Individual Submission
Internet Draft
Intended status: Experimental
Expires: April 2009

T. Savolainen
Nokia

October 23, 2008

Domain name based network interface selection
draft-savolainen-6man-fqdn-based-if-selection-00.txt

Status of this Memo

Abstract

A multi-homed host with multiple physical and/or virtual network interfaces has to select which one of the network interfaces to use for a new outgoing IPv4 or IPv6 connection. This document describes a method to select an interface by using destination's fully qualified domain name and DNS suffix information received dynamically for each network interface. The method is useful, for example, in split horizon DNS and walled garden scenarios, where right network interface has to be selected even before DNS resolution is conducted.

Table of Contents

1. Introduction

A host initiating an IP connection commonly uses destination's fully qualified domain name (FQDN). The FQDN has to be first resolved into an IP address with help of DNS, and afterwards the connection is created to one of the resolved IP addresses. The source and destination IP addresses that are used for the connection are determined by host's address selection algorithms, like the one defined for IPv6 in [RFC3484].

A multi-homed host may do network interface selection as part of host's source address selection algorithm. A host may also be configured to use only single network interface at any given time or for a given application.

This document identifies three problematic scenarios a multi-homed host may encounter and for which solutions are needed. The problems are listed below and described in detail in chapter 3:

1. Split horizon DNS

2. Firewalled walled gardens

3. Seemingly equal interfaces

An example of an application facing these problems is a web browser, which in multi-homed environments may need to dynamically access content over different network interfaces.

As a possible solution for these problems a method is described in chapter 4 that uses DNS suffixes for determining the best network interface for DNS resolution and for connecting to a given FQDN.

The solution presented in this memo is intended to be fully backwards compatible and one that can be fully ignored by hosts and networks that are not experiencing the described problem scenarios.

2. Conventions used in this document

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 RFC-2119 [RFC2119].

3. Problem descriptions

This chapter describes three multi-homing related problem scenarios for which the DNS suffix based network interface selection solution described in chapter 4 is targeted at. The scenarios are not excluding each other, but shown separately for sake of simplicity.

3.1. Split horizon DNS

A multi-homed host may be connecting to one or more networks that are using private fully qualified domain names. For example, the host may have simultaneously open a wireless LAN (WLAN) connection to open Internet, cellular (3GPP) connection to an operator network, and virtual private network (VPN) connection to a corporate network. When an application initiates connection to a FQDN, the host needs to be able to choose the right network interface for making successful DNS query. This is illustrated in figure 1. If the FQDN is for a public name, in figure 1 scenario it could be resolved with any DNS server in any network interface, but if the FQDN would be corporation's or operator's service's private name, the host would need to be able to correctly select the right network interface for DNS procedures, i.e. already before destination's IP address is known.

