DHC Working Group
INTERNET-DRAFT
Category: Proposed Standard
<draft-ietf-dhc-dna-ipv4-15.txt>
9 August 2005

Bernard Aboba
Microsoft Corporation

Detecting Network Attachment (DNA) in IPv4

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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.

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

This Internet-Draft will expire on February 10, 2006.

Copyright Notice

Copyright (C) The Internet Society 2005.

Abstract

The time required to detect movement between networks, and to obtain (or continue to use) an IPv4 configuration may be significant as a fraction of the total handover latency in moving between points of attachment. This document synthesizes from experience in the deployment of hosts supporting ARP, DHCP, and IPv4 Link-Local addresses a set of steps known as Detecting Network Attachment for IPv4 (DNAv4), in order to decrease the handover latency in moving between points of attachment.

Table of Contents

1. Introduction

The time required to detect movement between networks and to obtain (or continue to use) an operable IPv4 configuration may be significant as a fraction of the total handover latency in moving between points of attachment.

This document synthesizes from experience in the deployment of hosts supporting ARP [RFC826], DHCP [RFC2131], and IPv4 Link-Local addresses [RFC3927] a set of steps known as Detecting Network Attachment for IPv4 (DNAv4). DNAv4 optimizes the (common) case of reattachment to a network that one has been connected to previously by attempting to re-use a previous (but still valid) configuration, reducing the reattachment time to a few milliseconds on LANs. Since this procedure is dependent on the ARP protocol, it is not suitable for use on media that do not support ARP.

1.1. Requirements

In this document, several words are used to signify the requirements of the specification. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.2. Terminology

This document uses the following terms:

ar$sha
: ARP packet field: Sender Hardware Address [RFC826]. The hardware (MAC) address of the originator of an ARP packet.

ar$spa
: ARP packet field: Sender Protocol Address [RFC826]. For IP Address Resolution this is the IPv4 address of the sender of the ARP packet.

ar$tha
: ARP packet field: Target Hardware Address [RFC826]. The hardware (MAC) address of the target of an ARP packet.

ar$tpa
: ARP packet field: Target Protocol Address [RFC826]. For IPv4 Address Resolution, the IPv4 address for which one desires to know the hardware address.

DHCP client
: A DHCP client or "client" is an Internet host using the Dynamic Host Configuration protocol (DHCP) [RFC2131] 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.

Link
: A communication facility or medium over which network nodes can communicate. Each link is associated with a minimum of two endpoints. Each link endpoint has a unique link-layer identifier.

Link Down
: An event provided by the link layer that signifies a state change associated with the interface no longer being capable of communicating data frames; transient periods of high frame loss are not sufficient. DNAv4 does not utilize "Link Down" indications.

Link Layer
: Conceptual layer of control or processing logic that is responsible for maintaining control of the data link. The data link layer functions provide an interface between the higher-layer logic and the data link. The link layer is the layer immediately below IP.

Link Up
: An event provided by the link layer that signifies a state change associated with the interface becoming capable of communicating data frames.

Most Likely Networks (MLNs)
: The attached network(s) determined by the host to be most likely.

Point of Attachment
: The link endpoint on the link to which the host is currently connected.

Routable address
: In this specification, the term "routable address" refers to any IPv4 address other than an IPv4 Link-Local address. This includes private addresses as specified in [RFC1918].

Operable address
: In this specification, the term "operable address" refers to either a static IPv4 address, or an address assigned via DHCPv4 which has not been relinquished, and whose lease has not yet expired.

2. Overview

DNAv4 consists of three phases: determination of the Most Likely Networks (MLNs), reachability testing, and IPv4 address acquisition.

On connecting to a new point of attachment, the host responds to a "Link Up" indication from the link layer by carrying out the DNAv4 procedure. Based on the networks that the host has most recently connected to as well as hints available from the link and Internet layers, the host determines the "Most Likely Networks" (MLNs) and determines whether it has an operable IPv4 configuration associated with each of them.

If the host believes that it has an operable IPv4 configuration on a MLN, it performs a reachability test in order to confirm that configuration. The reachability test is designed to verify bi-directional connectivity to the default gateway(s) on the MLN. If the reachability test is successful, the host SHOULD continue to use an operable routable IPv4 address without needing to re-acquire it, thereby allowing the host to bypass DHCPv4 as well as Duplicate Address Detection (DAD).

