieee.org/802.11/dcn/18/11-18-2009-06-0rta-rta-report-draft.docx.

Appendix 1—Standards Summary

IEEE 802.1 AVB, IEEE 802.1 TSN, and IEEE 802.3 standards

Standards listed as "IEEE Std 802.xyz-2xxx" are complete, published standards. Those listed as "IEEE P802.xyz" (note the "P") are works in progress. A given standard or work in progress can be either a stand-alone document, or an amendment to a previous standard, as indicated in the text. See the IEEE 802.1 web site for the most up-to-date information. (The time to completion shown for IEEE P802.xxx projects are minimums; they are likely to take longer.)

IMPORTANT NOTE: IEEE 802 standards must be purchased from the IEEE web site for the first six months after publication, and are available free from the GetIEEE web site after that time. IEEE 802.1 work in progress is available from the IEEE private web site, using a username and password, to anyone, IEEE member or not, interested in making helpful comments to further the work of the committee. Contact the chair of IEEE 802.1 to get the password.

A. IEEE Std 802.1AS-2011, Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks. Defines a profile of IEEE 1588 Precision Time Protocol that is 1) plug-and-play, and 2) does not use transparent clocks.

B. IEEE Std 802.1Q-2018, Bridges and Bridged Networks. The root document for VLAN bridges. Earlier AVB standards, that were originally amendments to IEEE Std 802.1Q-2011, are included in IEEE Std 802.1Q-2018:
   - IEEE Std 802.1Qat-2010, Stream Reservation Protocol (Clause 34 of IEEE Std 802.1Q-2018). Defines a peer-to-peer protocol among Talkers, Listeners, and Bridges, that 1) identifies the extent of the AVB network, and 2) reserves resources for specific flows.
   - IEEE Std 802.1Qav-2009, Forwarding and Queuing Enhancements for Time-Sensitive Streams (Clause 35 of IEEE Std 802.1Q-2018). Defines the credit-based shaper. Note that this shaper does not guarantee zero congestion loss without a certain amount of overprovisioning.

C. IEEE Std 802.1BA-2011, Audio Video Bridging (AVB) Systems. A set of usage-specific profiles to help interoperability between networked devices using the AVB specifications, including IEEE Std 802.1AS, IEEE Std 802.1Qat, and IEEE Std 802.1Qav.

D. IEEE P802.1AS-Rev, Timing and Synchronization for Time-Sensitive Applications. Revision of IEEE Std 802.1AS-2011 to 1) allow implementation on any device (e.g., a router or a firewall), not just a bridge; 2) be more compatible with IEEE P1588 v2.1, currently in progress; 3) provide better support for multiple instances of the protocol in a network; and 4) support for redundancy.

E. IEEE Std 802.1CB-2017, Frame Replication and Elimination for Reliability. This is the basic technique used by both TSN and DetNet to overcome random packet errors and one or more equipment failures.

F. IEEE Std 802.1Qbu-2016, Frame Preemption (has been incorporated into IEEE Std 802.1Q-2018).

G. IEEE Std 802.3br-2016, Interspersing Express Traffic. Provides for interrupting a packet one or more times, after it has started transmission, in order to transmit packets with more immediate requirements for low latency. Only one packet can be interrupted.

H. IEEE Std 802.1Qcc-2018, Stream Reservation Protocol (SRP) Enhancements and Performance Improvements. Provides the parameters for resource reservation required by the queuing algorithms that have been developed since IEEE Std 802.1Qav.

I. IEEE Std 802.1Qbv-2015, Enhancements for Scheduled Traffic (has been incorporated into IEEE Std 802.1Q-2018). Attaches a time-synchronized rotating schedule to every output queue, so that transmissions can be tightly controlled in time.

J. IEEE Std 802.1Qca-2015, Path Control and Reservation (has been incorporated into IEEE Std 802.1Q-2018). Enhances the ISIS protocol used by IEEE Std 802.1Q-2018 to support the creation of the multiple paths required for IEEE P802.1CB.

K. IEEE Std 802.1Qch-2017, Cyclic Queuing and Forwarding (has been incorporated into IEEE Std 802.1Q-2018). A queue-draining technique employing double buffering on each port, with the buffer switching occurring simultaneously in all bridges in a network, in order to give tight control over latency and jitter.

