

NETWORK Working Group
INTERNET-DRAFT
Category: Informational
<[draft-aboba-dhc-mini-04.txt](#)>
[29](#) September 2001

Bernard Aboba
Microsoft

The Mini-DHCP Server

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#).

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/1id-abstracts.txt>.

To view the list Internet-Draft Shadow Directories, see <http://www.ietf.org/shadow.html>.

Copyright Notice

Copyright (C) The Internet Society (2001). All Rights Reserved.

Abstract

Today, with the rapid rise of home networking, there is a need for simple mechanisms of IPv4 address allocation and name resolution. This document describes the behavior of the mini-DHCP server, a small scale DHCP server that is typically implemented as part of a home gateway.

As described in this document, the mini-DHCP server is capable of allocating addresses either in single or multi-segment networks. It supports dynamic DNS, and is capable of automatically detecting the presence of a full-fledged DHCP server, or other mini-DHCP servers, and shutting down as required.

INTERNET-DRAFT

The Mini-DHCP Server

29 September 2001

Table of Contents

1.	Introduction	3
1.1	Terminology	3
1.2	Requirements language	3
2.	Overview	4
2.1	Resilience	4
2.2	Dynamic DNS support	4
2.3	Compatibility with existing DHCP servers	4
2.4	Bridged networks	5
3.	Addressing	6
3.1	Address allocation	6
3.2	Address selection	7
3.3	Multi-segment address allocation	7
4.	References	9
5.	Security considerations	10
6.	IANA considerations	10
	Acknowledgments	11
	Author's addresses	11
	Intellectual Property Statement	11
	Full Copyright Statement	11

INTERNET-DRAFT

The Mini-DHCP Server

29 September 2001

[1.](#) Introduction

Today, home gateways frequently include functionality beyond that of a router, as defined in [RFC 1812](#) [10]. For example, home gateways frequently support Network Address Translation (NAT), described in [8]-[10], as well as acting as a DHCP server as described in [RFC 2131](#) [3], and a DNS server as described in [13]. These small scale DHCP and DNS servers will be described as "mini-DHCP" and "mini-DNS" servers within this document.

While initial offerings were relatively simple devices, today's home gateways are increasingly sophisticated. For example, home gateways may include support for multiple Internet or home interfaces, including support for both 802.11 wireless [18], and wired networks. This implies that the mini-DHCP server may need to allocate addresses on multiple segments, instead of just one.

In some cases, multiple home gateways may exist within the home, or a home gateway may be brought into an enterprise environment, causing potential conflicts between the mini-DHCP server and an existing DHCP server.

The purpose of this document is to provide guidance on how a mini-DHCP server can behave so as to minimize the potential for conflict, and maximize the services provided to users of the home network.

[1.1.](#) Terminology

This document uses the following terms:

Site Administrator

A Site Administrator is the person or organization responsible for handing out IP addresses to client machines.

DHCP client

A DHCP client or "client" is an Internet host using DHCP to

obtain configuration parameters such as a network address.

DHCP server

A DHCP server or "server" is an Internet host that returns configuration parameters to DHCP clients.

[1.2.](#) Requirements language

In this document, the key words "MAY", "MUST", "MUST NOT", "OPTIONAL", "RECOMMENDED", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [\[1\]](#).

[2.](#) Overview

The mini-DHCP server provides DHCP server functionality, as described in [RFC 2131](#) [\[3\]](#), allocating IP addresses as well as providing for host configuration. Among the host configuration information typically provided by the mini-DHCP server is the address of the residential gateway as well as the address of the mini-DNS server.

[2.1.](#) Resilience

Since the mini-DHCP server will typically reside on a residential gateway along with a mini-DNS server, it will typically provide its own address in the default gateway and DNS server options, described in [RFC 2132](#) [\[4\]](#). However, in order to provide additional resilience, the residential gateway can provide the addresses of secondary servers as well. For example, the residential gateway can obtain the addresses of additional gateways (learned by listening to routing protocol announcements on the home network interfaces) or DNS servers (learned via PPP IPCP extensions [\[19\]](#) or DHCP [\[3\]](#) on the Internet interface). In the event that the home gateway is brought down (such as by a virus attack), this additional configuration information can enable hosts to continue accessing the Internet until the problem is resolved.

