From the Office of Russell S. Lewis
Executive Vice President & General Manager
Phone: (703) 948-3490
Facsimile: (703) 421-2129

FACSIMILE TRANSMITTAL SHEET

TO:
PLEASE DELIVER TO :

Paul Twomey

FROM: RUSSELL S. LEWIS

COMPANY: ICANN

DATE: OCTOBER 6, 2003

PHONE NUMBER: (310) 823-9358

TOTAL NO. OF PAGES INCLUDING COVER: 9

FAX NUMBER: (310) 823-8649

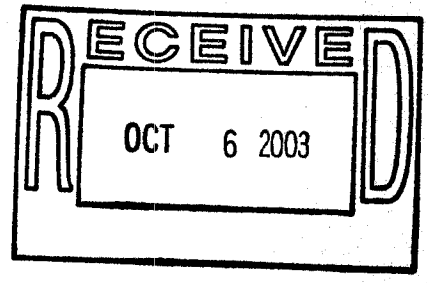
SENDER'S REFERENCE NUMBER: IAB RESPONSE

RE: IAB RESPONSE OCTOBER 06, 2003

YOUR REFERENCE NUMBER:

☐ URGENT ☐ FOR REVIEW ☐ PLEASE COMMENT ☐ PLEASE REPLY ☐ PLEASE RECYCLE

NOTES/COMMENTS:



October 6, 2003

Dr. Paul Twomey
President and Chief Executive Officer
Internet Corporation for Assigned Names and Numbers
4676 Admiralty Way #330
Marina del Rey, CA 90292

Re: IAB Commentary: Architectural Concerns on the Use of DNS Wildcards

Dear Paul:

Please find enclosed VeriSign's response to the IAB Commentary: Concerns on the Use of DNS Wildcards. I would be happy to discuss this further with you at your convenience.

Sincerely,

Russell S. Lewis
Executive Vice President
General Manager
Naming and Directory Services

cc: Kevin Golden, Esq.
Ben Turner
Rusty Lewis
John Jeffrey, Esq.
Esme Smith, Esq.
Dan Halloran

October 06, 2003

VeriSign's Response to IAB Commentary "Architectural Concerns on the Use of DNS Wildcards" dated September 23, 2003.

On September 23, 2003, the IAB issued a commentary entitled "Architectural Concerns on the use of DNS Wildcards." This commentary describes various implications of the implementation of DNS wildcards in a zone, paying particular attention to VeriSign's recent deployment of a wildcard A record in the .com and .net zones on September 15, 2003. As with the IAB's review of VeriSign's binary redirect for non-ASCII domain names, VeriSign appreciates the opportunity to comment on the IAB's views on our wildcard implementation and looks forward to continuing an open dialog with the IAB on this and future services.

This response will address the IAB commentary, using observed operational data to put the issues into context. This response does not address the wildcard primer nor any non-technical considerations raised in the commentary, which VeriSign believes are more appropriately addressed in a different form.

Standards

The IETF standards explicitly address the use of a wildcard A record in a zone. Therefore, any discussion of wildcards must begin with the applicable standards. RFCs 1034 and 1035, the core DNS specification documents, describe wildcards. VeriSign's implementation of a wildcard A record in the .com and .net zones is fully compliant with these documents. As the commentary states, "We must emphasize that, technically, this was a legitimate use of wildcard records that did not in any way violate the DNS specifications themselves."

It is worth noting that the addition of the wildcard A record to the .com and .net zones has not in any manner compromised the stability, security or performance of the .com/.net name server system. As was the case before the addition of the wildcard, VeriSign is resolving more than 10 billion DNS queries per day, at a rate of over 140,000 queries per second, with 100% availability.

