Stream: Internet Engineering Task Force (IETF)
RFC: 9760
Category: Standards Track
Published: May 2025
ISSN: 2070-1721
Authors: D. Arnold, *Meinberg-USA*; H. Gerstung, *Meinberg*

RFC 9760
Enterprise Profile for the Precision Time Protocol with Mixed Multicast and Unicast Messages

Abstract

This document describes a Precision Time Protocol (PTP) Profile (IEEE Standard 1588-2019) for use in an IPv4 or IPv6 enterprise information system environment. The PTP Profile uses the End-to-End delay measurement mechanism, allowing both multicast and unicast Delay Request and Delay Response messages.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9760.

Copyright Notice

Table of Contents

1. Introduction

The Precision Time Protocol (PTP), standardized in IEEE 1588, has been designed in its first version (IEEE 1588-2002) with the goal of minimizing configuration on the participating nodes. Network communication was based solely on multicast messages, which, unlike NTP, did not require that a receiving node as discussed in IEEE 1588-2019 [IEEE1588-2019] need to know the

identities of the time sources in the network. This document describes clock roles and PTP Port states using the optional alternative terms "timeTransmitter" instead of "master" and "timeReceiver" instead of "slave", as defined in the IEEE 1588g amendment [IEEE1588g] to [IEEE1588-2019].

The "Best TimeTransmitter Clock Algorithm" ([IEEE1588-2019], Subclause 9.3), a mechanism that all participating PTP Nodes **MUST** follow, sets up strict rules for all members of a PTP domain to determine which node **MUST** be the active reference time source (Grandmaster). Although the multicast communication model has advantages in smaller networks, it complicated the application of PTP in larger networks -- for example, in environments like IP-based telecommunication networks or financial data centers. It is considered inefficient that, even if the content of a message applies only to one receiver, the message is forwarded by the underlying network (IP) to all nodes, requiring them to spend network bandwidth and other resources, such as CPU cycles, to drop it.

The third edition of the standard (IEEE 1588-2019) defines PTPv2.1 and includes the possibility of using unicast communication between the PTP Nodes in order to overcome the limitation of using multicast messages for the bidirectional information exchange between PTP Nodes. The unicast approach avoided that. In PTP domains with a lot of nodes, devices had to throw away most of the received multicast messages because they carried information for some other node. The percent of PTP messages that are discarded as irrelevant to the receiving node can exceed 99% [Estrela_and_Bonebakker].

PTPv2.1 also includes PTP Profiles ([IEEE1588-2019], Subclause 20.3). These constructs allow organizations to specify selections of attribute values and optional features, simplifying the configuration of PTP Nodes for a specific application. Instead of having to go through all possible parameters and configuration options and individually set them up, selecting a PTP Profile on a PTP Node will set all the parameters that are specified in the PTP Profile to a defined value. If a PTP Profile definition allows multiple values for a parameter, selection of the PTP Profile will set the profile-specific default value for this parameter. Parameters not allowing multiple values are set to the value defined in the PTP Profile. Many PTP features and functions are optional, and a PTP Profile should also define which optional features of PTP are required, permitted, and prohibited. It is possible to extend the PTP standard with a PTP Profile by using the TLV mechanism of PTP (see [IEEE1588-2019], Subclause 13.4) or defining an optional Best TimeTransmitter Clock Algorithm, among other techniques (which are beyond the scope of this document). PTP has its own management protocol (defined in [IEEE1588-2019], Subclause 15.2) but allows a PTP Profile to specify an alternative management mechanism -- for example, the Network Configuration Protocol (NETCONF).

In this document, the term "PTP Port" refers to a logical access point of a PTP instantiation for PTP communication in a network.

2. Requirements Language

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Technical Terms

Acceptable TimeTransmitter Table: A list of timeTransmitters that may be maintained by a PTP timeReceiver Clock. The PTP timeReceiver Clock would be willing to synchronize to timeTransmitters in this list.