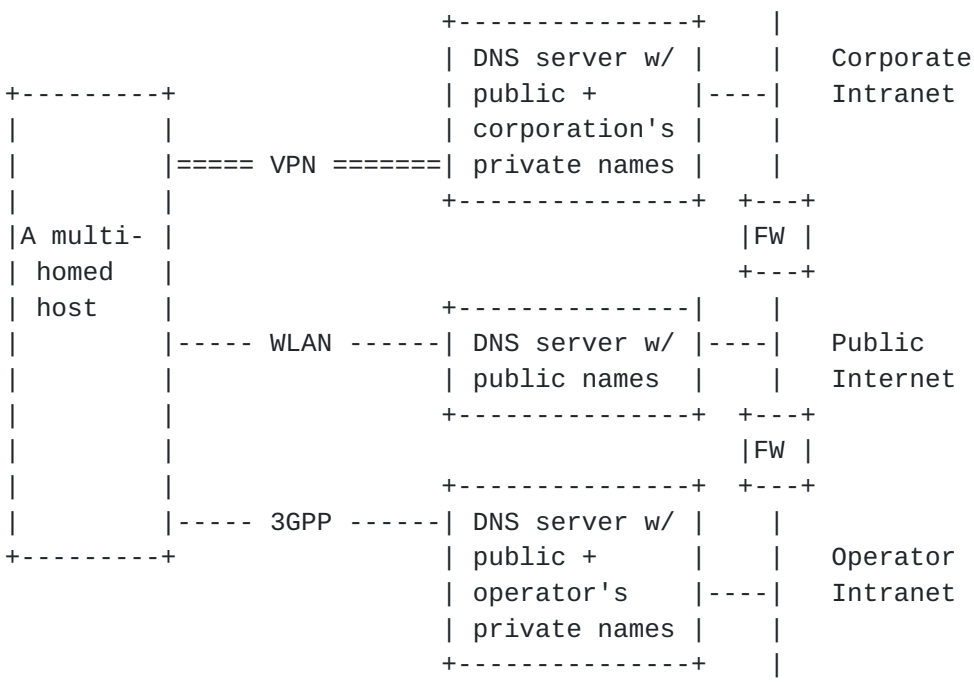


Figure 1 Split horizon DNS and firewalled walled gardens scenarios illustrated

3.2. Firewalled walled gardens

The firewalled walled gardens scenario is similar to what was described in 3.1 and figure 1, except that all DNS resolutions could be conducted with any DNS server over any network interface. However, for the actual IP connection creation to succeed right interface must be chosen, as otherwise firewalls at the edge of walled garden would block the incoming connection request. For example, a name of a server in operator's private network could be resolved to an IP address with any DNS server, but it could be contacted only over direct access to operator's network.

3.3. Seemingly equal interfaces

In third problematic scenario there are no firewalls and all DNS servers have all information, but traffic for certain destinations are preferred to be transmitted over certain network interface rather than others. The reasons can be, for example, route optimization or quality of service related. For example, if a host has two seemingly equal network interfaces from its point of view, the network operator(s) of both or one of the network(s) may be interested to guide a host to make better network interface selection decisions.

Figure 2 illustrates an example case where a multi-homed host should choose network interface A for contacting server 1 but interface B for contacting server 2, in order to select shortest path. This can be important e.g. if the two paths have significant geographical distance differences and thus different cost incurred for the network operator(s). A host sticking to using only interface A would be able to access both servers 1 and 2, but it would be suboptimal performance and network load/cost-wise.

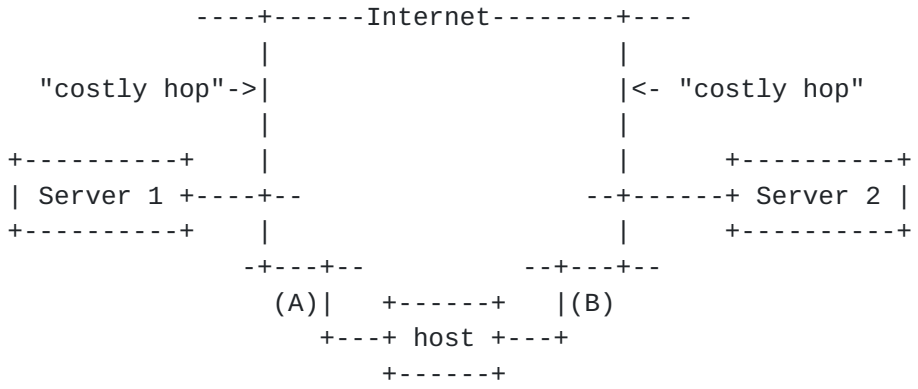


Figure 2 A multi-homed host with two seemingly equal network interfaces (from IP point of view)

Figure 3 illustrates case where a multi-homed host should choose network interface A for contacting real-time service 1 but interface B for non-real-time service 2. A host could contact service 1 via either interface, but using interface A provides better experience for real-time services (e.g. low latency) while interface B provides better experience for non-real-time services (e.g. high bandwidth).

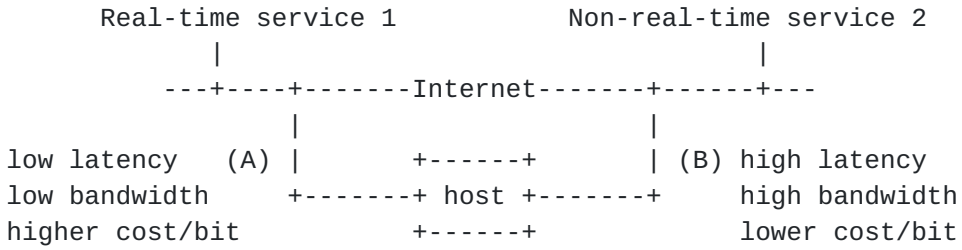


Figure 3 A multi-homed host with two network interfaces having different characteristics

It is worth noting that in IPv4 domain both A and B network interfaces, of figures 2 and 3, may be using private IPv4 [RFC1918] addresses, which makes IPv4 address based interface selection difficult. In IPv6 domain source address selection mechanisms such as defined in [RFC3484] and worked on e.g. in [MATS2008] and [FUJI2008] can be used to tackle seemingly equal interfaces problem.

