Internet Engineering Task Force	T. Creighton	
Internet-Draft	C. Griffiths	
Intended status: Informational	J. Livingood	
Expires: April 25, 2011	Comcast	
	R. Weber	
	Unaffiliated	
	October 22, 2010	

TOC

DNS Redirect Use by Service Providers
draft-livingood-dns-redirect-03

Abstract

The objective of this document is to describe the design of so-called DNS Redirect services deployed today by Internet Service Providers (ISPs), DNS Application Service Providers (ASPs), and other organizations providing so-called DNS Redirect services via their recursive DNS servers, as well as to describe the recommended practices regarding relating to DNS redirect. This document specifically and narrowly addresses those cases where DNS Redirect is being utilized to provide a web error redirect service to end users, and describes the critical implications for DNS Redirect when DNSSEC is deployed.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
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.”
This Internet-Draft will expire on April 25, 2011.

Copyright Notice

Table of Contents

1. Requirements Language
2. Introduction
3. Document Scope
4. DNSSEC Considerations and Implications
5. Terminology
6. Web Error Redirect
7. Opt-In or Opt-Out Mechanisms
    7.1. Opt-Out
    7.2. Opt-In
    7.3. Automated Mechanisms and Reasonable Processing Times
    7.4. Type of Opt-Out Method
8. Practices to Avoid
    8.1. Use of DNS Redirect with DNSSEC
    8.2. Improper Redirect of Valid Responses
    8.3. Redirect of SERVFAIL Responses
    8.4. Routinely Broken, Purposefully Broken, and Otherwise Unreliable Opt-Out Mechanisms
    8.5. Markedly Slower DNS Query Performance
    8.6. Override of a User's DNS Selection
9. Functional Design
10. Example DNS and HTTP Flows
11. Security Considerations
12. Controvery Surrounding DNS Redirect
13. Future Prospects for DNS Redirect
14. Why This Document Merits Publishing
15. IANA Considerations
16. Contributors
17. Acknowledgements

18. References
18.1. Normative References
18.2. Informative References
Appendix A. Document Change Log
Appendix B. Open Issues
§ Authors' Addresses

---

1. Requirements Language

TOC

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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

---

2. Introduction

TOC

Internet users typically are provided with several IP addresses for recursive DNS servers, as described in Section 2.3 of [RFC1591] (Postel, J., “Domain Name System Structure and Delegation,” March 1994.), by their respective ISPs, typically in an automated fashion via DHCP [RFC2131] (Droms, R., “Dynamic Host Configuration Protocol,” March 1997.). Some other users and organizations choose to use a different set of IP address for their DNS servers, which are hosted and managed by another organization, such as a DNS ASP. It is also the case that a number of users and organizations choose to operate their own DNS servers, though those use cases are outside of the scope of this document.

ISPs and DNS ASPs have over time created &quot enhanced &quot DNS services for their users, which often rely upon DNS Redirect functionality. These enhanced services, which are offered on an opt-in or opt-out basis, can perform a number of enhanced services for users, such as attempting to interpret web address errors when an invalid fully qualified domain name (FQDN, Section 5.1 of [RFC1035] (Mockapetris, P., “Domain names - implementation and specification,” November 1987.)) has been typed by a user.

This document describes the design and function of a DNS Redirect service, as well as recommended practices and practices to avoid. It also describes the critical implications for DNS Redirect when DNSSEC is adopted, in Section 4 (DNSSEC Considerations and Implications).

---

3. Document Scope

TOC

This document focuses on the systems and practices of ISPs and DNS ASPs. All other use cases, such as when an Internet user or organization chooses to operate their own DNS servers is outside of the scope of this document.

There are several ways that such entities can provide users with these enhanced DNS services. In addition to methods which rely primarily upon a recursive DNS server, alternate methods include (a) interception and replacement of the error by a web browser client software, (b) interception and replacement of the error by a tool bar, plug-in, personal firewall security software or other web browser client add-on. These alternate methods, which rely upon various types of client software, are also outside of the scope of this document.

It is important to note that while these alternate methods are considered out of scope for this document, this should not be interpreted as a negative judgment of their suitability or applicability to the relevant problem space. Instead, these should simply be considered as alternate methods since, as with most any technical problem, there are a variety of valid methods for solving a problem.

Lastly, while Section 7 (Opt-In or Opt-Out Mechanisms) indicates that users must be able to opt into or out of DNS Redirect services, the reasons for why an ISP or DNS ASP may choose one or the other as the default are out of scope.

---

4. DNSSEC Considerations and Implications

TOC

DNS security extensions defined in [RFC4033] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements,” March 2005.), [RFC4034] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Resource Records for the DNS Security Extensions,” March 2005.), and [RFC4035] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Protocol Modifications for the DNS Security Extensions,” March 2005.) use cryptographic digital signatures to provide origin authentication and integrity assurance for DNS data. This is done by creating signatures for DNS data on a DNS Security-Aware Authoritative Name Server that can be used by DNS Security-Aware Resolvers to verify the answers.

DNSSEC is now in the process of being deployed on authoritative servers, now that the DNS root has been signed and several key Top Level Domains (TLDs) have been signed. DNSSEC is also starting to be adopted by service providers, which are now in the process of adding DNSSEC validation in DNS recursive resolvers.

It is critically important that service providers understand that adoption of DNSSEC is technically incompatible with DNS redirect. As such, in order to properly implement DNSSEC and maintain a valid chain of trust, DNS redirect MUST NOT be used any longer. Thus, once DNSSEC is in widespread use, this document should be considered historical. That being said, sections of this document concerning opt-in and opt-out practices may be useful for future reference in other, unrelated documents.

---

5. Terminology

TOC

While these terms are generally well known, it is important to define them in the context of this document.