Alternate timeTransmitter: A PTP timeTransmitter Clock that is not the Best timeTransmitter and therefore is used as an alternative clock. It may act as a timeTransmitter with the Alternate timeTransmitter flag set on the messages it sends.

Announce message: Contains the properties of a given timeTransmitter Clock. The information is used to determine the Best timeTransmitter.

Best timeTransmitter: A clock with a PTP Port in the timeTransmitter state, operating as the Grandmaster of a PTP domain.

Best TimeTransmitter Clock Algorithm: A method for determining which state a PTP Port of a PTP clock should be in. The state decisions lead to the formation of a clock spanning tree for a PTP domain.

Boundary Clock: A device with more than one PTP Port. Generally, Boundary Clocks will have one PTP Port in the timeReceiver state to receive timing and other PTP Ports in the timeTransmitter state to redistribute the timing.

Clock Identity: In [IEEE1588-2019], a 64-bit number assigned to each PTP clock. This number **MUST** be globally unique. Often, it is derived from the Ethernet Media Access Control (MAC) address.

Domain: Treated as a separate PTP system in a network. Every PTP message contains a domain number. Clocks, however, can combine the timing information derived from multiple domains.

End-to-End delay measurement mechanism: A network delay measurement mechanism in PTP facilitated by an exchange of messages between a timeTransmitter Clock and a timeReceiver Clock. These messages might traverse Transparent Clocks and PTP-unaware switches. This mechanism might not work properly if the Sync and Delay Request messages traverse different network paths.

Grandmaster: The timeTransmitter Clock that is currently acting as the reference time source of the PTP domain.

IEEE 1588: The timing and synchronization standard that defines PTP and describes the node, system, and communication properties necessary to support PTP.

NTP: Network Time Protocol, defined by [RFC5905].

Ordinary Clock: A clock that has a single PTP Port in a domain and maintains the timescale used in the domain. It may serve as a timeTransmitter Clock or may be a timeReceiver Clock.

Peer-to-Peer delay measurement mechanism: A network delay measurement mechanism in PTP facilitated by an exchange of messages over the link between adjacent devices in a network. This mechanism might not work properly unless all devices in the network support PTP and the Peer-to-Peer delay measurement mechanism.

Preferred timeTransmitter: A device intended to act primarily as the Grandmaster of a PTP system or as a backup to a Grandmaster.

PTP: The Precision Time Protocol -- the timing and synchronization protocol defined by IEEE 1588.

PTP Port: An interface of a PTP clock with the network. Note that there may be multiple PTP Ports running on one physical interface -- for example, multiple unicast timeReceivers that talk to several Grandmaster Clocks in different PTP domains.

PTP Profile: A set of constraints on the options and features of PTP, designed to optimize PTP for a specific use case or industry. The profile specifies what is required, allowed, and forbidden among options and attribute values of PTP.

PTPv2.1: Refers specifically to the version of PTP defined by [IEEE1588-2019].

Rogue timeTransmitter: A clock that has a PTP Port in the timeTransmitter state -- even though it should not be in the timeTransmitter state according to the Best TimeTransmitter Clock Algorithm -- and that does not set the Alternate timeTransmitter flag.

TimeReceiver Clock: A clock with at least one PTP Port in the timeReceiver state and no PTP Ports in the timeTransmitter state.

TimeReceiver Only Clock: An Ordinary Clock that cannot become a timeTransmitter Clock.

TimeTransmitter Clock: A clock with at least one PTP Port in the timeTransmitter state.

TLV: Type Length Value -- a mechanism for extending messages in networked communications.

Transparent Clock: A device that measures the time taken for a PTP event message to transit the device and then updates the message with a correction for this transit time.

Unicast discovery: A mechanism for PTP timeReceivers to establish a unicast communication with PTP timeTransmitters using a configured table of timeTransmitter IP addresses and unicast message negotiation.

