Wireless Profiled DNS

Approved Version 1.0 – 06 Jun 2006

Open Mobile Alliance

OMA-WAP-DNS-V1_0-20060606-A

Continues the Technical Activities
Originated in the WAP Forum

Contents

Figures

1. Scope

The Wireless Application Protocol (WAP) is a result of work defining an industry wide specification for developing applications that operate over wireless communications networks.. The wireless market is growing very quickly, reaching new customers and providing new services. To enable operators and manufacturers to meet the challenges in advanced services, differentiation, and fast/flexible service creation, WAP provides a set of open, extensible protocols and content formats as a basis for interoperable implementations. In one instance of a WAP architecture, a WAP Proxy Gateway may be deployed which performs DNS (Domain Name Server) lookup on behalf of the terminal. . However, network service providers may choose not to install WAP Proxy Gateways, or allow usage patterns that circumvent the WAP Proxy Gateway. Without the availability of a WAP Proxy Gateway, the WAP terminal is required to perform DNS lookup. The specific reasons for including and profiling a WAP terminal DNS client are:

- To support IP address resolution within the direct access scenario depicted in the WAP Architecture specification [WAPARCH].
- To minimise the use of radio resources by controlling the behaviour of the DNS client.
- To specify an interoperable lightweight DNS client with minimal footprint, memory and processor requirements.

The scope of this document covers the functionality of the DNS client on the terminal, while remaining compliant with the IETF specifications listed in section **Error! Reference source not found.**. This document will not specify the behaviour of the DNS server, therefore Wireless Profiled DNS clients will be capable of performing DNS lookups with pre-existing DNS servers (i.e we impose no requirements on the server). This specification will also conform to IPv4 and IPv6 addressing schemes.

2. References

2.1 Normative References

[CREQ] "Specification of WAP Conformance Requirements". WAP Forum™. WAP-221-CREQ-20010425-a. URL:http//www.wapforum.org/

[RFC1034] "Domain Names – Concepts and Facilities", P. Mockapetris. November 1987 URL:http://www.ietf.org/rfc/rfc1034.txt

[RFC1035] "Domain Names – Implementation and Specification". P. Mockapetris. November 1987. URL:http://www.ietf.org/rfc/rfc1035.txt

[RFC1886] "DNS Extensions to Support IP version 6". S. Thomson, C. Huitema. December 1995. URL:http://www.ietf.org/rfc/rfc1886.txt

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels". S. Bradner. March 1997. URL:http://www.ietf.org/rfc/rfc2119.txt

[RFC2308] "Negative Caching of DNS Queries (DNS NCACHE)" M. Andrews. March 1998. URL:http://www.ietf.org/rfc/rfc2308.txt

2.2 Informative References

[PROVBOOT] "Provisioning Bootstrap". WAP Forum™. WAP-184-ProvBoot-20010314-a. URL:http//www.wapforum.org/

[PROVCONT] "Provisioning Content Type Specification". WAP Forum™. WAP-183-ProvCont-20010724-a. URL:http//www.wapforum.org/

[PROVSC] "Smart Card Provisioning Specification". WAP Forum™. WAP-186-ProvSC-20010710-a. URL:http//www.wapforum.org/

[PROVUAB] "Provisioning User Agent Behaviour", WAP Forum™. WAP-185-ProvUAB-20010314-a. URL:http://www.wapforum.org/

[RFC1123] "Requirements for Internet Hosts – Application and Support". R. Braden. October 1989. URL:http://www.ietf.org/rfc/rfc1123.txt

[RFC1332] "The PPP Internet Protocol Control Protocol (IPCP)". G. McGregor. May 1992. URL:http://www.ietf.org/rfc/rfc1332.txt

[RFC2132] "DHCP Options and BOOTP Vendor Extensions". S. Alexander, R. Droms. March 1997. URL:http://www.ietf.org/rfc/rfc2132.txt

[RFC2181] "Clarifications to the DNS Specification". R. Elz, R. Bush. July 1997. URL:http://www.ietf.org/rfc/rfc2181.txt

[RFC2535] "Domain Name System Security Extensions". D. Eastlake. March 1999. URL:http://www.ietf.org/rfc/rfc2535.txt

[RFC2845] "Secret Key Transaction Authentication for DNS (TSIG)". P. Vixie, O. Gudmundsson, D. Eastlake, B. Wellington. May 2000. URL:http://www.ietf.org/rfc/rfc2845.txt

[RFC3007] "Secure Domain Name System (DNS) Dynamic Update". B. Wellington. November 2000.