[2.2.](#) Dynamic DNS support

The mini-DHCP server SHOULD support the functionality described in "Resolution of DNS Name Conflicts Among DHCP Clients" [\[5\]](#), enabling dynamic registration of the PTR and (if configured to do so) A records for the hosts to whom it allocates addresses. Mini-DNS servers typically

do not support dynamic DNS update, so that the mini-DHCP server will typically register both A and PTR records. The host provides its fully qualified domain names to the mini-DHCP server via the DHCP Client FQDN option, described in [6].

This allows the mini-DNS server to resolve DNS queries relating to hosts on the internal network. Queries relating to Internet hosts are handled by proxying the DNS query to the DNS server configured on the external interface. This functionality is important, since multicast DNS, defined in [17], is disabled by default when a DHCP server is available on the network, and provides DNS server configuration. Thus, multicast DNS cannot be relied upon to provide for name resolution in situations where a mini-DHCP server is present.

[2.3](#). Compatibility with existing DHCP servers

In order to avoid conflicts with full-fledged DHCP servers, or other mini-DHCP servers, it is necessary for the mini-DHCP server to automatically determine whether it should be operating on an interface.

A mini-DHCP server MUST NOT be active on an interface if there is already a DHCP server active on that interface. Thus if the home gateway's BOOTP relay agent has already been configured on an interface, the mini-DHCP server MUST NOT be active on that interface.

In order to detect the presence of a DHCP server on interfaces that have not been configured as BOOTP relay agents, a mini-DHCP server MUST operate in promiscuous mode and send out periodic DHCPDISCOVER requests. If a response is received, the mini-DHCP server MUST NOT provide DHCP service on that interface. Similarly, if the mini-DHCP server hears a DHCPOFFER, DHCPACK or DHCPNAK on an interface, then it MUST NOT provide DHCP service on that interface.

In the case where there is more than one mini-DHCP server active on a segment, it is possible that the mini-DHCP servers will send DHCPDISCOVER queries simultaneously, and thus without an election mechanism, all of them might be shut down on an interface. As a result, it is desirable to provide a deterministic method for deciding which mini-DHCP servers shut down. As described in [20], the mini-DHCP election option can be utilized for this purpose.

Note that a mechanism is needed to allow the mini-DHCP server to be

brought up again once the other DHCP servers are removed. Once the mini-DHCP server has detected another DHCP server and has stopped offering service on an interface, it SHOULD set a timer. Once this timer expires, the mini-DHCP server MUST once again send out a DHCPDISCOVER and listen for responses. The recommended timer interval is 5 minutes.

Note that if one or more DHCP servers are found on other interfaces, it may not be desirable to run a mini-DHCP server on those interfaces lacking a DHCP server. Instead, it may make more sense to operate those interfaces in bridging mode as discussed in the next section.

[2.4.](#) Bridged networks

Today mini-DHCP servers are typically included as part of home gateways supporting Network Address Translation. However, the mini-DHCP server can also improve ease of use in situations where routable address space is available.

For example, the home gateway may be connected to an Intranet via a VPN, or it may be attached via a dialup or broadband connection to an ISP that operates its own DHCP server providing routable address space to customers with attached LANs.

In these situations, it is possible for hosts on the home network to obtain routable addresses from the ISP or Intranet DHCP server. Rather than acting as a mini-DHCP server and doing Network Address Translation,

the home gateway can act as a bridge. In this role the home gateway forwards DHCPDISCOVER broadcasts down the link, but does not act as a BOOTP relay agent.

In order to enable automated detection of bridged versus NATed operation, on bootup, the home gateway obtains an IP address on its external interface and then sends a DHCPDISCOVER on that interface. If the external interface is a LAN link, and the original address was obtained via DHCP, then a different client-identifier option must be used in the subsequent DHCPDISCOVER. If the external interface is a PPP link, then the home gateway can use the hardware address of its LAN interface in the htype and chaddr fields.