5.1. Internet Service Provider (ISP)

TOC

An Internet Service Provider, which provides Internet services, including basic network connectivity. It is not germane to this document what the method of connection is, such as wired or wireless, what the speed of such a connection is, or what other services are included or available to users. It is, however, assumed that the ISP is providing recursive DNS services to their users and is in some manner providing users with the IP addresses of these DNS servers, whether via DHCP, static assignment by users, or some other method.

5.2. DNS Application Service Provider (ASP)

TOC

A DNS Application Service Provider, which provides managed and/or hosted recursive DNS services (and possibly other DNS services) to their users. In the case of managed services, the DNS ASP may remotely manage the recursive DNS servers in a user's network. For a hosted recursive DNS service, these servers are typically located outside of the user's network and these hosted resources are shared across multiple users. In most instances, these are hosted services and users are manually configuring either their DHCP server or their individual computing devices with the IP addresses of the recursive DNS servers operated by their ASP.

TOC

5.3. Internet User

An Internet user, which is generally a person using a computing device to connect to and make use of the Internet. Such users are typically connected at the edge of the network, though the method by which they connect to the Internet is not particularly relevant to this document.

5.4. DNS Recursive Resolver

TOC

A DNS recursive resolver processes fully qualified domain name queries (FQDN, Section 5.1 of [RFC1035] (Mockapetris, P., “Domain names - implementation and specification,” November 1987.)) into IP addresses by finding the resource records in the authoritative DNS servers for the domain associated with the FQDN. The resource records are then cached on the recursive server for future requests until an expiration timer expires called time to live (TTL), as described in Section 5.2 of [RFC2181] (Elz, R. and R. Bush, “Clarifications to the DNS Specification,” July 1997.). These servers are in most cases provided by ISPs for name resolution.

5.5. Web Browser

TOC

Client software operated by the user locally on their computing device, such as Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, Google Chrome, etc.

5.6. Web Error Landing Server

TOC

The host that a user is directed to when the DNS Recursive Server receives a NXDOMAIN response. The contents of the web page that the web server sends the user varies widely across different ISPs and DNS ASPs. In some cases it is simply a more descriptive error that the user would otherwise receive, while in other cases it may include links to sites similar to the URL attempted and/or a search page, among many other possibilities.

TOC

5.7. User Options Web Server

The web server that a user is directed to via a link on a page served by the Web Error Landing Server, the Malicious Domain Web Error Landing Server, from another system such as an account management system, or via direct access, which enables a user to control whether or not they are opted into or opted out of DNS Redirect services. This is described in additional detail in the Section 7 (Opt-In or Opt-Out Mechanisms) section.

5.8. NXDOMAIN Response

TOC

In this document, an NXDOMAIN (nonexistent domain) response can be used interchangeably with an RCODE 3 response. The RCODE 3 response was first documented in see Section 4.1.1 of [RFC1035] (Mockapetris, P., "Domain names - implementation and specification," November 1987.). Subsequent RFCs introduced the term NXDOMAIN response, which is synonymous with RCODE 3 and tends to be used more frequently, as noted in Section 2.2 of [RFC2136] (Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)," April 1997.), and Section 1 of [RFC2308] (Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)," March 1998.).

---

6. Web Error Redirect

TOC

A web error redirect service enables an ISP or ASP to provide a user, who is generally utilizing a web browser, with an improved user experience when an attempt to reach a nonexistent domain is made.

6.1. Web Error Redirect Problem Statement

TOC

A user enters an incorrect URL into their web browser, such as http://www.example.invalid, where .invalid is a nonexistent Top Level Domain (TLD, see Section 2 of [RFC1591] (Postel, J., "Domain Name System Structure and Delegation," March 1994.)). In such a case, a user would typically receive an error.

TOC

6.2. Web Error Redirect Solution Description

When a recursive DNS server detects such a nonexistent domain error (NXDOMAIN, see Section 4.1.1 of [RFC1035] (Mockapetris, P., "Domain names - implementation and specification," November 1987.)), the ISP or ASP can instead provide a IP address for a Web Error Landing Server that can present the user with a list of suggested destinations rather than simply an error page. This page must also provide the user with a link to a method of opting out in the future. See Figure 1 (DNS Redirect Response), Figure 2 (Web Error Landing Server), and Figure 5 (DNS Redirect and HTTP Flow) for examples below.

6.3. Web Error Redirect Solution Considerations

TOC

It is important to note that this technology can directly impact non-web clients such as instant messaging, VPNs, FTP, email filters-related DNS queries. Thus, special exclusions may need to be made in order to prevent unintentional side effects. Design considerations for the Web Error Search and Malicious Site Protection services should include properly and promptly terminating non-HTTP connection requests. Only A and AAAA resource records should be redirected, all other resource record types must be answered as if there was no redirection.

---

7. Opt-In or Opt-Out Mechanisms

TOC

ISPs and DNS ASPs MUST provide their users with a method to opt into (opt-in) or out (opt-out) of some or all DNS Redirect services. Opt-out and opt-in methods should be reliable and should take into consideration the Section 8 (Practices to Avoid) section below. Whether such services are offered on an opt-in or opt-out basis depends on a range of factors which are outside of the scope of this document. The two different methods, opt-out and opt-in, are described below.

7.1. Opt-Out

TOC

Opt-Out is used when the users are by default offered all or some DNS Redirect services. As a result, the user must take an action to disable some or all such services. This is typically performed via a User Options Web Server. Users that have chosen to opt-out should receive DNS responses which are indistinguishable from those responses provided by a DNS server with no DNS Redirect functionality. In addition, opt-

out should be persistent in nature, which means that opt-out should be tied to a fixed credential or attribute of some type, such as an account identifier, billing identifier, or equipment identifier, which is not typically subject to change on a regular basis.

7.2. Opt-In

TOC

Opt-In is used when the users are by default not offered any DNS Redirect services. As a result, the user must take an action to enable some or all such services. This is typically performed via a User Options Web Server.