4. DNS suffix based interface selection

This chapter contains a solution approach and a solution for the problems described in chapter 3.

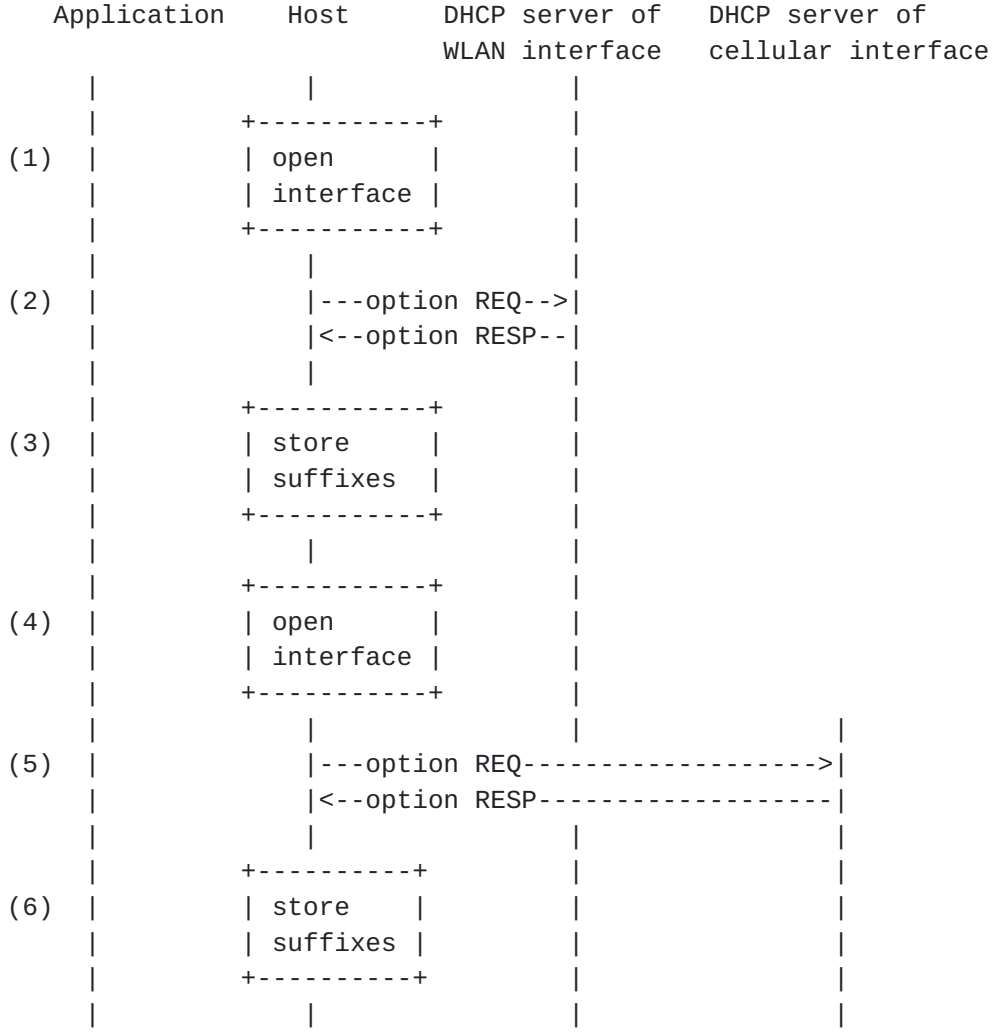
A host SHOULD learn which DNS suffixes in particular are resolvable, and accessible, via each network interface. By default a host MUST assume all FQDNs can be resolved and accessed via any network interface. When a connection is to be created to a FQDN, a host SHOULD prioritize available network interfaces for DNS resolution and address selection purposes based on possibly matching DNS suffix information.

This document describes how existing DHCP(v6) DNS search list options can be used for this purpose.

4.1. Learning of the DNS suffixes

A host can learn the DNS suffixes of attached network interfaces from DHCP search list options; DHCPv4 Domain Search Option number 119 [RFC3397] and DHCPv6 Domain Search List Option number 24 [RFC3646].

