IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

NETSPHERE, INC., MANILA INDUSTRIES, INC., AND MUNISH KRISHAN,	§ § § §	
Plaintiffs,	§ § §	
v.	§ §	Civil Action No. 3:09-CV-0988-F
JEFFREY BARON AND ONDOVA LIMITED COMPANY,	§ § § §	
Defendants.	§ § § §	

NON-PARTY ICANN'S RESPONSE TO THE RECEIVER'S SECOND MOTION AND SUPPLEMENT TO SECOND MOTION TO ENFORCE STAY

I.   EXECUTIVE SUMMARY

The Receiver asks that the Court order non-party ICANN to somehow take five domain names away from the current registered name holders in order to change the registration data of those five domain names to identify the Receiver as the new registered name holder.[1] Contrary to the Receiver's inaccurate and misleading assertions regarding ICANN's ability and authority to effectuate such domain name transfers – assertions made on information and belief and without <u>any</u> factual support – the domain names identified in the Receiver's motion are

---

[1] There are 22 domain names that are the subject of the Receiver's second motion to enforce the stay in this case. Each of the 22 domain names was subject to a UDRP proceeding and in each case the UDRP panel ordered that the domain names be transferred to the UDRP complainant. However, only five domain names were actually transferred by the registrar (Fabulous.com) to a new domain name holder as ordered by the URDP provider. Fifteen of the domain names have not been transferred and remain with the UDRP respondent; two of the domain names are not even registered anymore. Thus, insofar as ICANN is concerned, the Receiver seeks an order requiring ICANN to "re-transfer" five domain names to the Receiver.

For the Court's convenience, ICANN is filing a chart that shows each domain name identified in the Receiver's motion, along with the decision entered by of the UDRP provider, identification of the current registrar, current registered name holder, and the status of the domain name (i.e., whether it has been transferred or not). *See* Exhibit A, attached to the declaration of Kurt Pritz.

controlled by the respective registered name holders, not ICANN. Only a registered name holder has the authority and ability to change its registration information and thus effectuate a change in control of its domain name registration to a different registered name holder. ICANN lacks the authority to force a third party to give up its rights as a registered name holder and transfer domain names to the Receiver. And even if ICANN had such authority (which it does not), ICANN does not have access to a registered name holder's registration information and thus lacks the technical ability to change the registrations and effectuate a transfer of the domain names to the Receiver.

For these reasons and those described more fully below, ICANN respectfully requests that the Court deny the Receiver's second motion to enforce the stay.[2]

II.   ARGUMENT

By his second motion to enforce the stay, the Receiver seeks an order: (a) declaring certain default judgments entered by various UDRP tribunals void based on the Receivership stay; (b) requiring the registrar to disregard the default judgments and not transfer these domain names (as ordered by the respective UDRP tribunals); and (c) requiring ICANN to "re-transfer back to the Receivership estate any of these domain names already transferred pursuant to the default judgments." (Mot. at 1.)

ICANN takes no position regarding (a) – whether this Court may declare default judgments entered in UDRP proceedings void based on the receivership stay in this case. As established in ICANN's previous filings in this matter, ICANN does not preside over or otherwise administer or participate in UDRP proceedings. (*See* Dkt. #s 728, 737.) The interplay between UDRP decisions and orders entered in the instant case is an issue between the Receiver

---

[2] ICANN objected to this Court's jurisdiction over ICANN in its response to the Court's Order to Show Cause and incorporates such objection herein. (Dkt. # 728.) This response in no way constitutes a waiver of ICANN's defense of lack of personal jurisdiction, a defense that ICANN expressly preserves.

here, the Court, the dispute resolution provider administering the UDRP proceeding and the

parties to the UDRP proceeding – not ICANN.

Nor will ICANN address (b) – the Court's ability to direct the registrar (Fabulous.com) to

ignore UDRP decisions and not transfer the domain name registrations, except to note that

Fabulous.com is apparently already ignoring many of the UDRP decisions. When a UDRP

provider orders the transfer of a domain name, the transfer must take place within ten days.

Here, despite the entry of the UDRP panel's transfer orders many months ago, Fabulous.com has

not transferred 15 of the 22 domain names at issue in the Receiver's motion. (Pritz Decl., ¶¶ 6,

8, Ex. A.)[3] Because the UDRP decisions were entered months ago, coupled with

Fabulous.com's apparent willingness to ignore these orders, the Receiver's request appears moot.

The Receiver's request also is untimely, as it only now is asking the Court to order Fabulous.com

to ignore the UDRP decisions, some of which were entered nearly one year ago.[4]

ICANN is filing this response to address (c) – the Receiver's request that the Court order

ICANN to "re-transfer back to the Receivership estate any of these domain names already

transferred pursuant to the default judgments." (Mot. at 1.) Only five of the domain name

registrations have been transferred pursuant to a UDRP decision – wetafx.com,

publicstorge.com, pulicstorage.com, puplicstorage.com, and aplle.com. (Pritz Decl., ¶¶ 6, 8,

Ex. A.) ICANN was not involved in these transfers, and it lacks both the technical capability to

---

[3] The Registrar Accreditation Agreement that ICANN enters into with each ICANN-approved registrar, including Fabulous.com, requires the registrar to comply with UDRP decisions. As highlighted in the Receiver's second motion to enforce the stay, Fabulous.com's apparent failure to transfer these domain names pursuant to the UDRP panel decisions and its Registrar Accreditation Agreement may be cause for ICANN to initiate a contractual compliance review of Fabulous.com.