7.3. Automated Mechanisms and Reasonable Processing Times

TOC

Once a user has selected to opt-in or opt-out of DNS Redirect services, such changes should occur automatically, when this is technically possible, without requiring the user to manually change any settings on their computing device. Such changes should also occur within a reasonable period of time. In some cases, however, a user may be offered the ability to speed the period of time for these changes to take effect, such as by restarting the computing device or a piece of network equipment which connects them to their ISP's network, for example.

While an automated mechanism may be the easiest for users, since it requires no manual reconfiguration of their network settings, the authors also recognize that there may be extenuating circumstances where this is not achievable. In such cases, which may for example be due to the particular attributes of one or another ISP's network design, a fully automated mechanism may not be possible. Another example is where a user is switching from their ISP's DNS server IP addresses to those of a DNS ASP. As a result, a user in all of these cases, as well as other possible cases, must manually reconfigure their network with different DNS IP addresses.

7.4. Type of Opt-Out Method

TOC

There are several workable methods that can be employed to effect the actual opt-out for a given user. These include setting a local user application attribute, such as via a cookie in a web browser, as well as setting a network attribute, via a DHCP change or manually configuring the DNS IP addresses (in the operating system, modem, home

gateway device, or router) in order to change the DNS IP addresses for a particular user.
While all of these methods are workable and can be made reliable, the best current method is via a network-based change of some sort. In this way, all Internet-connected computing devices within a given household are included in the opt-out (these devices are generally connected in some manner to the LAN side of some type of customer premise device, such as a cable modem or DSL modem). This is in contrast to a method which uses a local user application attribute, such as a cookie in a web browser, where deletion of cookies, upgrade to a new operating system, upgrade to a new web browser, use of a different web browser, or countless other factors on that device could cause the user to be opted back into a DNS Redirect service. Thus, a network-based approach which sets opt-out-related attributes at the device, or household level, is the most inclusive and persistent method for providing a reliable opt-out method, and is the recommended practice.

---

8. Practices to Avoid

TOC

This document primarily focuses on the recommended practices for an ISP or ASP to provide users with DNS Redirect services. However, it is important to note that some entities may not operate in accordance with such practices. As such, some of these are catalogued below in order to contrast them with recommended practices and provide information which may be of interest and use to the community.

8.1. Use of DNS Redirect with DNSSEC

TOC

When DNSSEC has been implemented in a service provider's resolvers, DNS redirect MUST NOT be used, as it is technically incompatible with DNSSEC and breaks the chain of trust critical to proper DNSSEC validation functionality.

8.2. Improper Redirect of Valid Responses

TOC

It has been observed that some service providers improperly utilize DNS Redirect services when there is a valid DNS resource record returned in response to a DNS recursive query. The effect is to redirect users to a server not maintained by the intended destination, such as a web site that looks like the intended web site but is not actually the intended site and is instead controlled by the service provider. For example a

DNS query for www.example.com results in a valid A record response, but this valid response is instead replaced with an A record controlled by the service provider. In this case the intended server identified with the valid A record contained valid, lawful, non-malicious content, and there would otherwise appear to be no valid justification for a redirect to occur. See Figure 6 (Improper Redirect of Valid Response Redirect and HTTP Flow) for an example below.

If there is a valid and reasonable justification for such a redirect to occur, examples of which are not currently known by the authors of this document, then the resulting connection to the server that the user has been redirected to should clearly and prominently disclose that this is not the intended site. For example, in the case of an attempt by a user to connect to a web site, the site may contain a banner or frame which indicates that this is not the intended site or that the site is in some manner controlled by the service provider. In addition, such a notice should also offer a clear method to opt-out of this redirect function.

Thus, to summarize, redirection of valid responses SHOULD NOT be performed.

8.3. Redirect of SERVFAIL Responses

TOC

Redirection of SERVFAIL responses SHOULD NOT occur. SERVFAIL responses may occur intermittently in an operational network for a variety of highly transient reasons. As a result, a DNS Redirect should not be performed when a SERVFAIL response is received, as normal retry a short time later is likely to result in a valid response.

8.4. Routinely Broken, Purposefully Broken, and Otherwise Unreliable Opt-Out Mechanisms

TOC

There are several well known and dependable methods of opt-out mechanisms that ISPs and DNS ASPs can deploy for users to opt-out of their DNS Redirect services. These methods can rather easily be employed and are highly recommended, as noted in Section 7 (Opt-In or Opt-Out Mechanisms). However, some ISPs and DNS ASPs may instead choose to employ a less dependable mechanism, which routinely fails to work as expected by users or is known not to function properly.

For example, one routinely unreliable method for opt-out is the cookie-based method. When a user opts out of a DNS Redirect service, a cookie is installed in their web browser. The problem with this method occurs when a user clears their cookies or the cookies are deleted for some reason. In some cases, users may configure their web browsers to clear all cookies every time the close their web browser. Thus, one possible

effect upon the user in this case is that they are once again opted into the redirect service. Furthermore, a cookie-based method has the effect of only opting out browser-based protocols (generally HTTP and HTTPS), which means that the user may have non-web applications affected by DNS Redirect, even though they believe they have opted-out. As a result, there is no assured permanency with this opt-out method, nor does it work consistently across all applications and protocols, which can be aggravating to users who do not wish to utilize DNS Redirect services.

Another example of an unreliable method for opt-out is one where opt-out is tied to the IP address of the user, where that address may be subject to change on a regular basis, such as via an ISP-based DHCP lease. In such a case, if opt-out was tied to what can be considered a largely dynamic IP address, then the user would be opted-in every time they received a new IP address, forcing them to repeatedly opt-out.

Thus, to summarize, the opt-out mechanism provided to users SHOULD be reliable and SHOULD NOT be routinely broken, purposefully broken, or otherwise unreliable.