[WAPARCH] "WAP Architecture". WAP Forum™. WAP-210-WAPArch-20010712-a. URL:http//www.wapforum.org/

[W-HTTP] "Wireless Profiled HTTP". WAP Forum™. WAP-229-HTTP-20010329-a URL:http//www.wapforum.org/

[W-TCP] "Wireless Profiled TCP". WAP Forum™. WAP-225-TCP-20010331-a URL:http//www.wapforum.org/

3. Terminology and Conventions

3.1 Conventions

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].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

This is an informative document, which is not intended to provide testable requirements to implementations.

3.2 Definitions

KEY	DNSSec extension resource Record for distributing public keys of DNS network entities
Lightweight DNS	An IETF compliant interpretation of DNS that minimises the use of radio and terminal resources
Provisioned DNS Server	A DNS server that is provisioned as a point of contact for the DNS client
SIG	A DNSSec signature record

3.3 Abbreviations

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSSec	DNS Security
FTP	File Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
PPP	Point-to-Point Protocol
RFC	Request for Comments
RR	Resource Record
SIM	Subscriber Identity Module
SSH	Secure Shell
TCP	Transmission Control Protocol
TSIG	Transaction Signature
TTL	Time-to-Live
UDP	User Datagram Protocol
WAP	Wireless Application Protocol
W-DNS	Wireless Profiled DNS
WIM	WAP Identity Module
W-HTTP	Wireless Hypertext Transfer Protocol [W-HTTP]
W-TCP	Wireless Profiled TCP [W-TCP]

4. Introduction

Network service providers may choose not to install WAP Proxy Gateways, or allow usage patterns that circumvent the WAP Proxy Gateway. Without the availability of a WAP Proxy Gateway, the WAP terminal is required to perform DNS lookup.

As stated in the scope, this document seeks to support IP address resolution within the direct access scenario, as specified in the WAP Architecture specification [WAPARCH]. Architecturally this specification profiles the terminal and does not profile how the DNS server interacts with the DNS client, therefore Wireless Profiled DNS (W-DNS) clients will be capable of performing DNS lookups with existing DNS servers.

By controlling the behaviour of the DNS client on the terminal, the use of radio resources can be minimised. Effectively, the DNS client will prompt the type of response from the DNS service that is appropriate to the wireless network.

A lightweight DNS client will be recommended wherever possible - minimising footprint, memory and processor requirements. This specification will be particularly relevant to terminal software developers and network providers.

5. Architectural Context

This section is informative.

5.1 Generic Functional Architecture

W-DNS enables the appropriate request/response behaviour when resolving domain names to IP addresses in the direct access architecture as given in Figure 11 of [WAPARCH]. A contactable DNS Server, the Provisioned DNS Server in Figure 1, may be found inside the local network or outside the local network and elsewhere on the Internet. DNS provisioning methodologies are not illustrated in Figure 1.

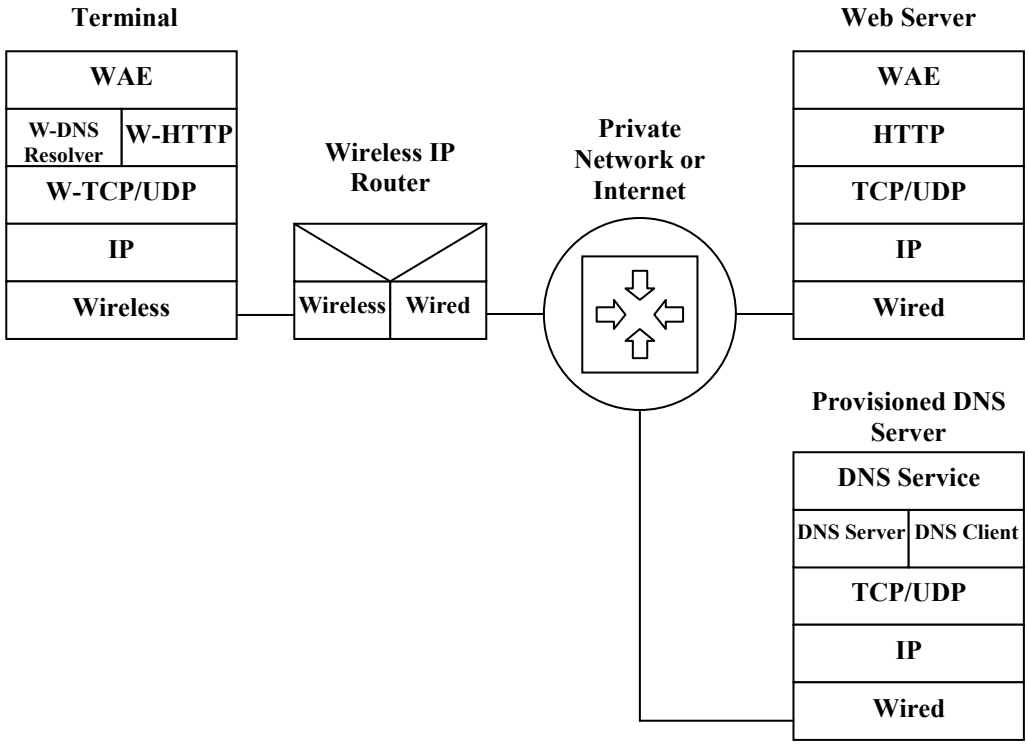

Figure 1 Direct Access DNS Architecture

Although this architecture is proxyless, the server-side implementation has the option to incorporate gateway functionality, such as access control and load management into their network. This additional functionality is not illustrated in Figure 1 in order to illustrate the generic use case.