[4] The exhibits filed in support of the Receiver's motion demonstrate that persons purporting to represent the Receiver were aware of and participated in the UDRP proceedings.

Each of the UDRP proceedings referenced by the Receiver resulted in a finding that the domain names were being used improperly and the names should be transferred to the complainants. The findings of the UDRP panels should not be taken lightly by this Court, and any consideration of the completion of a transfer should also take into account measures to protect the claimants from any further harm from the Receivership estate's use of the domain names.

effectuate the requested relief and the authority to require a registered name holder or a registrar to change the registration information in favor of the Receiver. As such, the Receiver's request for relief as to ICANN should be denied. ICANN will also address the Receiver's supplement to his second motion, which wrongly suggests that ICANN has the ability to order UDRP providers to terminate UDRP proceedings.

A.   ICANN Does Not Have The Technical Capability Or Authority To Transfer Domain Names.

Registering, transferring, or deleting a domain name involves interaction – and a series of contracts – between the registered name holder, the registrar and the registry.[5] ICANN is not involved. In order to register a domain name (and become a registered name holder), one first has to go to an ICANN-accredited registrar or reseller,[6] which collects information about the registered name holder (such as identifying information on the registered name holder, name server address, billing information, and other contact information) as part of the registration process. (Pritz Decl., ¶ 9.) The registered name holder and registrar then enter into a registration agreement. (*Id.*)

For that domain name registration to appear on the Internet, the registrar must then provide information to the registry (the registry for .COM is VeriSign). (*Id.* at ¶ 10.) The registrar maintains a contract with each registry for which it is authorized to do business, and the transfer of information between the registry and the registrar occurs pursuant to this agreement. (*Id.*)

---

[5] There is only one registry that maintains the central database for all domain names in a given TLD. By contrast, there are several hundred ICANN-accredited registrars authorized to register domain names in any given TLD for individual registered name holders.

[6] If through a reseller, the reseller acts as an agent for the ICANN-accredited registrar.

ICANN is not involved in either the collection or maintenance of information on individual domain name registrations. (*Id.* at ¶ 11.) Indeed, ICANN plays no role whatsoever in the registration of individual domain names.

Registrars are responsible for making some of the registered name holder's identifying information publicly available through a Whois service. (*Id.* at ¶ 12.) The Whois database is a standard or protocol that allows users to type in the domain name they wish to query for information on whether a name is registered, and if so, when it was registered and by whom. (*Id.*) Internet users around the world can access Whois services to identify information on registered name holders, but they do not have the ability to change the Whois information on names for which they are not the registered name holders. (*Id.*) ICANN does not maintain or have access (other than what is publicly available to everyone) to a registrar's Whois database. (*Id.* at ¶ 13.) In fact, for ICANN to learn information on individual domain name registrations, ICANN must perform the exact same query through a registrar's Whois service that this Court or anyone else would have to perform. (*Id.*)

ICANN does not have the authority, discretion or access to change registration information. (*Id.* at ¶ 14.) ICANN does not contract with registered name holders and maintains no policy or other initiative governing what steps a registered name holder must undertake to change its registration information to change control of a domain name to a new registered name holder. (*Id.* at ¶ 15.) That process is dictated by the registration agreement between the registered name holder and the registrar. The steps required to change the control over a domain name to a different registered name holder vary; each registrar maintains its own registration agreement. (*Id.*) Generally, however, the registered name holder and the registrar communicate via a secured electronic and automated system. Using automated commands, the current

registered name holder must inform the registrar of the change in registration information, and specifically identify of the new registered name holder. (*Id.*)

Only the current registered name holder (or registrar, pursuant to a court or UDRP tribunal order) has the discretion and authority to change the registration information and thus effectuate a "transfer" of a domain name to a new registered name holder. (*Id.* at ¶ 16.) Moreover, only the registered name holder is authorized to inform the registrar of a change in the registration information so that the registrar may accurately populate the Whois database. (*Id.* at ¶ 17.) ICANN lacks the discretion, authority and technical ability to transfer domains name from one registered name holder to another or force a registered name holder to give up its domain name registrations and transfer them elsewhere. (*Id.* at ¶ 18.)[7]

In sum, contrary to the Receiver's assertions (without evidentiary support), ICANN does not have access to the necessary data in order to change registration information from one registered name holder to another. (*Id.* at ¶ 25.) Nor does ICANN have the authority – by virtue of contract, policy or otherwise – to direct a registered name holder or a registrar to initiate a transfer request, approve a transfer request, or instruct a registry to undo a transfer already

---

[7] The only situations where ICANN is involved in a transfer of names is in "bulk" transfer scenarios between two registrars. The bulk transfer provisions require transfer of all registrations sponsored by one registrar to another, either due to: (i) the acquisition of that registrar or its assets by another registrar; or (ii) lack of accreditation of that registrar. The bulk transfer provisions do not allow for a change of registered name holder – only a change of registrar. (Pritz Decl., ¶ 23.)