VeriSign has invested tens of millions of dollars in this infrastructure to ensure high availability and reliability. Our consistent monitoring of the .com and .net infrastructure, and the fact that the company has continually deployed additional capacity based on anticipated demand, has been a key factor in the continued stable, secure, and predictable growth of the Internet. VeriSign spent years developing a proprietary and highly scalable technology called ATLAS to support the rapid growth of resolution on the .com/.net name server system, which has been doubling every 12 to 18 months. Our ATLAS infrastructure has the important added benefit of further fortifying the system against

DDoS (distributed denial of service) attacks. This investment ensures that the Internet continues to be a commercially vibrant and global medium, with an infrastructure that is deterministic, robust, reliable and highly scalable.

Discussion of Issues Raised in the IAB Commentary

Language Tags

The IAB commentary notes that, prior to a wildcard A record in the .com and .net zones, web browsers displayed "page not found" in the local language of the user but now return an English language web page. The concern raised by this point is that the prior user experience of receiving a technical error response in a user's native language may be more useful than ah navigation aid web page in English. Note however that some of the most common web browsers, such as Microsoft's Internet Explorer, already redirect the user to a web page that may not be in the user's preferred language when a "no such name" response is received.

In general, it is questionable as to whether a user finds a technical error page more helpful than a web page in English that assists in navigation, particularly given that 68% of all web pages are in English[1].

VeriSign realizes that the Internet is a global medium and believes offering a localized version of Site Finder would be positively received by the international community. In order to address additional languages, VeriSign is actively working on plans to introduce languages such as German (5% of web pages), Japanese (5% of web pages), Spanish (2% of web pages), French (2% of web pages) and Chinese (3% of web pages) in the near future. This will be accomplished using the best practices outlined by the W3C for use of HTTP Accept-Language headers to determine the desired language of the user. The localized Site Finder page will also allow the user to change to a version of the page rendered in another language.

Email

The IAB commentary notes that mail sent to a nonexistent hostname for TLDs that have deployed a wildcard A record now flows to a "bounce server" that rejects such messages. As a result, the commentary states a number of issues:

The SMTP bounce server increases load for MTAs (Mail Transfer Agents)

VeriSign is not aware of any empirical data supporting this claim. However, we would consider and welcome comments regarding the addition of a wildcard MX resource record set to the .com and .net zones. The MX resource record set would contain a single

[1] Global-Reach, September, 2003

record whose target domain name does not exist (i.e., queries for it will return a Name Error/RCODE=3 response.) According to RFC 2821, the presence of this MX record will inhibit any A record lookups by compliant SMTP servers, and the record's nonexistent target domain name is an error condition that must be reported. In VeriSign's testing, the vast majority of the installed base of SMTP implementations treats this condition as a "hard" failure: any message is bounced immediately back to the sender.

The SMTP bounce server does not return the proper SMTP response

The current SMTP bounce server rejects any mail sent to it by returning a 550 response to any number of RCPT TO commands. The initial version of the SMTP bounce server did reject emails that were directed to it. Based on feedback from the Internet community that this server did not support a complete implementation of the SMTP protocol, the server was quickly updated.

Problems with mail server configurations with mistyped MX records.

As a basic matter, email behavior has not changed for correctly configured existing domains. The failure of mail applications noted by the IAB commentary results from a misconfiguration of the MX records associated with a domain name on the user's part. In fact, the presence of a wildcard A record and the SMTP bounce server's current behavior actively helps identify an unrecognized incorrect configuration in the user's zones. The problem is easily corrected by the user.

This misconfiguration is extremely rare in practice. For example, an analysis by VeriSign of over 20 million MX records for .com and .net domains shows that less than one tenth of one percent of these records (only 0.077% to be precise) specify a domain name that resolved via the wildcard A record in .com and .net. To put this figure in perspective, a much more common misconfiguration of MX records listing an IP address rather than a correctly formatted domain name occurs 1.49% of the time in the same set—2000 times more frequently than the misconfiguration above.

In the event that the wildcard MX record option described above is implemented, the SMTP bounce server will be discontinued. Instead, connections to TCP port 25 at the wildcard A record's IP address will be reset. This behavior will cause a compliant SMTP implementation to discard the MX record with the nonexistent target and result in a "soft" error, not a "hard" error and a bounced message, effectively addressing the IAB's issue with mistyped MX records.