On receiving one or more DHCP OFFERS, the home gateway configures itself in bridging mode, and does not start the mini-DHCP or BOOTP relay

service on the external interface. It should be noted that in order to properly route packets back to the attached home LANs, the upstream router needs to keep track of the IP addresses assigned to the customer hosts, and plumb corresponding static host routes on its interfaces.

Since ISPs operating in bridging mode typically do not provide unlimited addresses, it is possible that the upstream DHCP server may stop responding after a certain number of addresses have been allocated. In this case it may be desirable for the home gateway to be able to act as a bridge for those hosts that have obtained routable addresses, and a router and mini-DHCP server for those hosts that are not able to do so. However, doing this is tricky because it implies that two address prefixes will co-exist on the home network segment. The home gateway will need to act as a brouter, bridging traffic from the routable addresses, while NAT'ing traffic from the private addresses allocated by the mini-DHCP server. The home gateway will also need to forward traffic from one prefix to the other on the home segment.

[3.](#) Addressing

[3.1.](#) Address allocation

By default, the mini-DHCP server configures itself to serve addresses out of the 192.168/16 scope with /24 prefixes allocated to each interface.

There are ISPs that use private address space internally in order to manage network devices. Thus it is conceivable that a home gateway will receive routing protocol announcements for a subnet of 192.168/16 on one of its interfaces. Were the home gateway to listen to these announcements, it is conceivable that it could become confused about the routing topology.

Thus home gateways implementing this specification MUST filter out routing announcements for the 192.168/16 prefix on the Internet-facing interface.

[3.2.](#) Address selection

Since DHCP servers typically use static addresses, it is desirable for the mini-DHCP server to have its IP addresses be persistent between

reboots. In order to choose an IP address on each interface, the mini-DHCP server will operate as follows:

- [a] The mini-DHCP server will initially claim the .1 address on each interface (e.g. 192.168.1.1, 192.168.2.1, etc.), and then will attempt to determine whether the address is already allocated. This is accomplished by ARPing for the claimed address. If there is no response to the ARP, the mini-DHCP server will utilize the claimed address.
- [b] If the initially claimed address is taken, then the mini-DHCP server will derive the host portion of the address on each interface from the interface MAC address, and will claim and defend that address. The formula for the computation of the host portion of the IPv4 address is as follows:

$$\text{host address} = (\text{0x'FFFF' XOR netmask}) \&\& (\text{CRC32 (MACAddr | hostname | interface-name)})$$

- [c] If both the initially chosen address and the computed address are taken, then the mini-DHCP server will choose a random address.

[3.3.](#) Multi-segment address allocation

It is possible for home networks to include multiple segments. This issue can arise, for example, in the case of a home network supporting [802.11](#) wireless as well as IEEE 1394 and Ethernet.

In multi-segment small networks connected by a single router, it may be desirable to provide for consistent IPv4 addressing in the case where the small network has not been assigned a routable IPv4 address prefix. The router may either be disconnected from the Internet, in which case the hosts on the multiple segments will only be able to reach other, or the router may offer Internet connectivity via Network Address Translation (NAT), described in [\[8\]](#)-[\[10\]](#).

In order to enable effective IPv4 address allocation in multi-segment networks connected by a single router it MUST be possible to consistently assign addresses within multiple segments. Consistent

or between segments. This consistency **MUST** be maintained in the event of addition or removal of segments, or in the event of interfaces going up or down.

In order to ensure consistency of addressing within multiple segments connected to a single router, the mini-DHCP server **MUST** automatically allocate /24 scopes out of the 192.168/16 prefix reserved for private addressing, as described in [\[11\]](#), with a unique /24 prefix allocated to each interface. Prefixes **SHOULD** be allocated from the bottom of the range toward the top, starting with the 192.168.1/24 prefix. The router **MUST NOT** allocate the 192.168.0/24 or 192.168.255/24 prefixes, as these are reserved for future use.

Note that in order to handle the case of interfaces coming up or down, a scope **MUST** be allocated to each interface, whether it is functioning or not. This allows a non-functioning interface to subsequently become functional and to support consistent addressing. In the case where an interface is added, such as by plugging in an additional card, a new scope **SHOULD** be allocated as soon as the interface is added.

