NETWORK Working Group
INTERNET-DRAFT
Category: Informational
<draft-aboba-zeroconf-multi-00.txt>
6 October 1999

Bernard Aboba
Microsoft

Auto-Addressing in Multi-segment Networks

1. Copyright Notice

2. Abstract

Today, with the rapid rise of home networking, there is an increasing need for simplified mechanisms for IPv4 address allocation within multi-segment networks connected by a single router. This issue can arise, for example, in the case of a home network supporting 802.11 wireless as well as 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. This draft describes how this problem may be solved through implementation of a mini-DHCP server within the router. 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), or another suitable mechanism, such as RSIP.

3. Introduction

Today, with the rapid rise of home networking, there is an increasing need for simplified mechanisms for IPv4 address allocation within multi-segment networks connected by a single router. This issue can arise, for example, in the case of a home network supporting 802.11 wireless as well as 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. This draft describes how this problem may be solved through implementation of a mini-DHCP server within the router. 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 another suitable mechanism, such as RSIP, described in [11].

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].

3.3. Configuration requirements for multi-segment networks

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 adressing 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.

4. Addressing scheme

In order to provide addressing consistency in multi-segment IPv4 networks connected to a single router, this document proposes addition of a mini-DHCP server to the router. In order to ensure consistency of addressing within the multiple segments, 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.

4.1. Compatibility with existing DHCP servers

A mini-DHCP server MUST NOT be active on an interface if there is already another DHCP server active on that interface. Thus if the

router'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.

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.

4.2. Compatibility with private address spaces

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

Thus routers implementing this specification MUST filter out routing announcements for the 192.168/16 prefix on all interfaces.

4.3. 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. 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", Internet draft (work in progress), draft-ietf-dhc-authentication-11.txt, June 1999.

[3] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[5] Alexander, S., Droms, R., "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[6] Thomson, S., Narten, T., "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[7] Troll, R., "DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients", RFC 2563, May 1999.

[8] Troll, R., "Automatically Choosing an IP Address in an Ad-Hoc IPv4 Network", Internet draft (work in progress), draft-ietf-dhc-ipv4-autoconfig-04.txt, April 1999.

[9] IEEE 802.11 specification.

[10] Srisuresh, P., Holdrege, M., "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[11] Lo, J., Borella, M., Grabelsky, D., "Realm Specific IP: A Framework", Internet draft (work in progress), draft-ietf-nat-rsip-framework-01.txt, November 1999.

[12] Thomson, S. and Narten, T., "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[13] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., Lear, E., "Address Allocation for Private Internets", RFC 1918, February, 1996.

6. 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.

7. IANA Considerations

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

8. Acknowledgements

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

9. Authors' Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

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

10. 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.

11. Full Copyright Statement

12. Expiration Date

This memo is filed as <draft-aboba-zeroconf-multi-00.txt>, and expires April 1, 2000.