Troubleshooting incorrectly configured mail clients such as Outlook Express is more difficult

The IAB commentary describes the situation when a user incorrectly configures his or her mail client's outgoing SMTP proxy. In the event that the wildcard MX record option described above is implemented, incorrectly configured mail clients would no longer be

able to submit mail to the bounce server and would not receive an SMTP response indicating that the destination domain does not exist.

Informing Users of Errors

In some cases application developers have written programs to use a domain name lookup as a validation step prior to the program progressing to the subsequent step. The IAB commentary notes that with the introduction of wildcards, this validation check may no longer work as intended. Using domain names for this purpose creates possible security issues, such as the accidental or malicious registration of a domain name that could result in application errors or email being misdirected. As a matter of best practices, for example, Microsoft encourages administrators to avoid this practice. In addition, even if domain names were used in this manner, application developers have always had the ability to query the DNS for the presence of a wildcard A record in a zone. VeriSign has created an "Applications Developer's Guide to DNS Wildcards" which describes these methods. The Guide can be found at: http://sitefinder.verisign.com/pdf/sitefinderdevguide.pdf

Spam

VeriSign believes that fighting spam on the Internet is an important endeavor. The IAB commentary states that the implementation of wildcards has degraded the effectiveness of using a DNS lookup to verify the existence of the sender's domain as a type of spam filter. VeriSign has investigated whether the major service providers or software vendors providing spam solutions use this type of filter. Based on feedback from these providers, it does not appear to be a widely implemented mechanism for spam identification and discovery. Though this mechanism is implemented in some MTAs, it identifies only 3% of spam messages[2]; that is, only 3% of all spam purports to come from a nonexistent domain. In addition, this check is apparently no longer effective because it is easily circumvented and those who send spam have learned of its ubiquity. Anti-spam software is frequently updated to counter the techniques used by spammers, and can be easily updated to operate in the presence of wildcard entries in the .com and .net zones. VeriSign will create a document describing options and recommending best practices for application developers to achieve the same result in the presence of wildcard records in the .com and .net zones.

Interaction with other protocols

Prior to the introduction of the wildcard, VeriSign developed a set of guidelines describing the proper implementation of wildcards in TLD zones that includes interaction

[2] This figure is based on internal VeriSign analysis of a large corpus of spam across various domains and is in line with other industry sources.

of protocols and possible mitigation strategies. The guidelines are available at http://www.verisign.com/nds/naming/sitefinder/index.html.

Automated Tools

The IAB commentary notes that some automated tools may fail in unexpected ways due to a wildcard A record. In order to address this concern for automated tools related to HTTP, the Site Finder web site includes a "robots.txt" file. This is a common practice used to direct automated web spidering tools not to spider a specific web site.

In addition, the Site Finder web server explicitly returns no information to media players using HTTP precisely because the content of the site is not the intended target of such applications. Also, using HTTP on port 80 for applications other than web browsing is explicitly discouraged according to BCP 56/RFC 3205. Tools incorporating such practices should be sufficiently robust when encountering unexpected web pages because the HTTP protocol on port 80 was not intended for any other use.

Charging

The IAB Commentary raises a concern over increased cost to a user because the Site Finder initial response page is 17 Kbytes of data as opposed to a smaller footprint for a negative response in DNS. VeriSign is not aware of any concerns raised by Internet users in this regard. It should also be noted that for comparison's sake, the default MSN search service page for mistyped domain names using Microsoft's Internet Explorer browser is 135 Kbytes or approximately eight times larger than the Site Finder response.

Single Point of Failure

The IAB commentary raises the issue that a wildcard service creates a possible single point of failure as well as a target for deliberate attacks. When considered as a unit, a zone's name servers are a single point of failure. A redundant architecture addresses this issue. For example, by employing redundancy, VeriSign has operated the .com and .net name servers with 100% uptime over the past six years. The Site Finder architecture follows the same principles. In addition, given our experience in operating critical portions of the Internet's DNS infrastructure as well as significant application services, VeriSign is aware of the operational security requirements for the Site Finder service. VeriSign is performing regular daily monitoring of the Site Finder service infrastructure using standard and specialized tools to ensure its continued operational robustness.