Even in these bulk transfer cases, it is not ICANN that completes the transfer. The transfer can only be completed by the registry. (*Id* at ¶ 24.) ICANN provides only the process and necessary approvals. ICANN does not have access to the registry database and cannot technically complete the transfer between registrars. (*Id.*) In any event, the Receiver has not asked the Court to order ICANN to undertake such a "bulk" transfer.

Nor does ICANN have the authority to transfer individual domain names between registrars. According to the .COM registry agreement, upon a request from the registered name holder, the new (gaining registrar) will issue a Transfer command to the registry. (*See id.* at ¶¶ 19-21, Ex. B (.COM Registry Agreement, App. C, § 4.3.10 (Transfer).) The current (and potential losing) registrar then has five days to approve or reject the transfer. The registry then processes the transfer. ICANN is not involved in the individual domain name transfer process. (*Id.* at ¶ 21.)

Moreover, only the registry has the technical ability and authority to undo an inter-registrar transfer after a transfer has occurred. (*Id.* at ¶ 22, Ex. C (Policy on Transfer of Registrations between Registrars, at § 6 (Registry Requirements) (specifying limited circumstances when the registry may undo a transfer).)

effectuated. (*Id.*) Each of these matters is specifically governed by contractual relationships between registered name holders and registrars and between registries and registrars. *Id.*

There is no policy or contract or other language anywhere that authorizes ICANN to initiate or process or "undo" transfer requests, either from one registered name holder to another or between registrars, or otherwise direct the registered name holders, registrars or registry to do so. (*Id.* at ¶¶ 14-15.) The Receiver fails to point the Court to <u>any</u> policy or process or contract language that would even arguably grant ICANN the authority to initiate or process or "undo" transfer requests. Nor does the Receiver offer evidence that there exists a technical process by which ICANN could effectuate such a transfer. Moreover, the Receiver can cite no case where ICANN was ordered to forcibly change rights of one registered name holder in favor of a different registered name holder. Instead, as he has done repeatedly in this matter, the Receiver makes bald assertions "on information and belief" but with <u>no evidence</u> to support those assertions.

In support of his statement that "ICANN has the ability to immediately re-transfer such domain name (sic) back to the LLCs (*i.e.*, the Receivership estate)" (Mot. at 8), the Receiver relies on the declaration of Damon Nelson. But Mr. Nelson's declaration does not contain any facts or other basis from which to conclude that Mr. Nelson has any personal knowledge on the issue. Instead, it posits Mr. Nelson's (unfounded) "belief." (Declaration of Damon Nelson, ¶ 22, Dkt. # 739) ("I also ***believe*** that, for any Domain Name at issue that might have already been transferred pursuant to a Default Decision, ICANN could immediately re-transfer such Domain name at issue back to the LLCs.") (emphasis added). "[D]eclarations on 'information and belief' are entitled to no weight where the declarant lacks personal knowledge." *Maddox v. Ladd*, No. 07-cv-1227, 2011 WL 2946174, at *5 (E.D. Cal. July 21, 2011). Mr. Nelson's declaration

therefore cannot support the Receiver's claims and should be rejected. *See also GN Trade, Inc. v. Siemens*, No. 11-994, 2011 WL 4591080, at *4 (E.D. Cal. Sept. 30, 2011) ("the declaration is basically an 'information and belief' allegation . . . and thus not enough to overcome defendant's unequivocal, sworn denials").

The Receiver also cites the declaration submitted in support of ICANN's reply to the Receiver's response to the Court's order to show cause in support of his belief that ICANN has the ability to re-transfer domain names. But this citation is, at best, in error and, at worst, a deliberate misrepresentation of facts. (Dkt. # 737-1, ¶ 14.) The statements cited by the Receiver only establish that the Registrar Accreditation Agreement that each registrar enters into with ICANN requires the registrar to comply with the UDRP. ICANN's Senior Vice President, Stakeholder Relations declared that "[t]o the extent that a registrar fails to comply with the UDRP, ICANN may deem the registrar in breach of its agreement. But even then, ICANN does not have authority to force the registrar to comply with a UDRP decision." *Id.* The declarant said nothing about ICANN's ability to re-transfer domain names (and that ability does not exist).

1.   **ICANN Cannot Change Registration Information For Domain Names That Are No Longer Registered.**

At the time of this filing, two of the domain names identified in the Receiver's motion (leghanesbali.com and publicstroagejob.com) are not registered to any registered name holder and therefore are not active domain names. (Pritz Decl., ¶¶ 6, 8, Ex A.) There is therefore no domain name for ICANN to "transfer" even if it had such authority or ability (which it does not). (*Id.*)

2.   **Fabulous.com Is Not The Accredited Registrar Of Two Of The Domain Names Identified In The Receiver's Motion.**

The Receiver wrongly states that "Fabulous.com is the registrar of the domain names at issue." (Mot. at 7.) In fact, as confirmed by the Whois database, two domain names

(wetafx.com and publicstorge.com) are registered through accredited registrars other than Fabulous.com (the registrars are Register.com and Network Solutions, respectively). (Pritz Decl., ¶¶ 7, 8, Ex. A.) As explained above, only the current registered name holder and its registrar have the authority and technical ability to effectuate a change in control of domain name registrations. The Receiver must seek relief from these parties, not Fabulous.com or ICANN.