Unicast message negotiation: A mechanism in PTP for timeReceiver Clocks to negotiate unicast Sync, Announce, and Delay Request message transmission rates from timeTransmitters.

4. Problem Statement

This document describes how PTP can be applied to work in large enterprise networks. Such large networks are deployed, for example, in financial corporations. It is becoming increasingly common in such networks to perform distributed time-tagged measurements, such as one-way packet latencies and cumulative delays on software systems spread across multiple computers. Furthermore, there is often a desire to check the age of information time-tagged by a different machine. To perform these measurements, it is necessary to deliver a common precise time to multiple devices on a network. Accuracy currently required in the financial industry ranges from 100 microseconds to 1 nanosecond to the Grandmaster. This PTP Profile does not specify timing performance requirements, but such requirements explain why the needs cannot always be met by NTP as commonly implemented. Such accuracy cannot usually be achieved with NTP, without adding non-standard customizations such as on-path support, similar to what is done in PTP with Transparent Clocks and Boundary Clocks. Such PTP support is commonly available in switches and routers, and many such devices have already been deployed in networks. Because PTP has a complex range of features and options, it is necessary to create a PTP Profile for enterprise networks to achieve interoperability among equipment manufactured by different vendors.

Although enterprise networks can be large, it is becoming increasingly common to deploy multicast protocols, even across multiple subnets. For this reason, it is desirable to make use of multicast whenever the information going to many destinations is the same. It is also advantageous to send information that is only relevant to one device as a unicast message. The latter can be essential as the number of PTP timeReceivers becomes hundreds or thousands.

PTP devices operating in these networks need to be robust. This includes the ability to ignore PTP messages that can be identified as improper and to have redundant sources of time.

Interoperability among independent implementations of this PTP Profile has been demonstrated at the International Symposium on Precision Clock Synchronization (ISPCS) Plugfest [ISPCS].

5. Network Technology

This PTP Profile **MUST** operate only in networks characterized by UDP [RFC0768] over either IPv4 [RFC0791] or IPv6 [RFC8200], as described by Annexes C and D of [IEEE1588-2019], respectively. A network node **MAY** include multiple PTP instances running simultaneously. IPv4 and IPv6 instances in the same network node **MUST** operate in different PTP domains. PTP clocks that communicate using IPv4 can transfer time to PTP clocks using IPv6, or the reverse, if and only if there is a network node that simultaneously communicates with both PTP domains in the different IP versions.

The PTP system **MAY** include switches and routers. These devices **MAY** be Transparent Clocks, Boundary Clocks, or neither, in any combination. PTP clocks **MAY** be Preferred timeTransmitters, Ordinary Clocks, or Boundary Clocks. The Ordinary Clocks may be timeReceiver Only Clocks or may be timeTransmitter capable.

Note that PTP Ports will need to keep track of the Clock ID of received messages and not just the IP or Layer 2 addresses in any network that includes Transparent Clocks or that might include them in the future. This is important, since Transparent Clocks might treat PTP messages that are altered at the PTP application layer as new IP packets and new Layer 2 frames when the PTP messages are retransmitted. In IPv4 networks, some clocks might be hidden behind a NAT, which hides their IP addresses from the rest of the network. Note also that the use of NATs may place limitations on the topology of PTP Networks, depending on the port forwarding scheme employed. Details of implementing PTP with NATs are out of scope for this document.

PTP, similar to NTP, assumes that the one-way network delay for Sync messages and Delay Response messages is the same. When this is not true, it can cause errors in the transfer of time from the timeTransmitter to the timeReceiver. It is up to the system integrator to design the network so that such effects do not prevent the PTP system from meeting the timing requirements. The details of network asymmetry are outside the scope of this document. See, for example, ITU-T G.8271 [G8271].

6. Time Transfer and Delay Measurement

TimeTransmitter Clocks, Transparent Clocks, and Boundary Clocks **MAY** be either one-step clocks or two-step clocks. TimeReceiver Clocks **MUST** support both behaviors. The End-to-End delay measurement method **MUST** be used.