Since DNAv4 represents a performance optimization, it is important to avoid compromising robustness. In some circumstances, DNAv4 may result in a host successfully verifying an existing IPv4 configuration where attempting to obtain configuration via DHCPv4 would fail (such as when the DHCPv4 server is down).

To improve robustness, this document suggests that hosts behave conservatively with respect to assignment of IPv4 Link-Local addresses [RFC3927], configuring them only in situations in which they can do no harm. Experience has shown that IPv4 Link-Local addresses are often assigned inappropriately, compromising both performance and connectivity.

In implementations where MLN selection is dependent on hints provided to the client, the performance of DNAv4 may be dependent on the reliability of the hints. However, the host will ultimately determine the correct IPv4 configuration even in the presence of misleading hints.

Where there is more than one MLN, the host can test reachability to the MLNs in serial or in parallel. An implementation can also attempt to obtain IPv4 configuration via DHCPv4 in parallel with one or more reachability tests, with the host using the first answer returned. These optimizations improve performance and reduce the reliance on link and Internet layer hints, which may not be present or may be misleading.

Attempting to obtain IPv4 configuration via DHCPv4 in parallel with reachability testing is particularly valuable in implementations that only test reachability of a single MLN. Since confirming failure of a reachability test requires a timeout, mistakes are costly and sending a DHCPREQUEST from the INIT-REBOOT state, as described in [RFC2131] Section 3.2 and 4.3.2 may complete more quickly than the reachability test.

DNAv4 does not increase the likelihood of an address conflict. The DNAv4 procedure is only carried out when the host has an operable IPv4 configuration on one or more MLNs, implying that duplicate address detection has previously been completed. Restrictions on sending ARP Requests and Responses are described in Section 2.2.1.

2.1. Most Likely Networks (MLNs)

In order to determine the MLN(s), it is assumed that the host saves to stable storage parameters relating to the networks it connects to:

[1] The IPv4 and MAC address of the default gateway(s) on each network.

[2] The link type, such as whether the link utilizes Ethernet, or 802.11 adhoc or infrastructure mode.

[3] Link and Internet layer hints associated with each network. Appendix A discusses hints useful for the determination of MLNs.

An implementation may select one or more MLNs by matching received hints against network parameters previously stored, by including networks it has most recently connected to, or by some combination of these strategies.

2.2. Reachability Test

If the host has an operable routable IPv4 address on a MLN, a host conforming to this specification SHOULD perform a reachability test for that MLN, in order to confirm the configuration.

The host skips the reachability test for a MLN if any of the following conditions are true:

[a] The host does not have an operable routable IPv4 address on a MLN. In this case, the reachability test cannot confirm that the host has an operable routable IPv4 address, so completing the reachability test would serve no purpose.

A host MUST NOT use the reachability test to confirm configuration of an IPv4 Link-Local address.

[b] The host does not know the default gateway(s) on a MLN. In this case, insufficient information is available to carry out the reachability test.

[c] If secure detection of network attachment is required. The reachability test utilizes ARP which is insecure, whereas DHCPv4 can be secured via DHCPv4 authentication, described in [RFC3118]. See Section 5 for details.

For a particular MLN, the host MAY test the reachability of the primary default gateway, or it MAY test reachability of the primary and secondary default gateways in series or in parallel. In order to ensure configuration validity, the host SHOULD only configure default gateway(s) which pass the reachability test.

In situations where more than one network is available on a given link, and more than one reachability test is performed in parallel, potentially with an attempt to obtain IPv4 configuration via DHCPv4, it is possible for the host to confirm more than one configuration. In this case, a DNAv4 implementation SHOULD prefer the configuration provided via DHCPv4.

2.2.1. Packet Format

The reachability test is performed by sending an ARP Request. The host MUST set the target protocol address (ar$tpa) to the IPv4 address of the default gateway being tested, and the sender protocol address field (ar$spa) to its own IPv4 address. The ARP Request MUST use the host's MAC address as the source, and the default gateway MAC address as the destination. The host includes its MAC address in the sender hardware address field (ar$sha), and sets the target hardware address field (ar$tha) to 0.