This is illustrated in example message flow 1 below.



Message flow 1: Learning DNS suffixes

Flow explanations:

(1) A host opens its first network interface, say WLAN

(2) The host obtains DNS suffix information for the new WLAN interface from DHCP server

(3) The host stores the learned DNS suffixes for later use

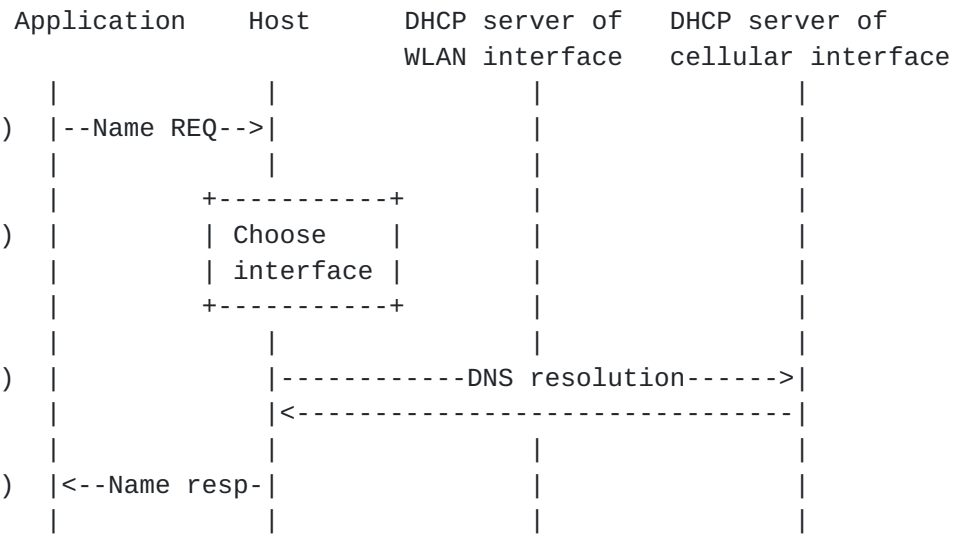
(4) The host opens its seconds network interface, say cellular

(5) The host obtains DNS suffix, say "operator.com" information for the new cellular interface from DHCP server

(6) The host stores the learned DNS suffixes for later use

4.2. Changes to DNS resolution procedures

When a DNS resolver in a host is requested by an application to do DNS resolution for a FQDN to an IP address, the host SHOULD look if any of the available network interfaces is known to advertise DNS suffix matching to the FQDN. If there is a matching DNS suffix, then that particular interface should be used for name resolution procedures. This is illustrated in example message flow 2 below.



Message flow 2: Choosing interface based on DNS suffix

Flow explanations:

(1) An application makes a request for resolving a FQDN, e.g. "private.operator.com"

(2) A host looks at stored DNS suffix information and chooses interface to use for DNS resolution

(3) The host has chosen cellular interface, as from DHCP it was learned that the cellular interface has DNS suffix "operator.com", and resolves the requested name using cellular interface's DNS server to IP 192.0.2.1

(4) The host replies to application with resolved address 192.0.2.1

4.3. Changes to host's address selection procedures

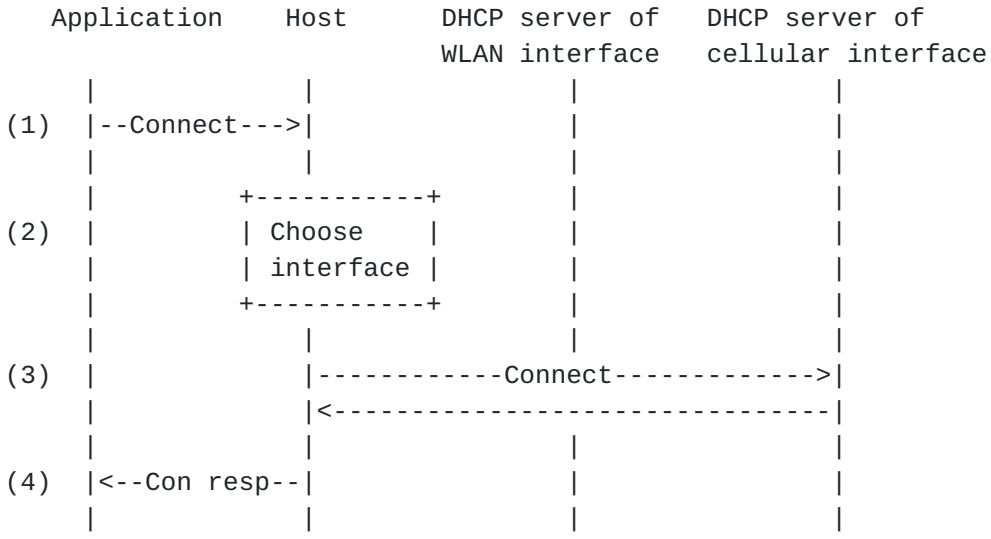
To avoid problems described in chapter 3, in addition to logic for conducting successful DNS query, the host's source IP address selection algorithms must be able to choose the IP address of the right network interface when application is providing only a destination IP address to connect to.