8.5. Markedly Slower DNS Query Performance

TOC

An ISP or DNS ASP should also understand that DNS query latency, the time between when a user's stub resolver issues a DNS query and receives a DNS response, should be kept as low as is reasonably possible. High DNS query latency is often perceived by users, and can have an adverse effect on a variety of applications where low DNS query latency may be especially important. Any additional processing which must be performed in order to provide DNS Redirect services should be monitored closely, in order that DNS Redirect functionality does not markedly slow DNS query performance.

Thus, to summarize, when DNS redirect is performed, DNS query performance SHOULD NOT suffer as a result, since this could provide an incrementally inferior user experience as compared to when DNS redirect is not performed.

8.6. Override of a User's DNS Selection

TOC

Some users may decide to use the DNS server IP addresses of a DNS ASP or other non-ISP-provided DNS servers. Such selections should be preserved as the free choice of a user, particularly when DNS Redirect services are offered. Thus, an ISP SHOULD NOT redirect port 53 DNS traffic from servers intended by the user via their selection of non-ISP DNS servers to the DNS servers of the ISP, except in reasonable and justifiable cases where a user has been placed into a so-called "walled

garden" for reasons of abuse, security compromise, account non-payment, new service activation, etc.
An exception to this is when, unbeknownst to the user, malicious software (malware) has changed the IP address of their DNS server to a known malicious DNS server. In such cases, it may be in the best interests of the user to take steps to ensure they do not use such a malicious DNS server, particularly since they did not intend to do so and may be infected with malware. While this is unrelated to DNS Redirect per se, it merits mentioning based on feedback received from the security community.

---

9. Functional Design

TOC

The functional design described in this section is intended to be generally representative of the many different ways that DNS Redirect services are deployed today. As such, they are necessarily high level and different implementations may vary somewhat, due to any number of factors.

9.1. DNS Recursive Resolver

TOC

The DNS Recursive Resolver is used by the host computer to translate fully qualified domain names into IP addresses, according to Section 3.6.1 of [RFC1034] (Mockapetris, P., “Domain names - concepts and facilities,” November 1987.). When a FQDN does not exist in authoritative DNS a NXDOMAIN response, as described in Section 4.1.1 of [RFC1035] (Mockapetris, P., “Domain names - implementation and specification,” November 1987.) is normally returned (see Figure 1 (DNS Redirect Response)). In the case of DNS Redirect, the NXDOMAIN response is changed to reply with a resource record (RR) response which instructs the host computer to send the original request to a new IP address (see Figure 1 (DNS Redirect Response)).

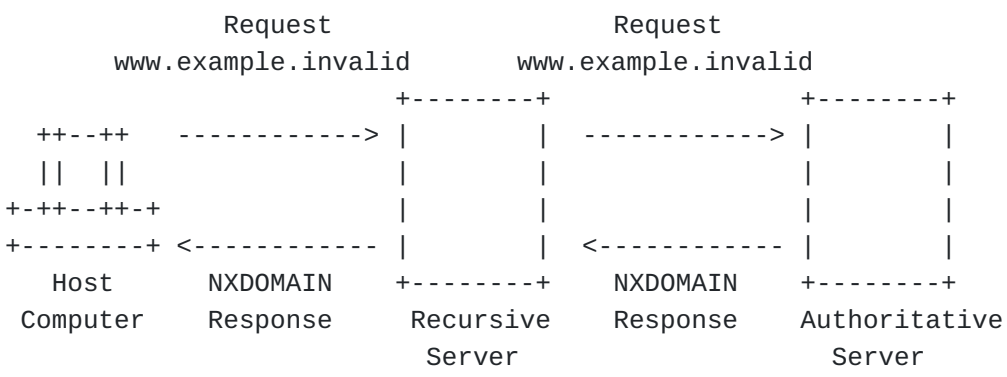

Figure 1: DNS Redirect Response

9.2. Web Error Landing Server

TOC

When a user requests an invalid URL or Domain, their web client is redirected to a Web Error Landing Server which presents several possible helpful website views (see Figure 2 (Web Error Landing Server)). The first is "Did you mean..." response which presents the user with possible correct results based on their original invalid request. The search server can also present search engine results to the user.