B.   ICANN Does Not Have The Power To Order UDRP Providers To Terminate UDRP Proceedings.

In the Receiver's "supplement" to the second motion to enforce the stay (Dkt. # 756), the Receiver directs the Court to two recent UDRP decisions that terminated two UDRP proceedings. As ICANN does not administer and is not involved in UDRP proceedings, ICANN will not address whether these decisions support or negate the Receiver's position that the default judgments previously entered in UDRP proceedings are void. However, ICANN here clarifies certain misrepresentations made by the Receiver in his supplemental filing.

First, the Receiver's representation that these WIPO panels are "both under ICANN's control" and suggestion that ICANN somehow had a role in terminating these UDRP proceedings is wrong. ICANN does not "control" UDRP proceedings or the panels of arbitrators constituted under the UDRP. (Pritz Decl., ¶ 27.) Nor does ICANN have the authority to instruct or direct a UDRP panel to terminate a UDRP proceeding. (*Id.* at ¶ 28.) The UDRP decisions attached to the Receiver's motion do not even mention ICANN, but instead rely on the panel's own authority and discretion to terminate UDRP proceedings under the UDRP rules. *See, e.g.,* Receiver's Supp. Mot., Ex. A ("In all circumstances, the Panel finds the appropriate course, pursuant to its authority under UDRP Rule 18, to order the termination of the instant UDRP proceeding.").

Second, the Receiver mischaracterizes the UDRP decisions, stating that "both state that the original stay established in the Receivership Order (the "Original Stay") necessitates termination of the UDRP Actions." (Mot. at 1.) In fact, only one UDRP decision even references the stay issued in the Receivership Order. And neither UDRP decision states that the Original Stay "necessitates termination of the UDRP Actions." Instead, the decision(s) to terminate the UDRP proceedings were made in the panel's sole discretion pursuant to the UDRP rules.

III.   CONCLUSION

ICANN lacks the technical capabilities necessary to change the registration information associated with a domain name from one registered name holder to another or even between registrars. ICANN also has no authority to initiate, process or "undo" domain name transfers. For these reasons and those described more fully above, ICANN respectfully requests that the Court deny the Receiver's second motion to enforce the stay.

Dated: January 3, 2012

Respectfully submitted,

JONES DAY

/s/ Jason Cross
———————————————————
Jeffrey A. LeVee
Kate Wallace
555 South Flower Street
Fiftieth Floor
Los Angeles, California 90071
Telephone: (213) 489-3939
Facsimile: (213) 243-2539
Email: jlevee@jonesday.com
         kwallace@jonesday.com

Jason Cross
Texas State Bar No. 24045727
2727 N. Harwood Street
Dallas, TX 75201
Telephone: (214) 220-3939
Facsimile: (214) 969-5100
Email: jcross@jonesday.com

ATTORNEYS FOR NON-PARTY
INTERNET CORPORATION FOR
ASSIGNED NAMES AND NUMBERS

CERTIFICATE OF SERVICE

I hereby certify that on January 3, 2012, I electronically filed the foregoing Non-Party

ICANN's Response To Order To The Receiver's Second Motion And Supplement To Second

Motion To Enforce Stay with the Clerk of the Court for the U.S. District Court, Northern District

of Texas, using the electronic case files system of the court. The electronic case files system sent

a "Notice of Electronic Filing" to the individuals who have consented in writing to accept this

Notice as service of this document by electronic means.

/s/ Jason Cross
———————————————————

LAI-3155933v3

11

EXHIBIT 1

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

NETSPHERE, INC., MANILA INDUSTRIES, INC., AND MUNISH KRISHAN,	§ § § §	
Plaintiffs,	§ § §	
v.	§ §	Civil Action No. 3:09-CV-0988-F
JEFFREY BARON AND ONDOVA LIMITED COMPANY,	§ § § §	
Defendants.	§ § §	

DECLARATION OF KURT PRITZ IN SUPPORT OF NON-PARTY ICANN'S RESPONSE TO THE RECEIVER'S SECOND MOTION AND SUPPLEMENT TO SECOND MOTION TO ENFORCE STAY

I, Kurt Pritz, declare and affirm as follows:

1.   I am Senior Vice President, Stakeholder Relations for the Internet Corporation for Assigned Names and Numbers ("ICANN"), a non-party in this action. I have personal knowledge of the matters set forth herein and am competent to testify to those matters. I make this declaration in support of ICANN's response to the Receiver's second motion and supplement to second motion to enforce the stay entered in this case.

Background On ICANN

2.   ICANN is a not-for-profit public benefit corporation organized under the laws of the State of California. Its principal place of business is in Marina del Rey, which is in Los Angeles County, California.

3.   ICANN does not engage in commercial business. Rather, ICANN administers the Internet's Domain Name System ("DNS") on behalf of the Internet community, pursuant to a series of agreements with the United States Department of Commerce. Background on the

privatization of the Internet is available in a publication published by the Department of Commerce on June 5, 1998 entitled *Management of Internet Names and Addresses* and is available at 63 Fed. Reg. 31741 (1998).

