INTERNET-DRAFT
Intended Status: Informational

M. Ackermann
BCBS Michigan
N. Elkins
W. Jouris
Inside Products
K. Haining
U.S. Bank

Expires: July 2014
January 24, 2014

Usage of NTP for the PDM DOH IPv6 Extension Header
draft-ackermann-ntp-pdm-ntp-usage-00

Abstract

The Performance and Diagnostic Metrics (PDM) Destination Options Header (DOH) for IPv6 defines metrics which are critical for timely end-to-end problem resolution, without impacting an operational production network. These metrics and their derivations can be used for network diagnostics. The base metrics are: packet sequence number and packet timestamp. The timestamp fields require time synchronization at the two end points. This document provides implementation guidelines for implementing Network Time Protocol (NTP) to provide such synchronization.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1 Background 3
1.1 General Implementation Guidelines 3
1.2 NTP and IPPM 4
1.3 Hierarchy 4
1.4 Architectural Principles 5
2 NTP Architectures 6
2.1 Generic NTP Architecture 6
2.2 Recommended NTP Architecture 6
3 Security Considerations 6
4 IANA Considerations 7
5 References 7
5.1 Normative References 7
5.2 Informative References 7
6 Acknowledgments 7
Authors' Addresses 7

1 Background

The Performance and Diagnostic Metrics (PDM) Destination Options Header (DOH) for IPv6 [RFC2460] defines metrics which are critical for timely end-to-end problem resolution, without impacting an operational production network. These metrics and their derivations can be used for network diagnostics. The base metrics are: packet sequence number and packet timestamp. The timestamp fields require time synchronization at the two end points.

This document provides implementation guidelines for implementing Network Time Protocol (NTP) [RFC5905] to provide such synchronization. If these guidelines are followed, accuracies at a minimum of 100 milliseconds, or better, should be achievable throughout the network.

For background, please see draft-elkins-6man-ipv6-pdm-dest-option-02 [ELKPDM], draft-elkins-v6ops-ipv6-packet-sequence-needed-01 [ELKPSN], draft-elkins-v6ops-ipv6-pdm-recommended-usage-01 [ELKUSE], draft-elkins-v6ops-ipv6-end-to-end-rt-needed-01 [ELKRSP] and draft-elkins-ippm-pdm-metrics-00 [ELKIPPM]. These drafts are companions to this document.

1.1 General Implementation Guidelines

This recommendation provides technical requirements, guidelines and parameters that, if followed, will enable organizations to implement a NTP environment successfully. Each entity should choose and implement the products, architecture, protocols and configurations that best address their specific requirements and environment, while achieving the minimum requirements as outlined.

In general, this will require a clocking hub with accuracies of 10 milliseconds or better. Where possible, subordinate servers and workstations should operate at stratum 4 or better (e.g., 3, 2 or 1). Servers should define at least three clock reference sources (if possible) at the same or better stratum for maximum availability, diversity and redundancy.

Each clocking hub should include at least three stratum 1 (primary) or stratum 2 (secondary) servers as clock reference sources. A primary server is synchronized to an external timing source (e.g., a GPS receiver, WWVB radio, NIST modem service). A secondary server is synchronized to one or more primary servers (e.g., internal server, Internet server).

Each primary and secondary server defined in the clocking hub should

have at least three timing paths to other servers with preference in order of: (a) on the local intranet; (b) the Internet at large; or (c) on another entity network. This order of preference is based on performance, stability and security. At least one of these paths should be to a server outside the local network. This will provide diversity and redundancy, which is critical in a successful NTP implementation.

NTP implementations should be version 4 where possible, practical and supported by the pertinent platform vendor. Version 3 implementations are considered acceptable at this time.

The preferred NTP operating software is the standard NTP code, which is publicly available. The standard code is natively provided in most Unix operating systems (e.g., Solaris, AIX). The Windows operating system natively provides proprietary NTP software, which operates acceptably, but the more effective method is to download the standard NTP code and install/operate it on the required Windows platform(s). If a Windows platform is acting as a clocking hub for non-Windows devices, it is highly recommended that the standard NTP code be used on the Windows platform acting as the hub.

By default, Windows servers and workstations will use proprietary protocols to receive clock from the controlling AD server. If the controlling AD server is using NTP to clock to primary or secondary NTP servers, the overall configuration should be operating acceptably. Therefore, a viable alternative at the present time is to use the current Windows synchronization architecture with the AD server(s), synchronizing to multiple primary or secondary NTP servers. It should be recognized that the crafted mitigation algorithms used in NTP may not be available in native Windows software.

1.2 NTP and IPPM

RFC2330, Framework for IP Performance Metrics, [RFC2330] discusses a number of issues with clocking and NTP including drift, skew, resolution, etc. We will not repeat these here but will refer the reader to that RFC for background.