Note that, in IP networks, Sync messages and Delay Request messages exchanged between a timeTransmitter and timeReceiver do not necessarily traverse the same physical path. Thus, wherever possible, the network **SHOULD** be engineered so that the forward and reverse routes traverse the same physical path. Traffic engineering techniques for path consistency are out of scope for this document.

Sync messages **MUST** be sent as PTP event multicast messages (UDP port 319) to the PTP primary IP address. Two-step clocks **MUST** send Follow-up messages as PTP general multicast messages (UDP port 320). Announce messages **MUST** be sent as PTP general multicast messages (UDP port 320) to the PTP primary address. The PTP primary IP address is 224.0.1.129 for IPv4 and FF0X:0:0:0:0:0:0:181 for IPv6, where "X" can be a value between 0x0 and 0xF. The different IPv6 address options are explained in [IEEE1588-2019], Annex D, Section D.3. These addresses are allotted by IANA; see the "IPv6 Multicast Address Space Registry" [IPv6Registry].

Delay Request messages **MAY** be sent as either multicast or unicast PTP event messages. TimeTransmitter Clocks **MUST** respond to multicast Delay Request messages with multicast Delay Response PTP general messages. TimeTransmitter Clocks **MUST** respond to unicast Delay Request PTP event messages with unicast Delay Response PTP general messages. This allows for the use of Ordinary Clocks that do not support the Enterprise Profile, if they are timeReceiver Only Clocks.

Clocks **SHOULD** include support for multiple domains. The purpose is to support multiple simultaneous timeTransmitters for redundancy. Leaf devices (non-forwarding devices) can use timing information from multiple timeTransmitters by combining information from multiple instantiations of a PTP stack, each operating in a different PTP domain. To check for faulty

timeTransmitter Clocks, redundant sources of timing can be evaluated as an ensemble and/or compared individually. The use of multiple simultaneous timeTransmitters will help mitigate faulty timeTransmitters reporting as healthy, network delay asymmetry, and security problems. Security problems include on-path attacks such as delay attacks, packet interception attacks, and packet manipulation attacks. Assuming that the path to each timeTransmitter is different, failures -- malicious or otherwise -- would have to happen at more than one path simultaneously. Whenever feasible, the underlying network transport technology **SHOULD** be configured so that timing messages in different domains traverse different network paths.

7. Default Message Rates

The Sync, Announce, and Delay Request default message rates **MUST** each be once per second. The Sync and Delay Request message rates **MAY** be set to other values, but not less than once every 128 seconds and not more than 128 messages per second. The Announce message rate **MUST NOT** be changed from the default value. The Announce Receipt Timeout Interval **MUST** be three Announce Intervals for Preferred timeTransmitters and four Announce Intervals for all other timeTransmitters.

The logMessageInterval carried in the unicast Delay Response message **MAY** be set to correspond to the timeTransmitter ports' preferred message period, rather than 7F, which indicates that message periods are to be negotiated. Note that negotiated message periods are not allowed; see Section 13 ("Forbidden PTP Options").

8. Requirements for TimeTransmitter Clocks

TimeTransmitter Clocks **MUST** obey the standard Best TimeTransmitter Clock Algorithm as defined in [IEEE1588-2019]. PTP systems using this PTP Profile **MAY** support multiple simultaneous Grandmasters if each active Grandmaster is operating in a different PTP domain.

A PTP Port of a clock **MUST NOT** be in the timeTransmitter state unless the clock has a current value for the number of UTC leap seconds.

If a unicast negotiation signaling message is received, it **MUST** be ignored.

In PTP Networks that contain Transparent Clocks, timeTransmitters might receive Delay Request messages that no longer contain the IP addresses of the timeReceivers. This is because Transparent Clocks might replace the IP address of Delay Requests with their own IP address after updating the Correction Fields. For this deployment scenario, timeTransmitters will need to have configured tables of timeReceivers' IP addresses and associated Clock Identities in order to send Delay Responses to the correct PTP Nodes.