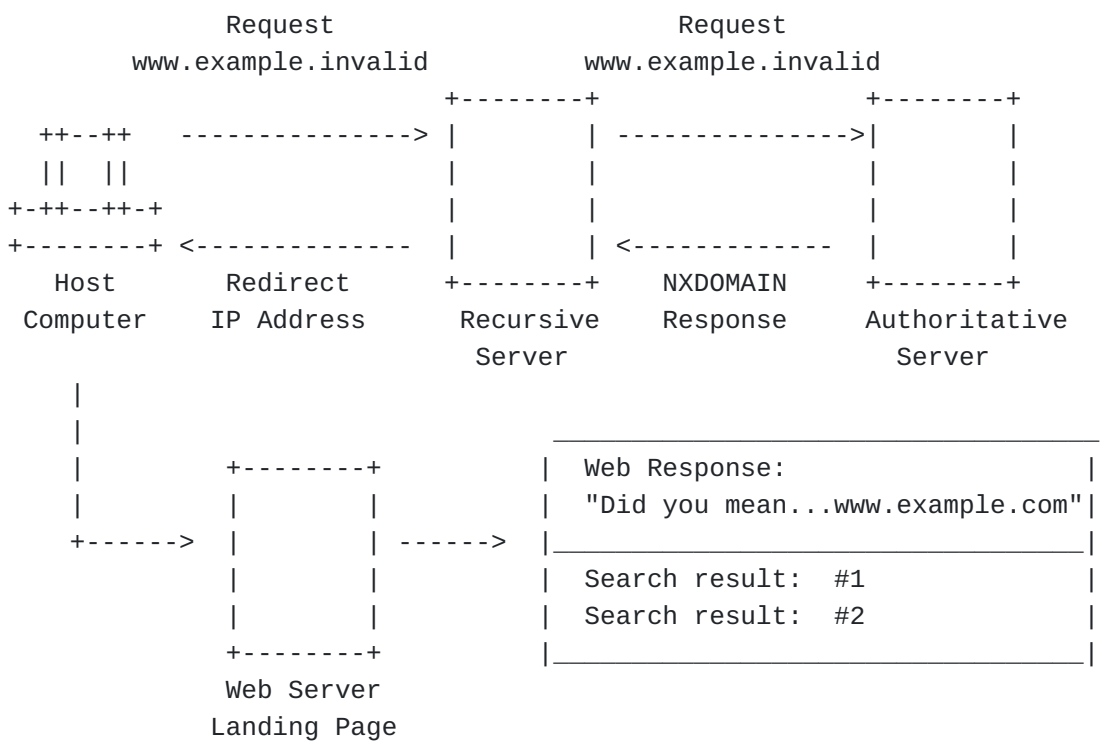

Figure 2: Web Error Landing Server

9.3. Web Browser Client

TOC

The Web Browser Client is redirected to a Web Server Landing Page instead of presenting an error page when there is no valid DNS record present.
Examples of common Web Browser Clients include:

* Microsoft Internet Explorer
* Mozilla Firefox
* Apple Safari
* Google Chrome
* Opera

9.4. Domain White List

TOC

There may be certain domains which should be not be redirected under any circumstances for technical, legal, business, or other reasons. The Domain White List can contain both domains, such as *.example.com, as well as specific FQDNs, such as www.example.com. For instance, the owner of example.com may request that the ISP or DNS ASP not perform DNS Redirect for the example.com domain, so that there is no DNS Redirect resulting from queries to nonexistent names, such as invalid.example.com.

---

10. Example DNS and HTTP Flows

TOC

This section shows several illustrated examples of DNS and HTTP flows, in order to better explain certain DNS and HTTP use cases.

10.1. Successful DNS Lookup and HTTP Flow

TOC

This example represents a successful lookup of a valid DNS RR, and the resulting HTTP transaction.

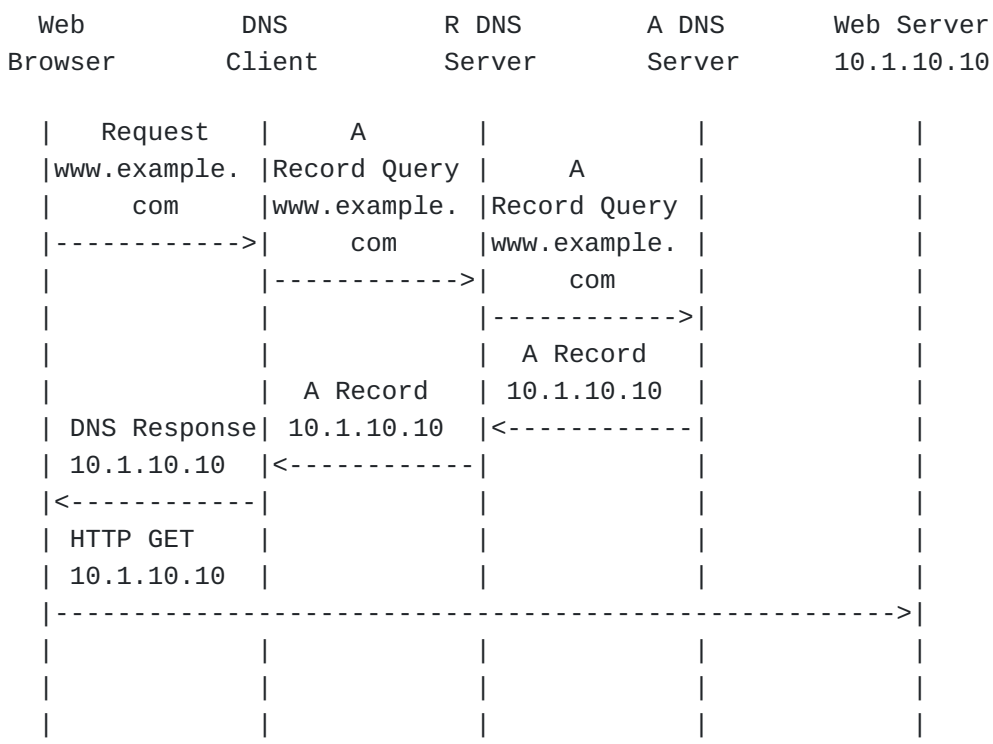

Figure 3: Successful DNS Lookup and HTTP Flow

10.2. Unsuccessful DNS Lookup and HTTP Flow

TOC

This example represents a lookup of a nonexistent DNS RR, and the resulting HTTP transaction.

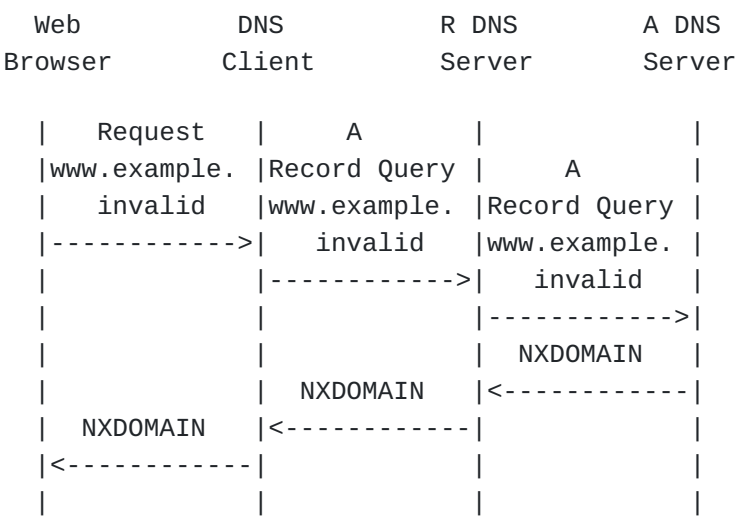

Figure 4: Unsuccessful DNS Lookup and HTTP Flow

10.3. DNS Redirect and HTTP Flow

TOC

This example represents a lookup of a non-existing DNS RR, and the HTTP transition that results from a typical DNS Redirect service.

