

MBONE Deployment Working Group
INTERNET-DRAFT
<[draft-ietf-mboned-sntp-heart-00.txt](#)>
[23](#) October 1996

Bernard Aboba
Microsoft Corporation
Thomas Pfenning
Microsoft Corporation

The Use of SNTP as a Multicast Heartbeat

[1.](#) Status of this Memo

This document is an Internet-Draft. 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.''

To learn the current status of any Internet-Draft, please check the ``[1id-abstracts.txt](#)' listing contained in the Internet-Drafts Shadow Directories on [ds.internic.net](#) (US East Coast), [nic.nordu.net](#) (Europe), [ftp.isi.edu](#) (US West Coast), or [munnari.oz.au](#) (Pacific Rim).

The distribution of this memo is unlimited. It is filed as <[draft-ietf-mboned-sntp-heart-00.txt](#)>, and expires May 1, 1997. Please send comments to the authors.

[2.](#) Abstract

This document describes how the Simple Network Time Protocol (SNTP) can be used to provide a multicast heartbeat. Given the current state of the art in multicast diagnostics, use of a heartbeat may prove a useful diagnostic tool for operators as well as for applications developers. Operators may use the heartbeat to alert themselves to losses of multicast connectivity in portions of the network. Applications developers may use the heartbeat to determine whether to enable multicast features or to default to unicast operation. In the long term, better solutions (such as improved IGMP diagnostics) are likely to become available, so that a multicast heartbeat is unlikely to have long-term utility.

[3.](#) Introduction

[3.1.](#) Problem statement

Today an increasing number of applications support both multicast and unicast modes of operation. Typically these applications default to

INTERNET-DRAFT

23 October 1996

unicast mode, switching to multicast mode on explicit instructions from the user. However, it is also possible to initially put an application into multicast mode, join a group, then wait to receive packets on the group. If packets arrive, then the application is left in multicast mode; otherwise, after a suitable timeout interval, the application is switched to unicast mode. However, this approach is usually not satisfactory since join latencies of several minutes are common.

Another issue arises with multicast applications running over dialup connections. In this case, applications are typically unaware of the state of the dialup interface; it is possible for the dialup connection to go down or come up again, possibly with a new IP address assignment, without the application being notified. In such a case, the IGMP state of the dialup interface may be cleared, leaving the dialup interface without any group memberships. Thus the host will not respond to subsequent IGMP membership queries on the dialup interface, even though the application believes that its group memberships persist.

[3.2.](#) Alternative solutions

The problems described above have several solutions, including:

- Use of a multicast heartbeat
- IGMP membership query detection
- Use of multicast diagnostic tools, such as mtrace
- SNMP queries
- Additional IGMP messages

[3.2.1.](#) Use of a multicast heartbeat group

Both of the problems described above can be addressed by use of a multicast heartbeat. A heartbeat group is a group to which routers and NAS devices are continually subscribed, providing low join latencies.

On startup, routers and applications looking to determine whether they have multicast connectivity can listen to the heartbeat group. Since the gateway router or NAS device is already subscribed to the heartbeat group, a host joining the group will experience low join latency, allowing an application to quickly determine whether to enable multicast features. Once it has determined that multicast connectivity is available, the application can close the connection, which (assuming the host is IGMP v2 capable) may result in the host leaving the heartbeat group.

Similarly, in the case where a dialup interface goes down and the application stops receiving packets on the multicast group, after a suitable interval, the application can listen for the presence of the multicast heartbeat. If it does not receive the heartbeat, it may then conclude that IGMP membership state has been lost, and should close and reopen multicast sockets.

[3.2.2.](#) IGMP membership query detection

While IGMP membership queries do not provide information on the state of multicast connectivity, they do provide an indication that a multicast-capable router is present on the network. This information, were it to be made available to an application, could be used to determine whether to enable multicast features.

Unfortunately for applications developers, current programming interfaces do not provide applications with this information.

[3.2.3.](#) Use of multicast diagnostics

Application-initiated mtrace queries could readily be used by applications to determine connectivity to specific groups. Alternatively, periodic mtrace queries with a multicast response address could be used to provide a heartbeat on the mtrace group 224.0.1.32, mtrace.mcast.net. However, these responses would take up considerably more bandwidth than SNMP, and it is doubtful that the additional information provided by mtrace would be useful in this context.

[3.2.4.](#) SNMP queries

The IGMP MIB, described in [3] provides access to the IGMP Interface Table as well as to the IGMP Cache Table. This could be used to determine whether a router is multicast-capable.

However, while SNMP information is typically available to a management station operated by a NOC, it is usually not made available to applications running on arbitrary hosts.

[3.2.5.](#) Additional IGMP messages

Today the Internet gets along quite well without a unicast heartbeat. So we would do well to ask ourselves "why do we not need a unicast heartbeat?" The answer is that we have ICMP messages to indicate when a host, network or port is unreachable. As a result, applications receive timely indications of connectivity problems, and can respond appropriately.

Not only are there no equivalent ICMP error messages for multicast, but it is expressly forbidden to generate ICMP messages in response to a packet with a multicast destination. As a result, a host has no immediate way of determining that its join request is being sent on a non-multicast capable network.

However, it may be desirable to provide for additional diagnostic capabilities within IGMP. Such facilities could include a means for retrieving the IGMP Interface Table as well as the IGMP Cache Table. Were such facilities to be required of all multicast-capable routers, then a host could determine the state of multicast connectivity via an

IGMP query. It is believed that this is the best long-term solution to the problem.