4.   ICANN's role is fulfilled in certain ways. For example, consumers (known as "registered name holders") may obtain the right to use second-level domain names (such as funnygames.com) through companies known as "registrars." ICANN has created principles and rules to determine which entities can serve as registrars; ICANN's accreditation system has produced a highly competitive registrar marketplace, with over 900 accredited registrars. ICANN enters into what is called a "Registrar Accreditation Agreement" or "RAA" with ICANN-accredited registrars. *See* http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm.

Background On The Domain Names Identified In The Receiver's Motion

5.   Based on the Receiver's second motion to enforce the stay in this case, I understand there are 22 domain names that are the subject of the Receiver's second motion. I am also aware of the UDRP default decisions entered by the various UDRP providers concerning the domain names at issue in the Receiver's second motion. In each of the 22 UDRP proceedings relating to these domain names, the UDRP panel ordered that the domain names be transferred to the UDRP complainant.

6.   From the publicly-available Whois information for each of the domain names at issue, I understand that as of today only five domain names (wetafx.com, publicstorge.com, pulicstorage.com, puplicstorage.com, and aplle.com) were transferred by the registrar (Fabulous.com) to a new registered name holder as ordered by the UDRP provider. Fifteen of the domain names have not been transferred and remain with the UDRP respondent; two of the domain names are no longer registered.

7.   In addition, two of the domain names (wetafx.com and publicstorge.com) are registered through ICANN-accredited registrars other than Fabulous.com. The registrars are Register.com and Network Solutions, respectively.

8.   For the Court's convenience, attached hereto as **Exhibit A** is a chart that shows each domain name identified in the Receiver's motion, along with the decision entered by of the UDRP provider, identification of the current registrar, current registered name holder, and the status of the domain name (i.e., whether it has been transferred or not).

Background On Domain Name Registrations

9.   Registering, transferring, or deleting a domain name involves interaction – and a series of contracts – between the registered name holder, the registrar and the registry.[1] In order to register a domain name (and become a registered name holder), one first has to go to an ICANN-accredited registrar or reseller,[2] which will collect information about the registered name holder (such as identifying information on the registered name holder, name server name and address, billing information, and other contact information) as part of the registration process. The registered name holder and registrar then enter into a registration agreement.

10.   For that domain name registration to appear on the Internet, the registrar must then provide information to the registry (such as .COM). The registrar maintains a contract with each registry for which it is authorized to do business, and the transfer of information between the registry and the registrar happens pursuant to this agreement.

11.   ICANN is not involved in either the collection or maintenance of information on individual domain name registrations.

12.   Registrars are responsible for making some of the registered name holder's identifying information publicly available through a Whois service. The Whois database is a standard or protocol that allows users to type in the domain name they wish to query for information on whether a name is registered, and if so, when it was registered and by whom. Internet users around the world can access Whois services to identify information on registered name holders, but do not have the ability to change the Whois information.

---

[1] There is only one registry that maintains the central database for all domain names in a given TLD. By contrast, there are several hundred ICANN-accredited registrars authorized to register domain names in any given TLD for individual registered name holders.

[2] If through a reseller, the reseller acts as an agent for the ICANN-accredited registrar.

13.   ICANN does not maintain or have access (other than what is publicly available to everyone) to a registrar's Whois database. In fact, for ICANN to learn information on individual domain name registrations, ICANN must perform the exact same query through a registrar's Whois service that this Court or anyone else would have to perform.

14.   ICANN does not have the authority, discretion or access to change registration information.

15.   ICANN does not contract with registered name holders and maintains no policy or other initiative governing what steps a registered name holder must undertake to change its registration information to complete a change in control of a domain name to a new registered name holder. That process is dictated by the registration agreement between the registered name holder and the registrar. The steps required to change the control over a domain name to a different registered name holder vary; each registrar maintains its own registration agreement. Generally, however, the registered name holder and the registrar communicate via a secured electronic and automated system. Using automated commands, the current registered name holder must inform the registrar of the change in registration information, and specifically identify of the new registered name holder.

16.   Only the current registered name holder (or registrar, pursuant to a court or UDRP tribunal order) has the discretion and authority to change the registration information and thus effectuate a "transfer" of a domain name to a new registered name holder.

17.   Moreover, only the registered name holder is authorized to inform the registrar of a change in the registration information so that the registrar may accurately populate the Whois database.

18.   ICANN lacks the discretion, authority and technical ability to transfer domains name from one registered name holder to another or force a registered name holder to give up its domain name registrations and transfer them elsewhere.

19.   Nor does ICANN have the authority to transfer individual domain names between registrars.

20.   Verisign operates as the exclusive registry for ".COM" domain names pursuant to a contract with the U.S. Department of Commerce and ICANN, and also enters into standard contracts with various registrars for the .COM TLD. A true and correct copy of the .COM Registry Agreement, Appendix C (which governs the functional specification for the Registry TLD) is attached hereto as **Exhibit B**; *see id.* at § 4.3.10 (Transfer).)

21.   According to the .COM agreement, upon a request from the registered name holder, the new (gaining registrar) will issue a Transfer command to the registry. The current (and potential losing) registrar then has five days to approve or reject the transfer. The registry then processes the transfer. ICANN is not involved in the individual domain name transfer process.