6. Provisioning the DNS Service

This section is informative.

When the W-DNS capable terminal is required to contact the DNS service, it is the responsibility of provisioning mechanisms to provide the terminal with the necessary IP address(es) of the first point(s) of contact for the DNS client. This form of provisioning may be achieved by implementing any of the following provisioning mechanisms listed below:

- WIM/Active SIM/User-Defined Settings [PROVUAB][PROVSC]
- WAP Client Provisioning [PROVBOOT][PROVCONT][PROVUAB][PROVSC]
- PPP/IPCP or DHCP (bearer dependent and provisioned by the server-side implementation) [RFC1332][RFC2132]

The settings for these provisioning mechanisms may be stored on the SIM or device. It is the role of the user agent to prioritise these provisioning mechanisms [PROVUAB].

7. IETF Protocol Compliance

This section is normative.

7.1 All W-DNS Resolvers

W-DNS resolvers MUST comply with the IETF documents listed in this section in order to interoperate with conventional and generic DNS Servers. In addition, the W-DNS resolvers MUST comply with the profile specification in section 8 to produce a lightweight protocol (i.e. a Wireless Profiled DNS).

- [RFC1034] (Domain Names – Concepts and Facilities)

  This RFC describes domain style names that must be supported.

- [RFC1035] (Domain Names – Implementation and Specification)

  This RFC describes the details of the domain system and protocols relevant to terminal implementations.

- [RFC2308] (Negative Caching of DNS Queries)

  This RFC describes how to cache and handle negative responses from DNS.

A W-DNS Resolver MUST only be installed on a terminal that supports IPv4 network layers or IPv6 network layers or both.

7.2 IPv6 W-DNS Resolvers

W-DNS Resolvers installed on terminals with IPv6 support MUST also comply with the following IETF document:

- [RFC1886] (DNS Extensions to Support IPv6)

8. DNS Profile

This section is normative.

8.1 The Terminal Based Resolver

[RFC1035] allows stub resolvers and full resolvers to be implemented optionally. The W-DNS client MUST implement at least a stub resolver in order to minimise the size of implementation and facilitate the delegation of the querying process to a Provisioned DNS server. A W-DNS client MAY support a full service resolver, for instance if the implementation wishes to maintain zone data.

8.2 Allowed Querying Modes

The use of recursive querying mode enables minimal interaction between the resolver and DNS directory service, using less radio resources than iterative mode querying. A W-DNS client MUST initially use recursive querying mode and MAY use iterative querying mode (if available to the W-DNS client) if recursive querying fails.

> Informational Note: This specification strongly recommends that server-side implementations must provision recursive capable DNS servers to a W-DNS client, when offering direct access.
>
> If the server side implementations neither support nor enable recursive querying mode, then the recursive query will fail.
>
> In order to avoid this failure, a full resolver may be implemented on the client when offering direct access, since a stub resolver only supports recursive querying mode.

8.3 Multicast and Broadcast Querying

Multicast or broadcast queries may lead to multiple separate responses that consume radio resources. Therefore W-DNS client implementations at the terminal MUST NOT send multicast or broadcast queries.

8.4 Caching Behaviour

Frequent querying for the IP address of the same domain wastes radio resources. W-DNS capable terminals MUST be able to cache DNS responses and perform normal caching operations. Longer duration TTL values may be considered by server-side implementations when sending RRs (Resource Records) of frequently used wireless services (e.g. portals, messaging services and search facilities).

For conformance purposes, the cache MUST be capable of storing a minimum of one entry. However, this specification recommends the implementation to enable the caching of multiple entries - where performance optimisation and size of storage allocation determine the allowed volume of stored entries. The W-DNS client in the terminal MUST NOT modify TTL values for caching entries. It is likely that TTL values have been optimised by the server-side implementation, therefore client-side adjustments to TTL values can result in more frequent connections to invalid IP addresses and an overall inefficient use of radio resources.

9. Implementation Notes

This section is informative

The intention of this section is to inform network providers about implementation optimisations that they may wish to consider. These implementation optimisations are recommendations and not requirements for WAP compliance.