L. IEEE Std 802.1Qci-2017, Per-Stream Filtering and Policing (has been incorporated into IEEE Std 802.1Q-2018). Time- and data-driven input filtering to 1) support IEEE Std 802.1Qch CQF, and 2) to prevent misbehaving transmitters from affecting the service provided to properly-behaving data flows.

M. IEEE Std 802.1CM-2018, Time-Sensitive Networking for Fronthaul. A profile document showing how to use the TSN capabilities to serve the cellular fronthaul market.

N. IEEE P802.1Qcr, Asynchronous Traffic Shaping. A queue-draining technique that does not require the synchronized buffering of IEEE Std 802.1Qch, but gives deterministic results, unlike IEEE Std 802.1Qav. There are two contending techniques for this standard. (This project is one year from completion.)

O. IEEE P802.1DF, TSN Profile for Service Provider Networks.

NOTE—YANG Interfaces for several of the above standards are under development. Further developments in the base technology are also underway.

IETF DetNet drafts

As yet, there are no RFCs or Standards from the IETF Deterministic Networking (DetNet) working group. Internet drafts are works in progress, and quickly become out-of-date. See the DetNet documents list for the most up-to-date list of DetNet drafts. The drafts listed, here, are the ones that are most likely (in this author's opinion) to progress towards standardization.

Drafts with names that start with "draft-ietf-" have been accepted as working documents by the DetNet Working Group, and thus have some official status. Drafts that do not have "ietf" after the first hyphen are submissions by individuals that may or may not be adopted by the Working Group.

A. draft-ietf-detnet-problem-statement Deterministic Networking Problem Statement—A description of the problem that DetNet is trying to solve.

B. draft-ietf-detnet-use-cases Deterministic Networking Use Cases—A list of descriptions of applications whose requirements can be filled by DetNet.

C. draft-ietf-detnet-architecture Deterministic Networking Architecture—The overall architecture of DetNet. The best statement of the goals of the Working Group.

D. draft-ietf-detnet-dp-alt DetNet Data Plane Protocol and Solution Alternatives—Discusses possibilities for the DetNet data plane, so that paths can be nailed down and sequence numbers attached to packets.

E. draft-dt-detnet-dp-sol DetNet Data Plane solution—The latest thinking on selecting one of the options in draft-ietf-detnet-dp-alt.

F. draft-sdt-detnet-security Deterministic Networking (DetNet) Security Considerations—This work has just started, but it promises to be important for users.

Other relevant standards

A. IEEE Std 1588-2008, IEEE Standard for Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. This is the root standard for all profiles of the Precision Time Protocol. Note that a new version (called 1588v3, informally) is nearing completion. This newer version will be more compatible with IEEE 802.1AS.

B. ISO/IEC 62439-3:2016, Industrial Communication Networks—High Availability Automation Networks. This defines 1) High-availability Seamless Redundancy (HSR), which uses dual-connected rings and a sequence number tag to improve the reliability of industrial networks, and 2) the Parallel Redundancy Protocol (PRP), which uses parallel redundant networks to accomplish the same goal.

C. Draft IEC TR 61850-90-13, Communication networks and systems for power utility automation—Part 90-13: Deterministic Networking Technologies. This Technical Report, currently in development, addresses deterministic network technologies to prepare the usage as a part of the IEC 61850 communication architecture. The document will make use of the IEEE 802.1TSN toolbox as well as of IETF DetNet specifications.

D. IEC 61850-5:2013, Communication networks and systems for power utility automation—Part 5: Communication requirements for functions and device models. This standard defines essential system requirements for the communication between intelligent electronic devices (IEDs).

E. IEC TR 61850-90-12:2015, Communication networks and systems for power utility automation—Part 90-12: Wide area network engineering guidelines. This Technical Report comprises definitions, guidelines, and recommendations for configuration and engineering of WANs used for protection, control and monitoring of IEC 61850-based systems.

F. IEC 62351-7: 2017, Power systems management and associated information exchange—Data and communications security—Part 7: Network and System Management (NSM) data object models. This standard defines network and system management (NSM) data object models that are specific to power system operations. The data is used to detect security intrusions, and to manage the performance and reliability of the communication and automation infrastructure.