22.   Moreover, only the registry has the technical ability and authority to undo an inter-registrar transfer after a transfer has occurred. The ICANN Policy on Transfer of Registrations between Registrars provides as follows:

> The Registry Operator shall undo a transfer if, after a transfer has occurred, the Registry Operator receives one of the notices as set forth below. In such case, the transfer will be reversed and the domain name reset to its original state. . . . The notice required shall be one of the following:
>
> i.   Agreement of the Registrar of Record and the Gaining Registrar sent by email, letter or fax that the transfer was made by mistake or was otherwise not in accordance with the procedures set forth in this policy;
>
> ii.   The final determination of a dispute resolution body having jurisdiction over the transfer;
>
> iii.   Order of a court having jurisdiction over the transfer.

A true and correct copy of ICANN's Policy on Transfer of Registrations between Registrars is attached hereto as **Exhibit C**.

- 5 -

23.   The only situations where ICANN is involved in a transfer of names is in "bulk" transfer scenarios between two registrars. The bulk transfer provisions will transfer all registrations sponsored by one registrar to another, either due to (i) the acquisition of that registrar or its assets by another registrar, or (ii) lack of accreditation of that registrar.[3] In either case, such "bulk" transfers may be made according to the following procedure:

> "(a)   The gaining Registrar must be accredited by ICANN for the Registry TLD and must have in effect a Registry-Registrar Agreement with Registry Operator for the Registry TLD.
>
> (b)   ICANN must certify in writing to Registry Operator that the transfer would promote the community interest, such as the interest in stability that may be threatened by the actual or imminent business failure of a Registrar."

Ex. C, § B (Policy on Transfer of Registrations between Registrars).

24.   Even in these bulk transfer cases, it is not ICANN that completes the transfer. The transfer can only be completed by the registry. ICANN only provides the process and necessary approvals. ICANN does not have access to the registry database and cannot technically complete the transfer between registrars.

25.   In short, ICANN does not have access to the necessary data in order to change registration information from one registered name holder to another. Nor does ICANN have the authority – by virtue of contract, policy or otherwise – to direct a registered name holder or a registrar to initiate a transfer request, approve a transfer request, or instruct a registry to undo a transfer already effectuated. Each of these matters is specifically governed by contractual relationships between registered name holders and registrars and between registries and registrars.

---

[3] A bulk transfer may also take place when a registrar loses authorization with a registry operator, for example .ORG operated by Public Interest Registry, and all of the registrations in .ORG would be transferred to a registrar authorized in .ORG. These bulk transfers occur pursuant to the Deaccredited Registrar Transition Process (which applies uniformly to all registrars) or the Bulk Transfer After Partial Portfolio Acquisition Process (BTAPPA) that is offered by many registries.

26.   There is no policy or contract or other language anywhere that authorizes ICANN to initiate or process or "undo" transfer requests, either from one registered name holder to another or between registrars, or otherwise direct the registered name holders, registrars or registry to do so.

27.   ICANN does not control or administer or govern proceedings commenced pursuant to the Uniform Domain Name Dispute Resolution Policy ("UDRP") or the panels of arbitrators constituted under the UDRP.

28.   Nor does ICANN have the authority to instruct or direct a UDRP panel to terminate a UDRP proceeding.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

This declaration was signed on January 3, 2012 at Marina del Rey, California.

Kurt Pritz

LAI-3156260v1

- 7 -

Exhibit A

The Domain Names Identified In The Receiver's Second Motion

Domain name	UDRP Decision	Current Registrar	Registered Name Holder	Status
wetafx.com	Transfer	Register.com	Weta Digital	Transferred
publicstorge.com	Transfer	Network Solutions	Public Storage	Transferred
publicstroagejob.com	Transfer	None	None	
pulicstorage.com	Transfer	Fabulous	Public Storage	Transferred
puplicstorage.com	Transfer	Fabulous	Public Storage	Transferred
dailycand.com	Transfer	Fabulous	UDRMC LLC	NOT Transferred
dailycandi.com	Transfer	Fabulous	UDRMC LLC	NOT Transferred
dailycandychicago.com	Transfer	Fabulous	UDRMC LLC	NOT Transferred
dailycandynyc.com	Transfer	Fabulous	UDRMC LLC	NOT Transferred
fanngo.com,	Transfer	Fabulous	UDRMC LLC	NOT Transferred
jandango.com	Transfer	Fabulous	UDRMC LLC	NOT Transferred
jobfandango.com	Transfer	Fabulous	UDRMC LLC	NOT Transferred
aplle.com	Transfer	Fabulous	Kilpatrick Townsend	Transferred
leghanesbali.com	Transfer	None	None	
korresproducts.com	Transfer	Fabulous	TIPA	NOT Transferred
zigris.com	Transfer	Fabulous	TIPA	NOT Transferred
amicains.com	Transfer	Fabulous	UDRMC LLC	NOT Transferred
gravelymowers.com	Transfer	Fabulous	UDRMC LLC	NOT Transferred
judahsmith.com	Transfer	Fabulous	UDRMC LLC	NOT Transferred
americanwoodmark cabinetry.com	Transfer	Fabulous	UDRMC LLC	NOT Transferred
lilycares.com	Transfer	Fabulous	UDRMC LLC	NOT Transferred
itoitravel.com	Transfer	Fabulous	Quantec, LLC/Novo Point, LLC	NOT Transferred

Exhibit B

Revised VeriSign Registry Agreements: Appendix C

Posted: 16 April 2001

ICANN

Functional Specification

This functional specification for the Registry TLD consists of the following elements:

1. Verisign Registry Registrar Protocol Version 1.1.0 (May 2000) (RFC 2832);

2. Supported initial and renewal registration periods;

3. Grace period policy;

4. Nameserver functional specifications;

5. Patch, update, and upgrade policy; and

6. Migration to provreg standard.

In addition, functional specifications are set forth in other parts of the registry agreement and its appendices. For example, specifications for Whois service are set forth in Appendix O.