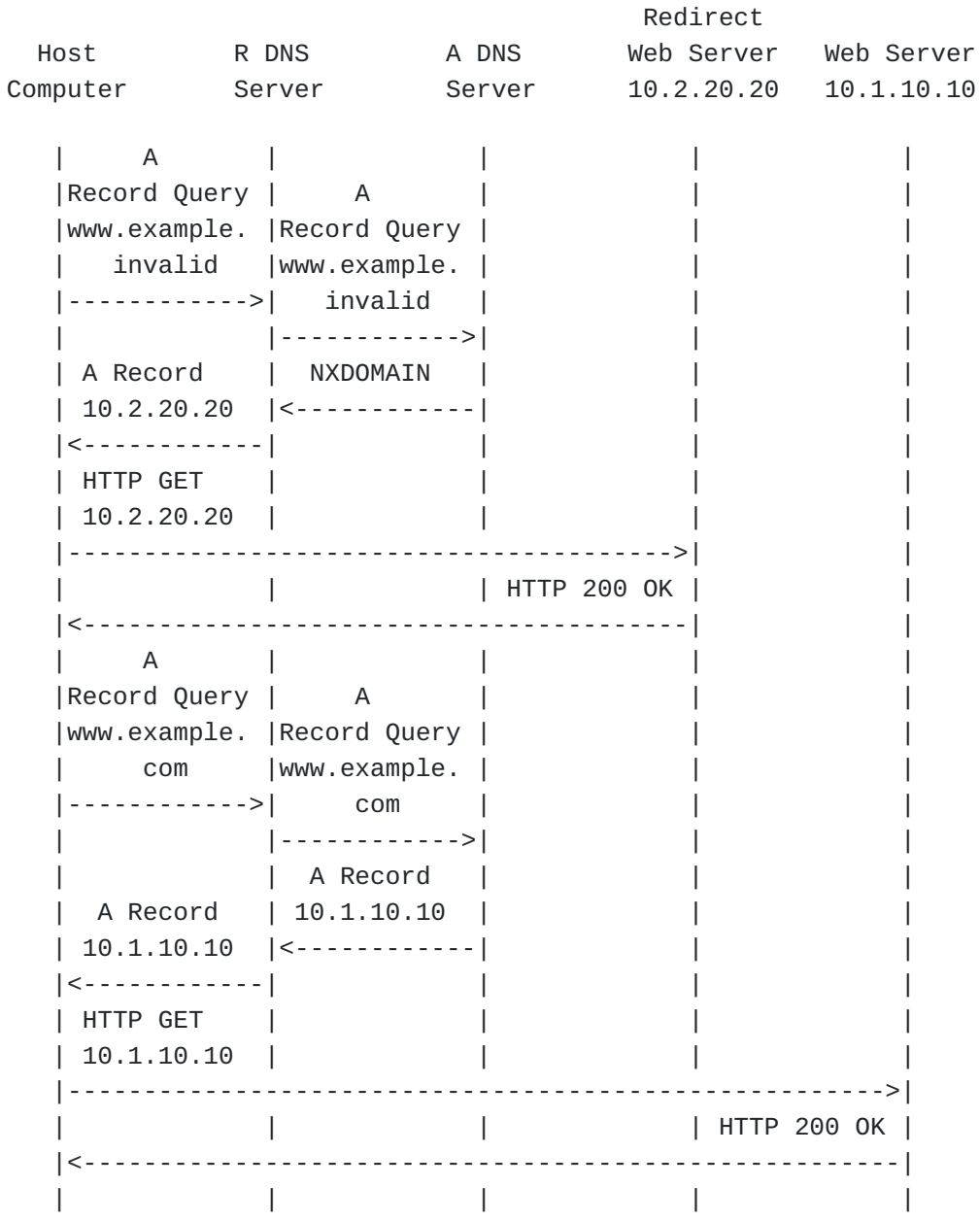

Figure 5: DNS Redirect and HTTP Flow

TOC

10.4. Improper Redirect of Valid Response Redirect and HTTP Flow

This example represents an improper redirect occurring when a valid DNS RR should have been returned in response to a DNS recursive query for an example website, the resulting HTTP transaction, and that no DNS query or HTTP traffic was sent to the valid authoritative DNS server and valid web server. Section 4 (DNSSEC Considerations and Implications) shows one of the reasons why this practice is problematic. Another reason is that a user intends to visit a valid resource with lawful and legitimate content, such as a web site, and is instead sent to a different destination (which may even closely resemble the intended site, in the pattern used by phishing sites).