The source address selection algorithm SHOULD do either or both of the following procedures:

A) The algorithm to make reverse DNS lookup for the destination IP address on host's own DNS cache, which should contain corresponding record if the IP address was earlier resolved from a FQDN. From this record FQDN matching the IP address is learned, and based on that FQDN network interface with corresponding DNS suffix can be chosen.

B) The algorithm to consult host's address selection policy table, which may have been dynamically received as described in [MATS2008] and [FUJI2008].

This is illustrated in example message flow 3 below.



Message flow 3: Choosing interface for outgoing connection

Flow explanations:

(1) An application initiates new connection to an IP address, e.g. 192.0.2.1

(2) The host either:

a. Consults host's internal DNS cache with reverse DNS lookup query and learns that FQDN "private.operator.com" is matching IP 192.0.2.1 and therefore cellular network interface with matching DNS suffix "operator.com" shall be selected

b. Consults dynamically received address selection policy table and learns that for destination IP 192.0.2.1 cellular interface should be used

(3)and (4) Connection is established over selected network interface

5. Network operator considerations

An operator of a network can continue to use DHCP DNS search list options as before, but the operator should take into account that multi-homed hosts may use the DNS suffix information also for interface selection purposes.

An operator wishing to assist hosts in network interface selection should configure DHCP servers with proper DNS suffix information, which hosts then can use as hints for improved operation. Furthermore, the operator should configure DHCP servers with IP address selection policies ([MATS2008], [FUJI2008]) that are corresponding to the configured DNS suffix information.

6. Further considerations

Overloading of existing DNS search list options is not without problems, though: hosts would obviously use the DNS suffixes learned from search lists also for name resolution purposes. This may not be a problem in deployment cases where DNS search list options already contain few DNS suffixes like "intranet.corporation.com", but can become a problem in other deployment scenarios.

An obvious alternative would be to define new DHCP options for distributing DNS suffix information designed only for network interface selection purposes.

7. Security Considerations

An attacker may try to lure traffic from multi-homed host to his network by advertising DNS suffixes attacker wishes to intercept or deny service. The host's security should not be based on correct functionality of source/destination address selection, but risks of this attack can be mitigated by properly prioritizing network

interfaces with conflicting DNS suffix advertisements. The prioritization can be based on trust level of a network interface over which DNS suffix was learned from:

- o VPN interfaces being most trustworthy
- o Managed networks being on the middle
- o Unmanaged networks having lowest priority

Now, for example, if all of the three abovementioned networks would indicate access for "corporation.com", the host would choose to use the VPN for connections destined to "corporation.com" domain.

8. IANA Considerations

No considerations identified at this point. TBD: if new DHCP options are defined instead, situation changes.

9. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3397] Aboba, B., Cheshire, S., "Dynamic Host Configuration Protocol (DHCP) Domain Search Option", RFC 3397, November 2002

[RFC3646] Ed., Droms, R., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003

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

[MATS2008] Matsumoto, A., Fujisaki, T., Hiromi, R., Kanayama, K., "Solution approaches for address-selection problems", June 2008, draft-ietf-6man-addr-select-sol-01.txt

[FUJI2008] Fujisaki, T., Niinobe, S., Hiromi, R., Kanayama, K., " Distributing Address Selection Policy using DHCPv6", June 2008, draft-fujisaki-dhc-addr-select-opt-06.txt

10.2. Informative References

[RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003

Author's Address

Teemu Savolainen
Nokia
Hermiankatu 12 D
FI-33720 TAMPERE
FINLAND

Email: teemu.savolainen@nokia.com

Full Copyright Statement

Intellectual Property Statement