In order to allow for consistent numbering between router and host reboots, scope assignments and address allocations should be handled as required by [RFC 2131](#) [\[3\]](#) with respect to use of stable storage. Scopes **MUST NOT** be de-allocated on interface-down or interface removal, so as to remain robust against short term configuration changes.

To enable reclaiming of scopes in the event of permanent removal of an interface, scope allocations of non-existent interfaces should timeout using with an interval of three times the DHCP lease time. For example, if the DHCP lease time is set to 3 days, then a scope allocated to a removed interface will timeout (using an interval of three times) after [9](#) days.

4. References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [2] Droms, R., Arbaugh, W., "Authentication for DHCP Messages", [RFC 3118](#), June 2001. July 2000.
- [3] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.
- [4] Alexander, S., Droms, R., "DHCP Options and BOOTP Vendor Extensions", [RFC 2132](#), March 1997.
- [5] Stapp, M., "Resolution of DNS Name Conflicts Among DHCP Clients", Internet draft (work in progress), [draft-ietf-dhc-ddns-resolution-02.txt](#), July 2001.
- [6] Stapp, M., Rekhter, Y., "The DHCP Client FQDN Option", Internet draft (work in progress), [draft-ietf-dhc-fqdn-option-02.txt](#), July 2001.
- [7] Thomson, S., Narten, T., "IPv6 Stateless Address Autoconfiguration", [RFC 2462](#), December 1998.
- [8] Srisuresh, P., Holdrege, M., "IP Network Address Translator (NAT) Terminology and Considerations", [RFC 2663](#), August 1999.
- [9] Srisuresh, P., Egevang, K., "Traditional IP Network Address Translator (Traditional NAT)", [RFC 3022](#), January 2001.
- [10] Holdrege, M., Srisuresh, P., "Protocol Complications with the IP Network Address Translator", [RFC 3027](#), January 2001.
- [11] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., Lear, E., "Address Allocation for Private Internets", [RFC 1918](#), February, 1996.
- [12] Baker, F., "Requirements for IP Version 4 Routers", [RFC 1812](#), June 1995.
- [13] Mockapetris, P., "Domain Names - Implementation and Specification", [RFC 1035](#), November 1987.
- [14] Mockapetris, P., "DOMAIN NAMES - CONCEPTS AND FACILITIES", [RFC](#)

INTERNET-DRAFT

The Mini-DHCP Server

29 September 2001

- [15] Vixie, P., Thomson, S., Rekhter, Y., Bound, J., "Dynamic Updates in the Domain Name System (DNS UPDATE)", [RFC 2136](#), April 1997.
- [16] Eastlake, D., "Domain Name System Security Extensions", [RFC 2535](#), March 1999.
- [17] Esibov, L., Aboba., B., Thaler, D., "Multicast DNS", Internet draft (work in progress), [draft-ietf-dnsext-mdns-07.txt](#), October 2001.
- [18] 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.
- [19] Cobb, S., "PPP Internet Protocol Control Protocol Extensions for Name Server Addresses", [RFC 1877](#), December 1995.
- [20] Akinlar, C., Braun, D., Mukherjee, S., "Mini-DHCP Election Option For DHCP", Internet draft (work in progress), [draft-akinlar-zeroconf-minidhcp-option-00.txt](#), March 2000.

[5](#). Security Considerations

As noted in [\[2\]](#), DHCP 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 DHCP authentication, 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 DHCP authentication, and that those networks will remain vulnerable to the attacks described in [\[2\]](#).

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 [\[18\]](#).

Where WEP is implemented, an attacker will need to obtain the WEP key prior to gaining access to the home network.

[6.](#) IANA Considerations

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

Aboba

Informational

[Page 10]

INTERNET-DRAFT

The Mini-DHCP Server

29 September 2001

Acknowledgments

This draft has been enriched by comments from Ryan Troll of @Home and Peter Ford and Yaron Goland of Microsoft.

Authors' Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

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

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any

copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2001). 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,

Aboba

Informational

[Page 11]

INTERNET-DRAFT

The Mini-DHCP Server

29 September 2001

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."

Expiration Date

This memo is filed as <[draft-aboba-dhc-mini-04.txt](#)>, and expires April 15, 2002.