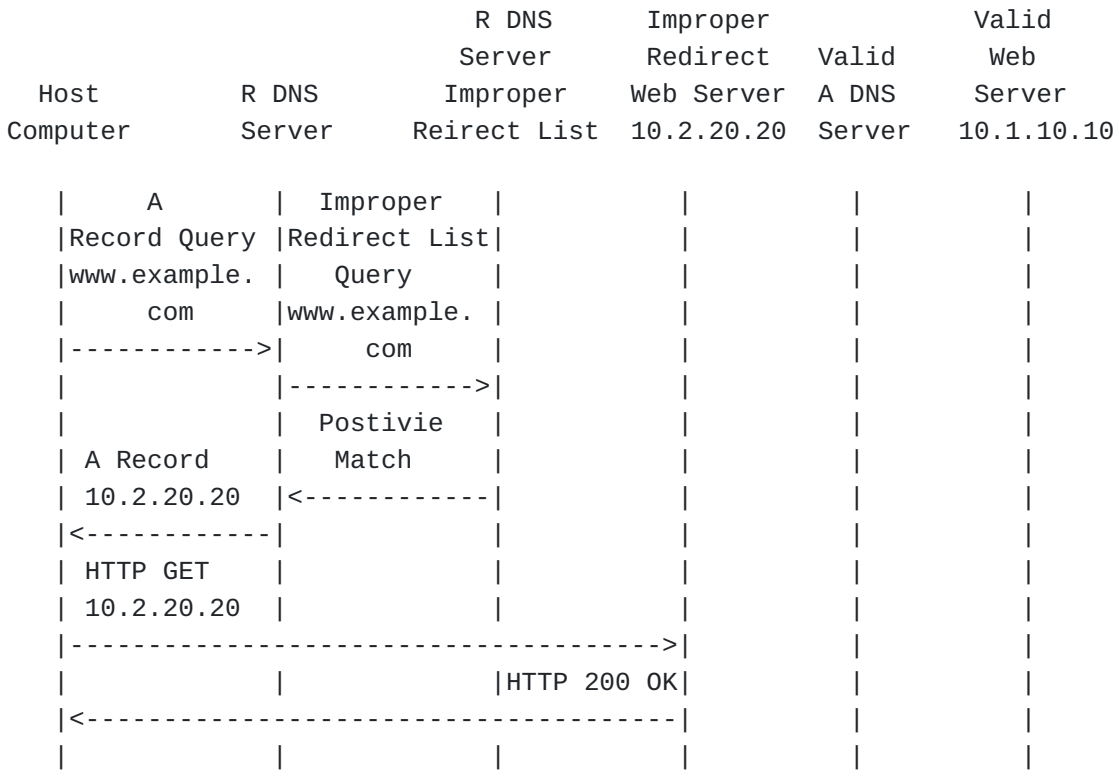

Figure 6: Improper Redirect of Valid Response Redirect and HTTP Flow

TOC

11. Security Considerations

The critical considerations relating to DNS Security Extensions are detailed in Section 4 (DNSSEC Considerations and Implications).
Security best practices should be followed regarding access to the opt-in and opt-out functions, in order that someone other than the user is able to change the user's DNS Redirect settings. For example, the User Options Web Server must not permit someone to modify a page URI to access and change another user's options. Thus, if the URI is "http://www.example.net/redirect-options.php?account=1234", someone must not be able to modify the account to be "=1235" and then be able to change the options for a different user with some other additional validation being performed. While web site security practices are outside the scope of this document, the authors believe it is important to identify such problematic use cases to any ISPs and DNS ASPs offering and/or implementing DNS Redirect functionality.

---

12. Controvery Surrounding DNS Redirect

TOC

It is clear based on the community feedback that this document has elicited, and from debates which have occurred over the years prior to this document, that DNS Redirect is a controversial topic. Views on whether DNS Redirect should be performed or not vary widely. Some feel strongly that it is a valid practice from which end users derive benefits. Some others feel that DNS Redirect should not be performed and that it puts at risk trust in and stability of the DNS. Others in the community are neutral on the topic and have expressed the view that as long as DNS Redirect does not slow the deployment of DNSSEC, that it is transparently disclosed to end users, and that those end users have easy opt-out methods, that it is an acceptable, or at least tolerated, practice. This moderate view is probably the majority view, though critics of DNS Redirect have expressed their views firmly and many of those holding such strongly critical views have played and continue to play a key role in DNS protocols and other critical areas of the IETF and the Internet community. Some strong critics also describe resolvers that perform DNS Redirect as "lying resolvers", explaining that the accurate and therefore honest response is an NXDOMAIN response and that anything else is not intended and is considered a lie.
Thus, it is important for readers to understand that DNS Redirect remains a practice which is subject to some controversy and that there is not strong consensus in support of it. At best, there is what could be described as grudging acceptance of the practice if it has been implemented along the lines recommended in this document. In addition, many critics take solace in the view that as DNSSEC is increasingly deployed that DNS Redirect is likely to decline correspondingly over time.

Finally, any provider implementing DNS Redirect is well advised to follow the recommendations outlined herein. This is because many critics of DNS Redirect have explained that their strong views developed or deepened when they observed that some implementers have deployed systems which fail to provide an easy and/or reliable opt-out method, redirect valid responses, or follow practices noted as ones to avoid in Section 8 (Practices to Avoid).

---

13. Future Prospects for DNS Redirect

TOC

As noted in Section 4 (DNSSEC Considerations and Implications), there exists today a technical incompatibility between DNSSEC and DNS Redirect. While it is possible that some provider implementing DNS Redirect today will uncover a method to implement DNSSEC and DNS Redirect, currently these two functions do not go well together. As such, providers will soon or are now facing a decision between embracing and deploying DNSSEC or continuing to perform DNS Redirect. It is likely that many of these providers will choose to deploy DNSSEC, as some already are doing [Comcast DNSSEC Rollout Announced] (Livingood, J., "DNS Security Rollout Begins," October 2010.). It is also possible that some others will deploy DNSSEC-validating DNS recursive resolvers alongside those resolvers performing DNS Redirect, giving their customers the choice between the two. In this case, it is likely that over time customers will express a preference for greater levels of Internet security, including DNSSEC and other forms of security, and that their respective service providers will evolve their offerings to satisfy these customer needs.

---

14. Why This Document Merits Publishing

TOC

Documentation of DNS Redirect is beneficial for the Internet community in and of itself. Prior to this document, the IETF lacked a stable reference document that described how DNS Redirect was designed and implemented, even though the practice has become relatively widespread. As a result, one benefit of publishing this is to document the design and implementation of DNS Redirect on the Internet.
An additional benefit of the document is to guide those providers which decide to implement DNS Redirect on what practices should be avoided and what steps should be taken to ensure that end users are able to easily and reliably opt out of such a system. While it does not seem appropriate, based on the community response noted in Section 12 (Controvery Surrounding DNS Redirect), to identify this as a Best Current Practices (BCP) document, this can guide implementers on what

to avoid and on "least worst" practices as some in the community have described them.
Furthermore, this documents other key aspects of DNS Redirect that are valuable. For example, this document encourages transparency and disclosure of DNS Redirect practices on the Internet, and notes community concerns and controversy regarding the practice, all of which may be valuable to refer back to in future documents or to refer to during future debates in the Internet community. There will also be future systems which call for well functioning opt-out systems. For such systems, the sections referring to automated opt-out mechanisms and reasonable processing times of opt-out requests, in Section 7.3 (Automated Mechanisms and Reasonable Processing Times), and the reliability of opt-out systems, in Section 8.4 (Routinely Broken, Purposefully Broken, and Otherwise Unreliable Opt-Out Mechanisms), may be valuable. Finally, Section 8.6 (Override of a User's DNS Selection) describes that a user's selection of an alternative DNS server IP address should not be overridden, which seems an important principle to highlight.