If a valid ARP Reply is received, the MAC address in the sender hardware address field (ar$sha) in the ARP Reply is matched against the target hardware address field (ar$tpa) in the ARP Request, and the and the IPv4 address in the sender protocol address field (ar$spa) of the ARP Reply is matched against the target protocol address field (ar$tpa) in the ARP Request. If a match is found, then if the host has an operable routable IPv4 address on the matched network, the host continues to use that IPv4 address, subject to the lease re- acquisition and expiration behavior described in [RFC2131], Section 4.4.5.

The risk of an address conflict is greatest when the host moves between private networks, since in this case the completion of Duplicate Address Detection on the former network does not provide assurance against an address conflict on the new network. Until a host with a private address has confirmed the operability of its IPv4 configuration, it SHOULD NOT respond to ARP Requests, and SHOULD NOT broadcast ARP Requests containing its address within the sender protocol address field (ar$spa). However, where the host has an operable routable non-private address on a MLN, it MAY send ARP Requests using its address within the sender protocol address field (ar$spa) prior to confirming its IPv4 configuration, and MAY respond to ARP Requests.

Sending an ICMP Echo Request [RFC792] to the default gateway IPv4 address does not provide the same level of assurance since this may require an ARP Request/Reply exchange. Where the host has moved between two private networks, this could result in ARP cache pollution.

Where a host moves from one private network to another, an ICMP Echo Request can result in an ICMP Echo Response even when the default gateway has changed, as long as the IPv4 address remains the same. This can occur, for example, where a host moves from one home network using prefix 192.168/16 to another one. In addition, if the ping is sent with TTL > 1, then an ICMP Echo Response can be received from an off-link gateway. As a result, if the MAC address of the default gateway is not checked, the host can mistakenly confirm attachment to a MLN, potentially resulting in an address conflict. As a result, sending of an ICMP Echo Request SHOULD NOT be used as a substitute for the DNAv4 procedure.

If the initial ARP Request does not elicit a response, the host waits for REACHABILITY_TIMEOUT. Where IPv4 address acquisition occurs in parallel, the host MAY retransmit; otherwise the host SHOULD move on to the IPv4 address acquisition phase. If a valid ARP Reply is received, but cannot be matched against known networks, the host assumes it does not have an operable IPv4 configuration.

2.3. IPv4 Address Acquisition

If the host has an operable routable IPv4 address on one or more MLNs, but the reachability test(s) fail, the host SHOULD attempt to revalidate the configuration by entering the INIT-REBOOT state, and sending a DHCPREQUEST to the broadcast address as specified in [RFC2131] Section 4.4.2. As noted in Section 2, it is also possible for IPv4 address acquisition to occur in parallel with the reachability test.

If the host does not have an operable routable IPv4 address on any MLN, the host enters the INIT state and sends a DHCPDISCOVER packet to the broadcast address, as described in [RFC2131] Section 4.4.1. If the host supports the Rapid Commit Option [RFC4039], it is possible that the exchange can be shortened from a 4-message exchange to a 2-message exchange.

If the host does not receive a response to a DHCPREQUEST or DHCPDISCOVER, then it retransmits as specified in [RFC2131] Section 4.1.

As discussed in [RFC2131], Section 4.4.4, a host in INIT or REBOOTING state that knows the address of a DHCP server may use that address in the DHCPDISCOVER or DHCPREQUEST rather than the IPv4 broadcast address. In the INIT-REBOOT state a DHCPREQUEST is sent to the broadcast address so that the host will receive a response regardless of whether the previously configured IPv4 address is correct for the network to which it has connected.

Sending a DHCPREQUEST to the unicast address in INIT-REBOOT state is not appropriate, since if the DHCP client has moved to another subnet, a DHCP server response cannot be routed back to the client since the DHCPREQUEST will bypass the DHCP relay and will contain an invalid source address.

2.4. IPv4 Link-Local Addresses

To avoid inappropriate assignment of IPv4 Link-Local addresses, it is recommended that hosts behave conservatively, assigning them only when they can do no harm. As described in [RFC3927] Section 1.9, use of a routable address is preferred when it is available:

2. If a host finds that an interface that was previously configured with an IPv4 Link-Local address now has an operable routable address available, the host MUST use the routable address when initiating new communications, and MUST cease advertising the availability of the IPv4 Link-Local address through whatever mechanisms that address had been made known to others.

