

NETWORK Working Group
INTERNET-DRAFT
Category: Informational
<[draft-thaler-zeroconf-multicast-02.txt](#)>
[4](#) October 2000

Dave Thaler
Bernard Aboba
Microsoft

Multicast Address Allocation in Auto-Configured Networks

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

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/ietf/lid-abstracts.txt>

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

[1](#). Copyright Notice

Copyright (C) The Internet Society (2000). All Rights Reserved.

[2](#). Abstract

Today, with the rapid rise of home networking, there is an increasing need for auto-configuration mechanisms. This document describes how small networks without a multicast address allocation server may auto-allocate multicast addresses.

[3](#). Introduction

The Internet Multicast Address Allocation Architecture [[1](#)] provides a framework which includes multicast address allocation servers (MAASs) that allocate addresses to hosts. The Multicast Address Dynamic Client Allocation Protocol (MADCAP) [[2](#)] has been proposed as the protocol via which hosts and servers communicate. The Multicast Address Allocation Protocol (AAP) [[3](#)] has been proposed as the protocol via which servers communicate with each other to prevent allocating the same addresses. However, servers may not be present in all environments.

INTERNET-DRAFT

Multicast Auto-Configured Networks

4 October 2000

Today, with the rapid rise of home networking, there is an increasing need for auto-configuration mechanisms. This document describes how small networks without a multicast address allocation server may auto-allocate multicast addresses.

[4.](#) Terminology

This document uses the following terms:

Configured environment

A network area (such as the Internet or an enterprise network) which are managed by one or more administrators or organizations.

Zero-configuration environment

A network area consisting of devices which have no manual configuration done to them, and are not managed by an administrator or organization.

There are two primary zero-configuration scenarios which we distinguish from a configured environment in this document.

Isolated: A group of hosts communicate as peers in a zero-configuration environment. In this scenario, there are no address allocation servers, and likely no routers.

Edge: In this scenario, we assume there is a router which connects a zero-configuration environment to a configured environment such as the Internet. In this scenario, there are no address allocation servers configured in the zero-configuration area, and there may or may not be servers in the configured environment.

In this document, the key words "MAY", "MUST", "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [\[4\]](#).

[5.](#) Configuration requirements for small networks

In order to enable effective multicast address allocation in small networks, the following requirements need to be met:

Allocation

A mechanism **MUST** be provided to allow for hosts to allocate multicast addresses. Ideally, host behavior should be the same in a zero-configuration environment and in a configured environment so that transitions can be done easily.

Isolated to Edge transition

A mechanism **MUST** be provided to transition between the Isolated and Edge scenarios. This happens when a router is added to connect an Isolated area to a configured environment, such as when a host in an Isolated environment dials an Internet Service Provider (ISP) and becomes a router. Similarly, the reverse transition occurs if the router goes down.

Isolated to Configured transition

A mechanism **MUST** be provided to transition between an Isolated and a Configured environment. This occurs, for example, in a corporate environment when a router comes up or goes down. When a router is down, any hosts on disconnected links may be in an Isolated environment.

[6.](#) Auto-configuration prescription

In this section, we assume that MADCAP and AAP are the protocols in use, since they appear to meet the requirements.

[6.1.](#) Zero-configuration host behavior

As described in [\[5\]](#), a host provides two services to its applications through some API. First, it must allow applications to enumerate the set of available multicast scopes. Second, it must allow applications to request, renew, and release addresses, where the scope must be specified by the application.

Note that acquiring the set of enumerated scopes does not necessarily imply that addresses are available in each scope, only that it is legal for an application to request an address in one.

[6.1.1.](#) Scope enumeration

To determine whether a multicast address allocation server is available,

a host SHOULD, at startup time, attempt to acquire the list of multicast scopes available by using MADCAP's GETINFO request as described in [2], and done periodically thereafter. This determination MAY instead be delayed until an application wants to enumerate scopes, at the expense of increasing the time needed.

If any servers are found, a host should use the set of scopes returned by the servers. In addition, if ranges are defined for allocation of Link-Local, Node-Local, and/or Single-Source addresses, these may be assumed as well (for example, such Link-Local and Node-Local are currently defined in IPv6 [6], and Single-Source is currently defined in IPv4 [7]).

If no servers are found, a host can assume that any scopes exist which are well-known with specified ranges. These include the Global scope, the Local scope [6], the Allocation scope [1], and the Single-Source scope. In this situation, a host MAY also begin passively listening to MZAP [8] messages to build up its scope list further. (MZAP sends very low frequency reports of scopes to listeners inside those scopes.)

6.1.2. Address Allocation

Node-Local and Single-Source addresses can be allocated immediately by any host. The algorithm for choosing an address is implementation-dependent, but the address range to use MUST be the range registered with IANA for the specified scope.

Link-Local addresses can be allocated only by hosts which implement at least a minimal subset of AAP consisting of the ACLM and AIU messages

For all other addresses, the following procedures apply.

If the host has recently tried to obtain the scope list, then the host already knows whether any MAAS's are present. If it has not tried recently, then the host can use MADCAP to discover a server when it wants to allocate an address.

If a server is present, the host simply uses MADCAP to allocate addresses.

If no server is present, then if the scope associated with the request is "big" (Global, or any scope obtained from MZAP and identified by MZAP

as "big"), then no addresses may be allocated; otherwise (if the scope is not "big") then the host MAY allocate addresses by participating in AAP. The host MUST NOT allocate the last 256 addresses in the range as these are reserved for scope- relative addresses [6].