1. Verisign Registry Registrar Protocol Version 1.1.0 (May 2000)

```
Network Working Group                                    S. Hollenbeck
Request for Comments: 2832                               M. Srivastava
Category: Informational                    Network Solutions, Inc. Registry
                                                             May 2000


              NSI Registry Registrar Protocol (RRP) Version 1.1.0
```

Status of this Memo

    This memo provides information for the Internet community. It does
    not specify an Internet standard of any kind. Distribution of this
    memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2000). All Rights Reserved.

Abstract

    This document describes a protocol for the registration and
    management of second level domain names and associated name servers
    in both generic Top Level Domains (gTLDs) and country code Top Level
    Domains (ccTLDs). This protocol was developed by the Network
    Solutions Registry for use within the Shared Registration System and
    is being published "as-is" to document the protocol implementation
    developed by the Network Solutions, Inc. Registry.

    Internet domain name registration typically involves three entities:
    a registrant who wishes to register a domain name, a registrar who
    provides services to the registrant, and a registry that provides
    services to the registrar while serving as the authoritative
    repository of all functional information required to resolve names
    registered in the registry's TLDs. This document describes a
    protocol for registry-registrar communication only. The protocol
    does not provide any registrant services.

    This document is being discussed on the "rrp" mailing list. To join
    the list, send a message to <majordomo@NSIRegistry.com> with the
    words "subscribe rrp" in the body of the message. There   is also a web
    site for the mailing list archives at

    <http://www.NSIRegistry.net/maillist/rrp>.

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 [MUSTSHOULD]. Further,

Hollenbeck & Srivastava Informational [Page 1]

RFC 2832   NSI Registry Registrar Protocol   May 2000

the term "implicit attribute" refers to an entity attribute whose
value is derived either from another attribute or is dependent on an
established RRP session.

In examples, "C:" represents lines sent by the registrar client and

"S:" represents lines sent by the registry server.
The term "System" is used in this document to collectively refer to
this protocol and the software and hardware that implements the
protocol.

Table of Contents

Hollenbeck & Srivastava   Informational   [Page 2]

RFC 2832   NSI Registry Registrar Protocol   May 2000

1. Introduction

   This document describes the specifications for the NSI Registry
   Registrar Protocol (RRP) version 1.1.0, a TCP-based, 7-bit US-ASCII
   text protocol that permits multiple registrars to provide second
   level Internet domain name registration services in the top level
   domains (TLDs) administered by a TLD registry. RRP is specified using
   Augmented Backus-Nauer Form (ABNF) as described in [ABNF]. Note that
   all ABNF string literals are case-insensitive and the examples
   provided in this document may use mixed case to improve readability.

   RRP was developed by the Network Solutions, Inc. Registry under the
   auspices of the Shared Registration System program. The protocol was
   initially deployed in April 1999 as part of a test bed implementation
   of the Shared Registration System with five registrars. Additional
   registrars began using the protocol in July 1999. The operational
   experiences of both the registry and the registrars identified
   several "lessons learned" which have been documented here as "Known
   Issues".

   This document provides both a description of a protocol and notice of
   learned operational issues that may be useful as first steps in
   developing a standards track domain registration services protocol.
   This document and the protocol it describes may be modified in the
   future based on continued operational experience and community
   reaction.

   The registry stores information about registered domain names and
   associated name servers. A domain name's data includes its name, name
   servers, registrar, registration expiration date, and status. A name
   server's data includes its server name, IP addresses, and registrar.
   A registrar MAY perform the following registration service procedures
   using RRP:

   - Determine if a domain name has been registered.
   - Register a domain name.
   - Renew the registration of a domain name.

- Cancel the registration of a domain name.
- Update the name servers of a domain name.
- Transfer a domain name from another registrar.
- Examine the status of domain names that the registrar has registered.
- Modify the status of domain names that the registrar has registered.
- Determine if a name server has been registered.
- Register a name server.
- Update the IP addresses of a name server.

Hollenbeck & Srivastava   Informational   [Page 3]

RFC 2832   NSI Registry Registrar Protocol   May 2000

- Delete a name server.
- Examine the status of name servers that the registrar has registered.

All RRP commands include features to provide idempotency. That is, the effect of each command is the same if the command is executed once or if the command is executed multiple times. This property is extremely useful in situations when a command is retried due to an error condition that results in a missed command response and a command retry is attempted. Command retries will be caught by the System and rejected with an appropriate error response code. Command parameters that do not provide idempotency will be explained fully as part of the appropriate command description.