Where the host does not have an operable routable IPv4 address on any MLN, the host MAY configure an IPv4 Link-Local address prior to entering the INIT state and sending a DHCPDISCOVER packet, as described in [RFC2131] Section 2.3. However, should a routable IPv4 address be obtained, the IPv4 Link-Local address is deprecated, as noted in [RFC3927] Section 1.9.

Where a host has an operable routable IPv4 address on one or more

MLNs, but the DHCP client does not receive a response after employing the retransmission algorithm, [RFC2131] Section 3.2 states that the client MAY choose to use the previously allocated network address and configuration parameters corresponding to one of the MLNs for the remainder of the unexpired lease. Where a host can confirm that it remains connected to a network on which it possesses an operable routable IPv4 address, that address SHOULD be used, rather than assigning a IPv4 Link-Local address.

Since a IPv4 Link-Local address is often configured because a DHCP server failed to respond to an initial query or is inoperative for some time, it is desirable to abandon the IPv4 Link-Local address assignment as soon as an IPv4 address lease can be obtained.

As described in [RFC3927] Appendix A, once a Link-Local IPv4 address is assigned, existing implementations do not query the DHCPv4 server again for five minutes. This behavior violates [RFC2131] Section 4.1:

> The retransmission delay SHOULD be doubled with subsequent retransmissions up to a maximum of 64 seconds.

Instead of waiting for five minutes, a DHCP client should continue to retry every 64 seconds, even after allocating a IPv4 Link-Local address. If the DHCP client succeeds in obtaining a routable address, then the IPv4 Link-Local address is deprecated, as noted in [RFC3927] Section 1.9.

Since it is inevitable that hosts will inappropriately configure IPv4 Link-Local addresses at some point, hosts with routable IPv4 addresses need to be able to respond to peers with IPv4 Link-Local addresses, as per [RFC3927] Section 1.8. For example, a host configured with a routable address may receive a datagram from a link-local source address. In order to respond, the host will use ARP to resolve the target hardware address and send the datagram directly, not to a router for forwarding.

3. Constants

The suggested default value of REACHABILITY_TIMEOUT is 200 ms. This value was chosen so as to accommodate the maximum retransmission timer likely to be experienced on an Ethernet network.

4. IANA Considerations

This specification does not request the creation of any new parameter registries, nor does it require any other IANA assignments.

5. Security Considerations

Detecting Network Attachment for IPv4 (DNAv4) is based on ARP and DHCP and inherits the security vulnerabilities of these two protocols.

ARP [RFC826] traffic is not secured, so that an attacker gaining access to the network can spoof a response to the reachability test described in Section 2.2, leading the querier to falsely conclude that it is attached to a network that it is not connected to.

Similarly, where DHCPv4 traffic is not secured, an attacker could masquerade as a DHCPv4 server, in order to convince the host that it was attached to a particular network. This and other threats relating to DHCPv4 are described in "Authentication for DHCP Messages" [RFC3118].

The effect of these attacks will typically be limited to denial of service, unless the host utilizes its IP configuration for other purposes, such as security configuration or location determination. For example, a host that disables its personal firewall based on evidence that it had attached to a home network could be compromised by spoofing of the DNAv4 reachability test. In general, adjustment of the security configuration based on DNAv4 is NOT RECOMMENDED.

Hosts that depend on secure IP configuration SHOULD NOT use DNAv4, but SHOULD instead utilize DHCP authentication [RFC3118], possibly in combination with the Rapid Commit Option [RFC4039].

6. References

6.1. Normative References

[RFC792] Postel, J., "Internet Control Message Protocol", RFC 792, USC/Information Sciences Institute, September 1981.

[RFC826] D. Plummer, "An Ethernet Address Resolution Protocol -or- Converting Network Addresses to 48-bit Ethernet Address for Transmission on Ethernet Hardware", STD 37, RFC 826, November 1982.

[RFC1256] Deering, S., "ICMP Router Discovery Messages", RFC 1256, Xerox PARC, September 1991.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March, 1997.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC3118] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

[RFC3927] Cheshire, S., Aboba, B. and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", RFC 3927, May 2005.

6.2. Informative References

[DNALINK] Yegin, A., Njedjou, E., Veerepalli, S., Montavont, N. and T. Noel, "Link-layer Event Notifications for Detecting Network Attachments", draft-ietf-dna-link-information-01.txt, February 2005.