1.3 Hierarchy

Each entity should have a clocking hub that receives its clock from a Stratum one or better source. This received clock should then be made available to every platform in the network, either directly or indirectly. Indirectly involves multiple levels of the hierarchy as depicted in the generic NTP architecture diagram (2.1). The clock is transported via NTP sessions which are Client/Server in nature. Note

that for every additional hierarchal level, the received Stratum level (accuracy of the clock), is reduced, which means that the received clock is slightly less accurate.

NTP Client/Server Sessions can be connected in three basic fashions:

1. Broadcast,
2. Server,
3. Peer.

Our recommendation is to utilize server connections in most cases. Broadcast is considered less stable, accurate and secure, but is still a viable option which requires less parameter definition at the client level. Peer sessions are a good solution when platforms are truly peer in the implemented hierarchy (e.g. dual Router Clocking Hubs).

1.4 Architectural Principles

Most of the architectural principals and objectives are described in section 1.1. Several of the salient concepts include:

- Servers should define at least three clock reference sources (if possible) at the same or better stratum for maximum availability, diversity and redundancy.- DNS should be used at all levels. In some situations Round Robin to achieve load balancing and redundancy.Redundancy should be used at all levels if possible. This may not be necessary with workstations.- Sessions between NTP Clients and NTP Servers will usually be point to point but can also be broadcast. The recommendation of this document is to utilize point to point, because it is more stable, accurate and more secure. - NTP sessions between the Client and the Server can be defined to run in "Authenticated Mode". Utilizing NTP in Authenticated Mode allows a connected entity to assure that the NTP Server that clock is being received from the intended NTP Server and not an IP imposter. "Shared Secret" keys, hashed using MD5, are used to authenticate the NTP sessions requested by NTP clients.

2 NTP Architectures

Following are sample diagrams of a generic NTP architecture and a suggested scheme which will achieve the required synchronization for the PDM.

2.1 Generic NTP Architecture

The following is a sample generic NTP architecture:

```
     __________          ___________
    (          )        (  Internet )
    ( Internal )        (  Time     )
    ( Network  )        (  Sources  )
    (__________)        (___________)
         ^                   ^
         |                   |
         |                   |
    +-----------------------------+    +----------+
    |                             |    | Internal |
    |   Clocking Hub Router       |<---| Router   |
    |                             |    |          |
    +-----------------------------+    +----------+
         ^                  ^
         |                  |
         |                  |
     +--------+       +----------+
     | Unix   |       | Windows  |
     | Server |       | Server   |
     | Hub    |       | Hub      |
     +--------+       +----------+
         ^                  ^
         |                  |
         |                  |
    _____|_____      _______|_______
   (           )    (  Windows      )
   (  Unix     )    (  Servers &    )
   (  Servers  )    (  Workstations )
   (___________)    (________________)
```

2.2 Recommended NTP Architecture

This diagram represents an example of what a successful NTP implementation could look like, including the recommended levels of redundancy, diversity, load sharing, accuracy, and DNS usage.

3 Security Considerations

There are no security considerations.

4 IANA Considerations

There are no IANA considerations.

5 References

5.1 Normative References

[RFC2330] Paxson, V., Almes, G., Mahdavi, J., and M. Mathis, "Framework for IP Performance Metrics", RFC 2330, May 1998.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, June 2010.

5.2 Informative References

[ELKPDM] Elkins, N., "draft-elkins-6man-ipv6-pdm-dest-option-02", Internet Draft, September 2013.

[ELKPSN] Elkins, N., "draft-elkins-v6ops-ipv6-packet-sequence-needed-01", Internet Draft, September 2013.

[ELKRSP] Elkins, N., "draft-elkins-v6ops-ipv6-end-to-end-rt-needed-01", Internet Draft, September 2013.

[ELKUSE] Elkins, N., "draft-elkins-v6ops-ipv6-pdm-recommended-usage-01", Internet Draft, September 2013

[ELKIPPM] Elkins, N., "Draft-elkins-ippm-pdm-metrics-01", Internet Draft, September 2013.

6 Acknowledgments

The authors would like to thank Al Morton for his assistance.

Authors' Addresses

Michael S. Ackermann
Blue Cross Blue Shield of Michigan
P.O. Box 2888
Detroit, Michigan 48231
United States
Phone: +1 310 460 4080
Email: mackermann@bcbsmi.com
http://www.bcbsmi.com

Nalini Elkins
Inside Products, Inc.
36A Upper Circle
Carmel Valley, CA 93924
United States
Phone: +1 831 659 8360
Email: nalini.elkins@insidethestack.com
http://www.insidethestack.com

Keven Haining
US Bank
16900 W Capitol Drive
Brookfield, WI 53005
United States
Phone: +1 262 790 3551
Email: keven.haining@usbank.com
http://www.usbank.com

William Jouris
Inside Products, Inc.
36A Upper Circle
Carmel Valley, CA 93924
United States
Phone: +1 925 855 9512
Email: bill.jouris@insidethestack.com
http://www.insidethestack.com