9.1 Host Requirements

W-DNS will not specify host requirements or the behaviour of the DNS server. However W-DNS recommends the use of [RFC1123] while considering a network implementation. [RFC2181] is also recommended for informational purposes.

This specification also recommends that server-side implementations must ensure their Provisioned DNS servers are capable of handling recursive querying in order to support W-DNS terminals. Recursive querying minimises the use of radio resources, enhancing throughput. It is strongly recommended that server-side implementations install DNS servers capable of recursive querying, as iterative querying is not mandated on W-DNS capable terminals.

9.2 Limiting Access in Closed Service Domains

Some server-side deployments may wish to implement closed service domains that only allow subscribers to access affiliated services (e.g. within a single private network or over a virtual private network). Users on other networks may also be disallowed access to these affiliated services.

It is recommended that server-side deployments wishing to implement a closed service domain should disconnect their Provisioned DNS server network from the global DNS server network. This isolation of the Provisioned DNS server network will also disallow users on other networks from resolving the domain name of restricted services.

Other security mechanisms (e.g. deploying firewalls policy enforcement) must also be considered.

9.3 Optimising TTL Attributes

Stored on the DNS database are time-to-live (TTL) attributes associated with each DNS entry and sent in RR responses to the DNS client. Server-side implementations that own Provisioned DNS servers have the opportunity to automatically calculate and optimise the TTL attributes in order to minimise radio utilisation.

9.4 Security Considerations

In the typical WAP environment, there is rarely a need to protect large, “Internet scale” DNS data transfers. However, there is always a need to protect local (i.e. within a zone) DNS transfers, as well as ensure that zone data is changed only by authorised agents. Similarly, the network administrator may want to restrict DNS server transactions to authorised clients only. To address those needs, DNSSec [RFC2535] contains mechanisms that provide data origin authentication, transaction and request authentication and key distribution. New resource records contain public keys, certificates and digital signatures. Additional mechanisms include meta-records that augment query-response security.

This extra security does have drawbacks. Authenticated data usually “expires” after some time and the parties (clients and servers) exchanging this information must maintain their security relationship. TSIG [RFC2845] avoids the performance impact of public key cryptography by using “shared secrects”, but secure distribution of the shared secret is still an issue.

Local (i.e. within zone) data transfers between servers should be protected using any of the DNSSec mechanisms. Updates to zone data should be authenticated and authorised using the Secure Dynamic Update [RFC3007] mechanism, although non-DNSSec mechanisms, such as secure FTP/SSH transfers, may be adequate for small-scale zones.

In order to evaluate the servers’ response, resolvers may request that servers respond to queries with the desired set, SIG, and possibly KEY and SIG(KEY)s. However, when provisioned to do so, resolvers should issue lightweight queries to a “preferred” server using SIG(0) or TSIG. Such provisioning would require the list of preferred servers and the shared secret

to be used with TSIG. Otherwise DNSSec should not be used in the WAP environment until lower overhead DNSSec mechanisms are available.

Appendix A. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [CREQ]. This specification has NO server-side requirements.

A.1 Client Features

A.1.1 DNS Profile Features

Item	Function	Reference	Status	Requirement
DNS-DPF-C-001	Support for [RFC1034] (Domain Names – Concepts and Facilities)	7.1	M	
DNS-DPF-C-002	Support for [RFC1035] (Domain Names – Implementation and Specification)	7.1	M	
DNS-DPF-C-003	Installed on an IPv4 or IPv6 capable terminals	7.1	M	*DNS-DPF-C-004 or DNS-DPF-C-005*
DNS-DPF-C-004	Installed on an IPv4 capable terminal	7.1	O	
DNS-DPF-C-005	Installed on an IPv6 capable terminal	7.1	O	*DNS-DPF-C-006*
DNS-DPF-C-006	Support for [RFC1886] (DNS Extensions to Support IPv6)	7.2	O	
DNS-DPF-C-007	Support for [RFC2308] (Negative Caching of DNS Queries)	7.1	M	
DNS-DPF-C-008	Stub Resolver	8.1	M	
DNS-DPF-C-009	Full Resolver	8.1	O	
DNS-DPF-C-010	Recursive Querying	8.2	M	
DNS-DPF-C-011	Iterative Querying	8.2	O	*DNS-DPF-C-009*
DNS-DPF-C-012	Prohibit multicast or broadcast queries	8.3	M	
DNS-DPF-C-012	Caching Behaviour	8.4	M	

Appendix B. Change History (Informative)

B.1 Approved Version History

Reference	Date	Description
OMA-WAP-DNS-V1_0	06 Jun 2006	Approved by TP OMA-TP-2006-0200-DNS-V1_0-for-Approval.