[RFC1058] Hedrick, C., "Routing Information Protocol", RFC 1058, June 1988.

[RFC1661] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, Daydreamer, July 1994.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. and E. Lear, "Address Allocation for Private Internets", RFC 1918, February 1996.

[RFC2453] Malkin, G., "RIP Version 2", RFC 2453, STD 56, November 1998.

[RFC3580] Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, September 2003.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC4039] Park, S., Kim, P., and B. Volz, "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)", RFC 4039, March 2005.

[IEEE-802.1AB]
IEEE Standards for Local and Metropolitan Area Networks: Station and Media Access Control - Connectivity Discovery, IEEE Std 802.1AB, March 2005.

[IEEE-802.1X]
IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2004, December

2004.

[IEEE-802]
IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, ANSI/IEEE Std 802, 1990.

[IEEE-802.1Q]
IEEE Standards for Local and Metropolitan Area Networks: Draft Standard for Virtual Bridged Local Area Networks, P802.1Q, January 1998.

[IEEE-802.11]
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. 802.11-2003, 2003.

Acknowledgments

The authors would like to acknowledge Greg Daley of Monash University, Erik Guttman, James Carlson, and Erik Nordmark of Sun Microsystems, Ralph Droms of Cisco Systems, Ted Lemon of Nominum, John Loughney of Nokia, Thomas Narten of IBM, Stuart Cheshire of Apple Computer and David Hankins of ISC for contributions to this document.

Authors' Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

EMail: bernarda@microsoft.com
Phone: +1 425 818 4011
Fax: +1 425 936 7329

Appendix A - Hints

A.1 Introduction

In order to assist in detecting network attachment, information associated with each network may be retained by the host. Based on Internet and link-layer information, the host may be able to make an educated guess as to whether it has moved between networks, or has remained on the same network, as well as whether it has connected to an infrastructure or adhoc network.

If the host is likely to have moved between networks, it may be possible to make an educated guess as to which network it has moved to. Since an educated guess may be incorrect, prior to concluding that the host remains on the same network, further tests (such as a reachability test or a DHCPREQUEST sent from the INIT-REBOOT state) are REQUIRED.

In practice, it is necessary for hints to be highly reliable before they are worth considering, if the penalty paid for an incorrect hint is substantial. For this reason, implementations may wish to test reachability to multiple MLNs simultaneously, or attempt IPv4 address acquisition in parallel with one or more reachability tests.

In order to examine the tradeoffs in implementations that only test reachability to a single MLN, assume that a DHCPREQUEST requires DHCPREQUEST_TIME to determine if a host has remained on the same network, while a reachability test typically completes in REACH_TIME and times out in REACHABILITY_TIMEOUT, after which a DHCPREQUEST is sent.

If a hint that the host has remained on the same network cannot be confirmed x fraction of the time, then it is only worth considering if:

$$\text{DHCPREQUEST\_TIME} > (1 - x) * \text{REACH\_TIME} + x * (\text{REACHABILITY\_TIMEOUT} + \text{DHCPREQUEST\_TIME})$$

$$x < \frac{\text{DHCPREQUEST\_TIME} - \text{REACH\_TIME}}{\text{REACHABILITY\_TIMEOUT} + \text{DHCPREQUEST\_TIME} - \text{REACH\_TIME}}$$

If we assume that DHCPREQUEST_TIME = 50 ms, REACH_TIME = 10 ms, and REACHABILITY_TIMEOUT = 200ms, then:

$x < (50 - 10)/(200 + 50 - 10) = 16.67$ percent

In this example, if the hint cannot be confirmed more than one sixth of the time, it is not worth considering. A hint may not be confirmable because it is wrong (the host has changed networks) or because of packet loss in the reachability test.

If instead in the above example IPv4 address acquisition were carried out simultaneously with the reachability test, then performance would not suffer, even where hints are unreliable.

A.2 Link-Layer Hints

"Link-layer Event Notifications for Detecting Network Attachments" [DNALINK] discusses the definition of link layer events on various media. Therefore this section focuses solely on hints useful in determining MLN(s).

For networks running IPv4 over PPP [RFC1661], IPv4 parameters negotiated in IPCP provide direct information on whether a previously obtained address remains operable on the link.