9. Requirements for TimeReceiver Clocks

In a network that contains multiple timeTransmitters in multiple domains, timeReceivers **SHOULD** make use of information from all the timeTransmitters in their clock control subsystems. TimeReceiver Clocks **MUST** be able to function in such networks even if they use

time from only one of the domains. TimeReceiver Clocks **MUST** be able to operate properly in the presence of a rogue timeTransmitter. TimeReceivers **SHOULD NOT** synchronize to a timeTransmitter that is not the Best timeTransmitter in its domain. TimeReceivers will continue to recognize a Best timeTransmitter for the duration of the Announce Receipt Timeout Interval. TimeReceivers **MAY** use an Acceptable TimeTransmitter Table. If a timeTransmitter is not an Acceptable timeTransmitter, then the timeReceiver **MUST NOT** synchronize to it. Note that IEEE 1588-2019 requires timeReceiver Clocks to support both two-step and one-step timeTransmitter Clocks. See [IEEE1588-2019], Subclause 11.2.

Since Announce messages are sent as multicast messages, timeReceivers can obtain the IP addresses of a timeTransmitter from the Announce messages. Note that the IP source addresses of Sync and Follow-up messages might have been replaced by the source addresses of a Transparent Clock; therefore, timeReceivers **MUST** send Delay Request messages to the IP address in the Announce message. Sync and Follow-up messages can be correlated with the Announce message using the Clock ID, which is never altered by Transparent Clocks in this PTP Profile.

10. Requirements for Transparent Clocks

Transparent Clocks **MUST NOT** change the transmission mode of an Enterprise Profile PTP message. For example, a Transparent Clock **MUST NOT** change a unicast message to a multicast message. Transparent Clocks that syntonize to the timeTransmitter Clock might need to maintain separate clock rate offsets for each of the supported domains.

11. Requirements for Boundary Clocks

Boundary Clocks **SHOULD** support multiple simultaneous PTP domains. This will require them to maintain separate clocks for each of the domains supported, at least in software. Boundary Clocks **MUST NOT** combine timing information from different domains.

12. Management and Signaling Messages

PTP management messages **MAY** be used. Management messages intended for a specific clock, i.e., where the targetPortIdentity.clockIdentity attribute (defined in [IEEE1588-2019]) does not have all bits set to 1, **MUST** be sent as a unicast message. Similarly, if any signaling messages are used, they **MUST** also be sent as unicast messages whenever the message is intended solely for a specific PTP Node.

13. Forbidden PTP Options

Clocks operating in the Enterprise Profile **MUST NOT** use the following:

- Peer-to-Peer timing for delay measurement
- Grandmaster Clusters
- The Alternate timeTransmitter option

- Alternate Timescales
- Unicast discovery
- Unicast message negotiation

Clocks operating in the Enterprise Profile **MUST** avoid any optional feature that requires Announce messages to be altered by Transparent Clocks, as this would require the Transparent Clock to change the source address and prevent the timeReceiver nodes from discovering the protocol address of the timeTransmitter.

14. Interoperation with IEEE 1588 Default Profile

Clocks operating in the Enterprise Profile will interoperate with clocks operating in the Default Profile described in [IEEE1588-2019], Annex I.3. This variant of the Default Profile uses the End-to-End delay measurement mechanism. In addition, the Default Profile would have to operate over IPv4 or IPv6 networks and use management messages in unicast when those messages are directed at a specific clock. If neither of these requirements is met, then Enterprise Profile clocks will not interoperate with Default Profile clocks as defined in [IEEE1588-2019], Annex I.3. The Enterprise Profile will not interoperate with the variant of the Default Profile defined in [IEEE1588-2019], Annex I.4, which requires the use of the Peer-to-Peer delay measurement mechanism.