---

15. IANA Considerations

TOC

There are no IANA considerations in this document.

---

16. Contributors

TOC

The following people made significant textual contributions to this document and played an important role in the development and evolution of this document:
Don Bowman, Sandvine (don@sandvine.com)
Rick Hiester, Verizon (richard.hiester@verizon.com)
Chris Roosenraad, Time Warner Cable (chris.roosenraad@twcable.com)
David Ulevitch, OpenDNS (david@opendns.com)

---

17. Acknowledgements

TOC

The authors and contributors also wish to acknowledge the assistance of the following individuals in helping us to develop and/or review this document:
John Barnitz, Comcast Cable Communications
(john_barnitz@cable.comcast.com)
Mike Burns, Cablevision (mburns@cablevision.com)

Phil Marcella, Comcast Interactive Media
(phillip_marcella@cable.comcast.com)
Luis Uribarri, Comcast Cable Communications
(luis_uribarri@cable.comcast.com)
Sandy Wilbourn, Nominum (sandy.wilbourn@nominum.com)
Matt Williams, Cox Cable (matt.williams@cox.com)
The authors and contributors also wish to thank ICANN's Security and Stability Advisory Committee (SSAC) for their review and debate of this document, as well as for raising important questions concerning DNSSEC compatibility.

18. References

TOC

18.1. Normative References

TOC

[RFC1034]	Mockapetris, P., “Domain names - concepts and facilities,” STD 13, RFC 1034, November 1987 (TXT).
[RFC1035]	Mockapetris, P., “Domain names - implementation and specification,” STD 13, RFC 1035, November 1987 (TXT).
[RFC1536]	Kumar, A., Postel, J., Neuman, C., Danzig, P., and S. Miller, “Common DNS Implementation Errors and Suggested Fixes,” RFC 1536, October 1993 (TXT).
[RFC1591]	Postel, J., “Domain Name System Structure and Delegation,” RFC 1591, March 1994 (TXT).
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2131]	Droms, R., “Dynamic Host Configuration Protocol,” RFC 2131, March 1997 (TXT, HTML, XML).
[RFC2136]	Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, “Dynamic Updates in the Domain Name System (DNS UPDATE),” RFC 2136, April 1997 (TXT, HTML, XML).
[RFC2181]	Elz, R. and R. Bush, “Clarifications to the DNS Specification,” RFC 2181, July 1997 (TXT, HTML, XML).
[RFC2308]	Andrews, M., “Negative Caching of DNS Queries (DNS NCACHE),” RFC 2308, March 1998 (TXT, HTML, XML).
[RFC4033]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements,” RFC 4033, March 2005 (TXT).
[RFC4034]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Resource Records for the DNS Security Extensions,” RFC 4034, March 2005 (TXT).
[RFC4035]	

	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions," RFC 4035, March 2005 (TXT).

18.2. Informative References

TOC

[Comcast DNSSEC Rollout Announced]	Livingood, J., "DNS Security Rollout Begins," Comcast Blog , October 2010.

Appendix A. Document Change Log

TOC

[RFC Editor: This section is to be removed before publication]
-03: Changed some text to make it more neutral, and introduced new sections: Controvery Surrounding DNS Redirect, Future Prospects for DNS Redirect, and Why This Document Merits Publishing. Also closed out an open issue to remove references to RFC 2535, which is obsolete. Lastly, updated the section 8.6 on override of user DNS choices to note a malware case raised during a document review.
-02: Fixed some small grammatical nits.
-01: Removed sections regarding malicious domain protection, legally-mandated redirect, and content-based redirect based on DNSOP WG feedback to split those out into separate documents which will be published in the future. Also significantly modified the DNSSEC section and moved it to the top of the document. Also, capitalized applicable 2119 language.
-00: First version published.

Appendix B. Open Issues

TOC

[RFC Editor: This section is to be removed before publication]

1. RW: Consider whether it is a good idea to add to section 4.9 (NXDOMAIN RESPONSE) a reference to Authenticated Denial of Existence described in RFC4035 section 5.4 as these should be also redirected.

2. MB: Consider addressing how opt-out works when a user roams across a shared WiFi AP.

3. Ensure that references are in the appropriate section (normative vs. informative).

Authors' Addresses

TOC

	Tom Creighton
	Comcast Cable Communications
	One Comcast Center
	1701 John F. Kennedy Boulevard
	Philadelphia, PA 19103
	US
Email:	tom_creighton@cable.comcast.com
URI:	http://www.comcast.com
	Chris Griffiths
	Comcast Cable Communications
	One Comcast Center
	1701 John F. Kennedy Boulevard
	Philadelphia, PA 19103
	US
Email:	chris_griffiths@cable.comcast.com
URI:	http://www.comcast.com
	Jason Livingood
	Comcast Cable Communications
	One Comcast Center
	1701 John F. Kennedy Boulevard
	Philadelphia, PA 19103
	US
Email:	jason_livingood@cable.comcast.com
URI:	http://www.comcast.com
	Ralf Weber
	Unaffiliated
	Bleichgarten 1
	Hohenahr-Hohensolms 35644
	Germany
Email:	rw@hohensolms.de