On media supporting EAP [RFC3748], network identification information may be passed within the EAP-Request/Identity or within an EAP method exchange. For example, the EAP-Request/Identity may contain the name of the authenticator. During the EAP method exchange the authenticator may supply information that may be helpful in identifying the network to which the device is attached. However, as noted in [RFC3580], it is possible for the VLANID defined in [IEEE-802.1Q] to be assigned dynamically, so that static advertisements may not prove definitive.

On IEEE 802 [IEEE-802] wired networks, hints can be obtained via the Link Layer Discovery Protocol (LLDP) defined in [IEEE-802.1AB]. LLDP advertisements can include the chassis ID, which represents the authenticator's chassis identification, enabling a host to determine if it has attached to a previously encountered device. However, since a device may support dynamic VLANs, re-attachment does not necessarily imply that the VLAN has remained the same, although this is likely.

LLDP also enables advertisement of the port's VLAN identifier, as well as a VLAN name, allowing the host to determine whether it has attached to a VLAN on which it had previously obtained an operable IPv4 configuration. Since such an advertisement cannot be heard until 802.1X authentication has completed, the advertised VLAN will reflect a dynamic VLAN assignment if one has been made, so that it is likely to be definitive.

In IEEE 802.11 [IEEE-802.11] stations provide information in Beacon

and/or Probe Response messages, such as the SSID, BSSID, and capabilities, as well as information on whether the station is operating in Infrastructure or Ad hoc mode. As described in [RFC3580], it is possible to assign a Station to a VLAN dynamically, based on the results of IEEE 802.1X [IEEE-802.1X] authentication. This implies that a single SSID may offer access to multiple VLANs, and in practice most large WLAN deployments offer access to multiple subnets. While a Station associating to the same SSID may not remain within the same subnet, a Station associating to a different SSID is likely to have changed subnets.

In IEEE 802.11, the SSID is a non-unique identifier, and SSIDs such as "default", "linksys" and "tsunami" are often configured by manufacturers by default. As a result, matching an advertised SSID against those of previously encountered networks may be misleading. Where an SSID known to be configured by default is encountered, it is recommended that the BSSID be stored and subsequently compared against the advertised BSSID to determine whether a match exists.

In order to provide additional guidance on the subnets to which a given AP offers access, additional subnet-related Information Elements (IEs) have been proposed for addition to the IEEE 802.11 Beacon and Probe Response messages. As noted earlier, VLANs may be determined dynamically so that these information elements may not be reliable.

In IEEE 802.11, the presence of an IBSS can be used as a hint that a link supports adhoc networking, and therefore that assignment of a IPv4 Link-Local address is likely. When running IPv4 over PPP, if an IPv4 address is not statically configured or assigned via IPv4CP, this can also be taken as a hint that assignment of an IPv4 Link-Local address is likely. Media such as USB or IEEE 1394 may be considered inherently more likely to support adhoc operation, so that attachment to these media may by itself be considered a hint.

A.3 Internet Layer Hints

Aside from utilizing link layer indications, a host may also be able to utilize Internet layer information in order to determine MLN(s). IPv4 ICMP Router Discovery messages [RFC1256] provide information relating to prefix(es) available on the link, as well as the routers that serve those prefix(es). A host may use ICMP Router Discovery to conclude that an advertised prefix is available; however it cannot conclude the converse -- that prefixes not advertised are unavailable.

However, since [RFC1256] is not widely implemented, it is NOT RECOMMENDED that hosts utilize ICMP Router Discovery messages as an

alternative to the reachability test outlined in Section 2.2. Instead, ICMP Router Advertisements can be used to obtain information on available prefixes and default gateway(s). This can provide additional resilience in the case where default gateway(s) become unavailable.

Similarly hosts that support routing protocols such as RIP [RFC2453] can use these protocols to determine the prefix(es) available on a link and the default gateway(s) that serve those prefixes. Full support is not required to glean this information. A host that passively observes routing protocol traffic may deduce this information without supporting a fully conformant routing protocol implementation. For a description of "Silent RIP", see [RFC1058] Section 3.1.

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

Open issues

Open issues relating to this specification are tracked on the following web site:

http://www.drizzle.com/~aboba/DNA/