Enterprise Profile clocks will interoperate with clocks operating in other PTP Profiles if the clocks in the other PTP Profiles obey the rules of the Enterprise Profile. These rules **MUST NOT** be changed to achieve interoperability with other PTP Profiles.

15. Profile Identification

The IEEE 1588 standard requires that all PTP Profiles provide the following identifying information.

PTP Profile: Enterprise Profile
Profile number: 1
Version: 1.0
Profile identifier: 00-00-5E-01-01-00

This PTP Profile was specified by the IETF.

A copy may be obtained at <https://datatracker.ietf.org/wg/tictoc/documents>.

16. IANA Considerations

This document has no IANA actions.

17. Security Considerations

Protocols used to transfer time, such as PTP and NTP, can be important to security mechanisms that use time windows for keys and authorization. Passing time through the networks poses a security risk, since time can potentially be manipulated. The use of multiple simultaneous timeTransmitters, using multiple PTP domains, can mitigate problems from rogue timeTransmitters and on-path attacks. Note that Transparent Clocks alter PTP content on-path, but in a manner specified in [IEEE1588-2019] that helps with time transfer accuracy. See Sections 9 and 10. Additional security mechanisms are outside the scope of this document.

PTP management messages **SHOULD NOT** be used, due to the lack of a security mechanism for this option. Secure management can be obtained using standard management mechanisms that include security -- for example, NETCONF [RFC6241].

General security considerations related to time protocols are discussed in [RFC7384].

18. References

18.1. Normative References

[IEEE1588-2019] IEEE, "IEEE Standard for a Precision Clock Synchronization for Networked Measurement and Control Systems", IEEE Std 1588-2019, DOI 10.1109/IEEESTD.2020.9120376, June 2020, <https://ieeexplore.ieee.org/document/9120376>.

[IEEE1588g] IEEE, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems Amendment 2: Master-Slave Optional Alternative Terminology", IEEE Std 1588g-2022, DOI 10.1109/IEEESTD.2023.10070440, March 2023, <https://ieeexplore.ieee.org/document/10070440>.

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, DOI 10.17487/RFC0768, August 1980, <https://www.rfc-editor.org/info/rfc768>.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[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>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

18.2. Informative References

[Estrela_and_Bonebakker] Estrela, P. and L. Bonebakker, "Challenges deploying PTPv2 in a global financial company", Proceedings of the IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication, pp. 1-6, DOI 10.1109/ISPCS.2012.6336634, September 2012, <https://www.researchgate.net/publication/260742322_Challenges_deploying_PTPv2_in_a_global_financial_company>.

[G8271] ITU-T, "Time and phase synchronization aspects of telecommunication networks", ITU-T Recommendation G.8271/Y.1366, March 2020, <https://www.itu.int/rec/T-REC-G.8271-202003-I/en>.

[IPv6Registry] IANA, "IPv6 Multicast Address Space Registry", <https://iana.org/assignments/ipv6-multicast-addresses>.

[ISPCS] Arnold, D. and K. Harris, "Plugfest", Proceedings of the IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS), August 2017, <https://2017.ispcs.org/plugfest>.

[RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010, <https://www.rfc-editor.org/info/rfc5905>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC7384] Mizrahi, T., "Security Requirements of Time Protocols in Packet Switched Networks", RFC 7384, DOI 10.17487/RFC7384, October 2014, <https://www.rfc-editor.org/info/rfc7384>.

Acknowledgements

The authors would like to thank Richard Cochran, Kevin Gross, John Fletcher, Laurent Montini, and many other members of the IETF for reviewing and providing feedback on this document.

Authors' Addresses

Doug Arnold
Meinberg-USA
3 Concord Rd
Shrewsbury, Massachusetts 01545
United States of America
Email: doug.arnold@meinberg-usa.com

Heiko Gerstung
Meinberg
Lange Wand 9
31812 Bad Pyrmont
Germany
Email: heiko.gerstung@meinberg.de