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.

1. Copyright Notice

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

2. 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 implementation that typically resides on the home gateway.

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

3. Introduction

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 implementation that typically resides on the home gateway.
As described in this document, the mini-DHCP server is capable of allocating addresses either in single or multi-segment networks. It is also capable of automatically detecting the presence of a full-fledged DHCP server, or other mini-DHCP servers, and shutting down as required.

3.1. 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.

3.2. 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].

4. Overview

The mini-DHCP server provides DHCP server functionality, as described in [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. 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.
4.1. Dynamic DNS support

The mini-DHCP server SHOULD support the functionality described in [4], enabling dynamic registration of the PTR and (if configured to do so) A records for the hosts to whom it allocates addresses. This will allow the mini-DNS server to resolve DNS queries relating to hosts on the internal network. Queries relating to Internet hosts will be handled by proxying the DNS query to the DNS server configured on the external interface.

4.2. Address selection

Since DHCP servers typically use static addresses, it is desirable for the mini-DHCP server to have its IP addresses be per persistent between reboots. In order to choose an IP address on each interface, the mini-DHCP server will operate as follows:

1. The mini-DHCP server will initially claim the .1 address on each interface (e.g. 192.168.0.1, 192.168.1.1, 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.

2. 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:

   host address = (0x'FFFF' XOR netmask) && (CRC32 (MACAddr | hostname | interface-name ))

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

4.3. 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 router running a mini-DHCP
server MUST send out periodic DHCPDISCOVER requests on each interface with the should-I-autoconfig flag set. If the DHCPDISCOVER is responded to (either with a DHCPOFFER or with a never-autoconfig response), the router MUST NOT provide DHCP service on that interface. Similarly, if the router running a 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 [15], 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 router has detected another DHCP server and has shut down its own mini-DHCP server, it SHOULD set a timer. Once this timer expires, the router 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.

For example, in the case of a bridged network in which addresses are allocated by the ISP DHCP server, hosts may obtain routable addresses via DHCP and therefore it is not necessary for the home gateway to use Network Address Translation.

In order to enable automated detection of bridged versus NATed operation, on bootup, a home gateway sends a DHCPDISCOVER on the Internet-facing interface. On receiving one or more DHCPOFFERS, the home gateway configures itself in bridging mode.

Since ISPs operating in bridging mode typically do not provide unlimited addresses, it is possible that the ISP DHCP server may stop responding after a certain number of addresses have been allocated. In this case it may be desirable for the mini-DHCP server to be able to act as a BOOTP relay agent for those hosts that have obtained routable addresses, and a 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 be co-existing on the same 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.
5. 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 [10], or RSIP, described in [11].

In order to enable effective IPv4 address allocation in multi-segment networks connected by a single router, the following requirements need to be met:

Multi-segment addressing consistency
  It MUST be possible to consistently assign addresses within multiple segments so as to avoid address conflicts either within segments 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.

Auto-config to Non-auto-config transition
  It MUST be possible to effectively transition a series of segments auto-configured as described in [8], to a consistent addressing scheme as described in this document.

Non-auto-config to Auto-config transition
  It SHOULD be possible for auto-configured hosts to be able to converse with non-auto-configured hosts during a period in which a mini-DHCP server is unavailable.

5.1. Addressing scheme

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 [13], 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 [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 after 9 days.

5.2. Transition from auto-config to non-auto-config

In order to allow a series of segments, each auto-configured within the 169.254/16 prefix as described in [8], to transition to a consistently addressed state within the 192.168/16 prefix, the mini-DHCP server will need to respond to the periodic DHCPDISCOVER messages sent by the auto-configured hosts. In the response, the mini-DHCP server will utilize the scope allocations described previously, and will also utilize the option described in [7] in order to discourage hosts from subsequently utilizing auto-configuration should a segment become temporarily disconnected.

Note that the transition from individual auto-configured segments to a consistently addressed multi-segment network may take some time. As described in [8], auto-configured hosts continue to send out DHCPDISCOVER messages in order to be able to reconfigure themselves in the event of the addition of a DHCP server. The suggested default for Ethernet implementations is to check every 5 minutes.

Thus it is conceivable that when the previously partitioned segments are first connected, addressing conflicts may result. As noted in [8], there is currently no way to address this issue without causing all hosts involved to re-configure IP addresses. This will occur within the default reconfiguration interval.

In order to lessen the transition time, it may be desirable to decrease the reconfiguration interval. It also may be useful for nodes detecting an address conflict to send out a DHCPDISCOVER so as to detect the presence of a DHCP server more quickly, or to select another address.
within the auto-config range after detection of a conflict.

5.3. Allocation out of the linklocal scope zone

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.

It is also possible for the mini-DHCP to allocate addresses out of the 169.254/16 linklocal scope. The purpose of doing this would be to enable auto-configured hosts to continue to use their auto-configured addresses rather than having to renumber.

Allocation out of the 169.254/16 linklocal scope is problematic for several reasons. As described in [8], auto-configured hosts periodically attempt to locate a DHCP server by sending DHCPDISCOVERs. However, since these DHCPDISCOVER packets do not contain the auto-configured address, there is no way for the mini-DHCP server to know what address had previously been allocated. Thus it may be necessary for the mini-DHCP server to allocate another address within the 169.254/16 scope. Thus even when allocating out of the 169.254/16 linklocal scope, it does not appear possible to avoid renumbering.

Other problems arise as well. When allocating out of the 169.254/16 linklocal scope, addressing conflicts are likely. Therefore the mini-DHCP server must take extra care to check that an address is not in use before allocating it. In addition to measures described in [3], such as attempting to ping the address, it is also recommended that the mini-DHCP server allocating out of the 169.254/16 scope utilize the claim and defend techniques described in [8] to determine whether the address is already in use. Since addresses within the 169.254/16 scope are linklocal, all such hosts can be reached via an ARP broadcast.

As a result of these issues, mini-DHCP servers SHOULD NOT allocate out of the 169.254/16 linklocal scope.

6. References


7. Security Considerations

DHCP, as noted in [2], 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 [9]. Where WEP is implemented, an attacker will need to obtain the WEP key prior to gaining access to the home network.

8. IANA Considerations

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

9. Acknowledgements

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

10. Authors’ Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

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

11. 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.

12. 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."

13. Expiration Date

This memo is filed as <draft-aboba-dhc-mini-00.txt>, and expires November 1, 2000.