[6.2.](#) Zero-configuration router behavior

In the Edge scenario, a zero-configuration router exists, with a link which connects to a configured environment. Here, there is likely a well-understood distinction between the local area and the external environment, as well as a potential requirement to be able to scope some data to the local area. Hence, if the router detects that it is an "Edge" router (i.e. a router in an Edge scenario), it should instantiate a Local scope boundary on that link.

However, before it can do this, a router must be able to distinguish between whether it is in an Edge scenario, or in a configured environment. This could be done in any implementation- specific manner. For example, the router could assume it is in a zero-configuration

environment unless it is specifically configured otherwise. This would appear to be acceptable, since if it is in a configured environment, the router would typically be configured anyway.

If the router determines that it is an Edge router, the router SHOULD instantiate a Local scope boundary and become a mini-MAAS with behavior as follows.

[6.2.1.](#) Scope enumeration

To acquire a set of scopes, the router performs the same actions as those described for hosts in [Section 5.1.1](#) above, with MADCAP queries being sent out over the link to the configured environment.

When the router receives GETINFO messages from clients in the zero-configuration environment asking for the scope list, it responds as a MADCAP server would, by including the scope list it acquired above.

[6.2.2.](#) Address Allocation

Local scope addresses can be allocated immediately by the router as if it were a MADCAP server. For addresses in all larger scopes, the

following procedures apply.

If a MADCAP server was found in the configured environment, the router acts as a MADCAP proxy and relays the request to an appropriate server as if it were a client. The response is relayed back to the client as if it were a server.

if no MADCAP server was found in the configured environment, the router MAY allocate addresses itself if it implements AAP to coordinate with any other MAASs (such as other Edge routers) reached via the configured environment.

7. Transitioning Between Scenarios

In an Isolated environment, each host should periodically (either at regular intervals, or only when applications request addresses or scope lists) re-check whether a server is available. This allows simple transition to an Edge or configured environment.

Similarly, if the host stops receiving responses from any servers, the behavior specified in [Section 5.1](#) allows it to continue allocating addresses.

In an Edge environment, the Edge router should periodically (either at regular intervals, or only when hosts request addresses or scope lists) re-check whether a server is available in the configured environment.

Similarly, if the Edge router stops receiving responses from any servers in the configured environment, the behavior specified in [Section 5.2](#) allows it to continue allocating addresses.

8. References

- [1] Thaler, D., Handley, M., and D. Estrin, "The Internet Multicast Address Allocation Architecture", Internet Draft, [draft-ietf-malloc-arch-05.txt](#), December 2000.
- [2] Hanna, S., Patel, B., and M. Shah, "Multicast Address Dynamic Client Allocation Protocol (MADCAP)", Work in progress, [draft-ietf-malloc-madcap-07.txt](#), September 1999.
- [3] Handley, M. and S. Hanna, "Multicast Address Allocation Protocol

- (AAP)", Work in progress, [draft-ietf-malloc-aap-02.txt](#), October 1999.
- [4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
 - [5] Finlayson, R., "An Abstract API for Multicast Address Allocation", [RFC 2771](#), February 2000.
 - [6] Meyer, D., "Administratively Scoped IP Multicast", [BCP 23](#), [RFC 2365](#), July 1998.
 - [7] IANA, "Single-source IP Multicast Address Range", <http://www.isi.edu/in-notes/iana/assignments/single-source-multicast>, October 1998.
 - [8] Handley, M., Thaler, D., and Kermode, R., "Multicast-Scope Zone Announcement Protocol (MZAP)", [RFC 2776](#), February 2000.
 - [9] Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11-1997, 1997.
 - [10] Thomson, S. and Narten, T., "IPv6 Stateless Address Autoconfiguration", [RFC 2462](#), December 1998.
 - [11] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., Lear, E., "Address Allocation for Private Internets", [RFC 1918](#), February, 1996.

[9.](#) Security Considerations

In the interest of simplicity, this draft does not prescribe a means of securing the multicast auto-configuration mechanism. Thus it is possible that hosts will allocate conflicting multicast addresses for a period of time, or that non-conforming hosts will attempt to deny service to other hosts by allocating the same multicast addresses.

Since MADCAP is used as a mechanism for determining whether to auto-configure, it should be noted that it is likely that hosts in small network scenarios will not attempt to secure their MADCAP traffic.

If unsecured, MADCAP is vulnerable to a number of threats, including message modification and attacks by rogue servers and unauthenticated clients. While the procedure described in this document does not preclude implementation of MADCAP security, the extra configuration required to set this up represents an implementation barrier in the home network. As a result, it is likely that most home routers will not support MADCAP authentication, and that those networks will remain vulnerable to attack.

These threats are most serious in wireless networks such as 802.11, since attackers on a wired network will require physical access to the home network, while wireless attackers may reside outside the home. In order to provide for privacy equivalent to a wired network, the 802.11 specification provides for RC4-based encryption. This is known as the "Wired Equivalency Privacy" (WEP) specification, described in [9]. Where WEP is implemented, an attacker will need to obtain the WEP key prior to gaining access to the home network.

[10.](#) IANA Considerations

This draft does not create any new number spaces for IANA administration.

[11.](#) Acknowledgments

This draft has been enriched by comments from Steve Hanna of Sun Microsystems.

[12.](#) Authors' Addresses

Dave Thaler
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: +1 (425) 703-8835

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: +1 (425) 936-6605
EMail: bernarda@microsoft.com

13. Full Copyright Statement

Copyright (C) The Internet Society (2000). All Rights Reserved.
This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

14. Expiration Date

This memo is filed as <[draft-thaler-zeroconf-multicast-02.txt](#)>, and expires May 1, 2001.