Privacy

The IAB commentary states that a wildcard may raise privacy issues. VeriSign does not collect or retain any personal information through the Site Finder service. In addition, VeriSign does not retain, nor do we have any intention to retain, any email addresses from SMTP transactions. In fact, to achieve optimum performance, all logging at the SMTP bounce server has been disabled. Further, if the wildcard MX record is deployed, the SMTP bounce server will be eliminated.

VeriSign's Site Finder privacy policy is available to Internet users via a link in the bottom left hand corner of the Site Finder page. VeriSign has developed a FAQ related to privacy for the Site Finder service, which can be found at http://www.verisign.com/nds/naming/sitefinder/privacy_faq.html.

The commentary also raises the additional privacy concern that the new Site Finder service would be particularly attractive to malicious attack or hijacking. As part of standard operating procedures, VeriSign is monitoring the service closely to detect the advent of any such activity and is using industry standard and highly robust tools and practices to prevent and detect potential attacks.

Reserved Names

The IAB commentary raises an issue with reserved names and IDNs. The issue with IDNs as described by the commentary is still evolving. ICANN confirms "As the deployment of IDNs proceeds, ICANN and the IDN registries will review these Guidelines at regular intervals, and revise them as necessary based on experience." It is perhaps appropriate to review the IDN guidelines in the context of conformance with the DNS protocol, since the guidelines require conformance with RFC 3490, which incorporates Standard 13 (including RFCs 1034 and 1035) as a normative reference. RFC 1034 specifically allows wildcard resource records to appear in zones. Further, the use of wildcards with IDNs can help the user with improved navigation by mapping the reserved variants to the registered domain name.

To the issue of whether the wildcard service resolves registered names that are not in the .com or .net zones, it should be noted that such names couldn't be resolved. Similar to both the Microsoft and AOL error pages, the initial Site Finder page displays a message reflecting that a particular domain name is not present in DNS. VeriSign is receptive to implementing a solution that will not return the initial Site Finder page for domains not in the .com and .net zones and welcomes comments from the community.

Undesirable Workarounds

The commentary notes that the IAB is concerned about various workarounds that have appeared in order to bypass wildcards. VeriSign shares the IAB's concerns. In order to assist application developers to write software that is consistent with the DNS standards, VeriSign has published the "Application Developer's Guide to DNS Wildcards", which can be found at http://sitefinder.verisign.com/pdf/sitefinderdevguide.pdf. To the extent that workarounds are not standards-based, the appropriate action by the IAB and other technical coordinating bodies should be to discourage these practices.

IAB Recommendations

The IAB commentary makes two basic recommendations:

1. Wildcards should not be used unless the zone operator has a clear understanding of the risks.
2. Wildcards should not be used without the informed consent of those entities, which have been delegated below the zone.

Wildcards should not be used Without an Understanding of the Risks

In the case of the wildcard A record in the .com and .net zones, VeriSign conducted extensive evaluation and testing of the service both internally and externally and with the assistance of third-party experts. The pre-launch testing results indicated, and current operational data confirms, no impact to the stability of the Internet. Other concerns raised by the IAB have been addressed in this document.

Wildcards Should not be used without Informed Consent

This comment overlooks the fact that extensive debate and consideration went into the drafting and acceptance of the IETF standards for DNS that explicitly anticipate wildcards and allow for their usage. The establishment of best practices regarding notices of the introduction of non-regulated services for a zone would be an alternative constructive recommendation.

Conclusion

VeriSign is fully committed to a secure, stable and interoperable Internet that will continue to innovate and grow in a responsible manner. It is important to recognize that striving to make the user experience the best it can be without sacrificing stability and security is an objective that benefits us all.