[4.](#) Use of SNTP as a multicast heartbeat

While it is likely that better diagnostic methods will become available in the long term, given the current state of the art, use of a multicast heartbeat may prove useful. If such a heartbeat is needed, then the Simple Network Time Protocol (SNTP) appears ideal for this purpose.

SNTP was created in order to support synchronization of clocks on the Internet in situations where the high precision of the Network Time Protocol (NTP) is not required. SNTP supports unicast, broadcast, and multicast modes. Unicast mode provides for clock synchronization via a client/server interaction, and is typically used prior to initiation of multicast mode. In multicast mode, the SNTP server periodically sends the time to a designated multicast group, and clients listen to the messages, but do not reply. Existing SNTP implementations typically support all three modes, and allow for adjusting both the sending interval as well as the destination port.

With SNTP it is possible to multicast to an address with global scope or to an administratively scoped address. For example, reference [\[1\]](#) describes SNTP use of the group address 224.0.1.1 as well as UDP port [123](#) for both the source and destination ports. In addition, use of an address in the administratively scoped region may also be desirable. The use of separate heartbeats for global and administratively scoped addresses allows an application to determine if multicast connectivity is available, and if so, whether it is global or exists only within the administratively scoped region.

Today we face a scarcity of multicast diagnostic tools suitable for use by Network Operations Centers. By enabling routers as SNTP listeners, and adding one or more SNMP MIB variables, the ability to monitor multicast connectivity on a network-wide basis can be enhanced.

[5.](#) Implementation issues

[5.1.](#) Address allocation and group announcements

In cases where a firewall is used, multicast connectivity may be restricted to the administratively scoped region. In this case, listening to the SNTP multicast group (224.0.1.1) will not allow an application or device to determine whether it has multicast connectivity. It will also need to listen to an equivalent group within the administratively scoped region.

Currently there is no static multicast group allocated for use of SNTP within the administratively scoped region. As a result, an announcement mechanism (such as that provided by SAP) can be used to announce

the heartbeat group in the administratively scoped region.

[5.2.](#) Use by clients and network devices

In order to provide the desired heartbeats, an SNTP server will typically be operated within the administratively scoped region, as well as on the global Internet. On startup, network devices such as routers or NASes will join 224.0.1.1 as well as the administratively scoped SNTP group, and will listen to SNTP multicasts on UDP port 123. Having routers and NASes as perennial members of the heartbeat group is necessary in order to guarantee low latency for host join requests.

On startup, host applications will typically join both the 224.0.1.1 group as well as the administratively scoped heartbeat group, and will listen on UDP port 123. Should they not receive the expected SNTP multicasts within 15 seconds (three heartbeat periods), they may then conclude that multicast connectivity is not available, and take action accordingly. These actions could include defaulting to unicast operation, or presenting a dialog indicating the failure to detect multicast connectivity. If multicast connectivity is detected, the application may then close the connection.

Similarly, after not receiving packets on a multicast group for at least 30 seconds, an application may once again listen for the multicast heartbeat. If it does not receive the expected SNTP multicasts within 15 seconds, it may conclude that multicast connectivity has been lost, and take action accordingly. These actions could include closing and reopening multicast sockets (in case dialup connectivity was lost), or presenting a dialog indicating the loss of signal.

[5.3.](#) Security issues

The use of SNTP as a multicast heartbeat makes it a target for malicious individuals interested in disrupting network operation. As noted in [1], it is possible for any SNTP server to send to the 224.0.1.1 group address. As a result, client implementations will need to check the authenticity of the source. This should be accomplished by checking the source IP address, as well as by taking advantage of the authenticator field within SNTP.

[5.4.](#) Bandwidth consumption

A major concern with implementation of a heartbeat capability is the resulting bandwidth consumption, and CPU utilization. Since the SNTP heartbeat described in this document would be implemented by a variety of network devices, it will consume bandwidth on an Internet-wide

basis. In addition, determining the authenticity of the SNTP multicast heartbeat requires use of public-key cryptography, and can take as long as several hundred milliseconds.

INTERNET-DRAFT

23 October 1996

As defined in [1], the SNTP packet is 60 octets in length. This when added to the 28 octet IP/UDP header gives a total packet size of 88 octets. In order to keep bandwidth consumption to an minimum, we recommend that the interval between SNTP multicasts be set to 5 seconds or greater. Keeping to these guidelines will keep the SNTP bandwidth consumption under 200 bps.

[6.](#) Acknowledgements

Thanks to Tom Blank of Microsoft and Louis Mamakos of UUNET for many useful discussions of this problem space.

[7.](#) References

- [1] D. Mills. "Simple Network Time Protocol." [RFC 1769](#), University of Delaware, March 1995.
- [2] S.E. Deering. "Host Extensions for IP Multicasting." RFC 1112, Stanford University, August, 1989.
- [3] K. McCloughrie, D. Farinacci. "Internet Group Management Protocol MIB." [draft-ietf-idmr-igmp-mib-03.txt](#), cisco Systems, June 1996.

[8.](#) Authors' Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: 206-936-6605
EMail: bernarda@microsoft.com

Thomas Pfenning
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: 206-703-4830
EMail: thomaspf@microsoft.com