2. Security Services

   RRP provides only basic password-based registrar authentication services. Additional security services, including privacy and registrar authentication using public key cryptography, are provided through other System features.

2.1 Connection Security

   Each RRP session MUST be encrypted using the Secure Socket Layer (SSL) v3.0 protocol as specified in [SSL]. SSL provides privacy services that reduce the risk of inadvertent disclosure of registrar-sensitive information, such as the registrar's user identifier and password.

SSL supports mutual authentication of both the client and server using signed digital certificates. The Shared Registration System implemented by the NSI Registry requires digital certificates issued by a commercial certification authority for both registrar clients and public registry RRP servers. Both the registrar client and the public registry RRP server are authenticated when establishing an SSL connection. Further, a registrar MUST be authenticated when establishing an RRP connection via the RRP SESSION command by providing a registrar user identifier and password known only to the registrar and the System. Registrars may change their session password at any time using the RRP SESSION command.

The SSL protocol is not an IETF Standards Track protocol. The Transport Layer Security protocol, specified in [TLS], is a Standards Track protocol that provides SSL v3.0 compatibility features.

Hollenbeck & Srivastava   Informational   [Page 4]

RFC 2832   NSI Registry Registrar Protocol   May 2000

2.2 System Data Security

   The System stores information about the registered domain names and their name servers. Only the current registrar of a registered domain name is authorized to query it, update its name servers, and cancel or renew it. Any registrar can request a transfer of a domain name and its associated name servers from another registrar to the requesting registrar. Only the current sponsoring registrar can receive and explicitly approve or reject domain transfer requests.

   Only a name server's registrar can query, update, and delete it. In general, name servers must be registered through the current registrar of the name server's parent domain name, though an implementation MAY allow use of name servers registered in other TLDs without specifying IP addresses or requiring parent domain registration. Use of ccTLD name servers for a gTLD domain name is one such example.

   Name servers are implicitly transferred by the System when their parent domain name is transferred. In addition, a name server cannot be deleted if it is hosting domain names.

3. Connection Model

IANA has assigned TCP port 648 for RRP use. All RRP implementations
MUST provide RRP services over SSL on TCP port 648. An RRP server
MUST return a banner in the following format to confirm that a
connection has been established:

```
<registry name> RRP Server version <version><crlf>
<server build date and time><crlf>
```

Each line ends with carriage return and line feed characters. The
server build date and time string includes the day, month, date, time
(specified in hours, minutes, and seconds), the local time zone, and
the four-digit year. A dot (".") in column one on a line by itself
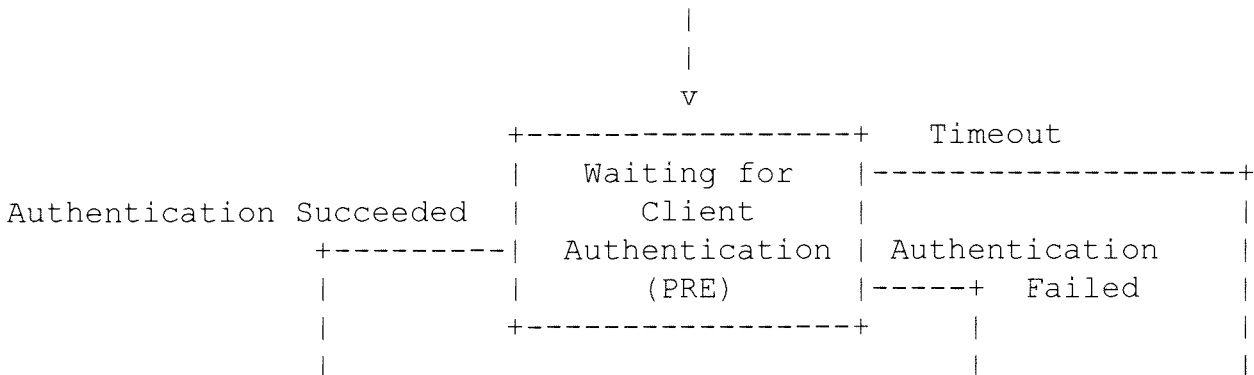marks the end of banner text.

Example

A registrar successfully establishes a connection with the NSI
Registry on TCP port 648:

```
S:NSI RRP Server version 1.1.0
S:Mon Oct 25 20:20:34 EDT 1999
S:.
```

Hollenbeck & Srivastava   Informational   [Page 5]

RFC 2832   NSI Registry Registrar Protocol   May 2000

4. Protocol Description

   A typical RRP session will go through a number of states during its
   lifetime. Figure 1 illustrates the possible states of an RRP server.

   Initially, the server waits for a client connection and
   authentication (PRE). All client connections MUST be authenticated.

```
                                    |
                                    |
                                    v
                          +-----------------+  Timeout
                          |  Waiting for    |-------------------+
  Authentication Succeeded|     Client      |                   |
              +---------|  Authentication | Authentication  |
              |         |     (PRE)       |-----+  Failed    |
              |         +-----------------+     |            |
              |                                 |            |
```

```
              V                                          V            |
  +-----------+      Succeeded      +----------------------+ |
  |Waiting for|<-----------------|      Waiting for     | |
  |  Command  |----------+        |Authentication Retry| |
  |   (WFC)   |  Timeout |        |        (WFR)       | |
  +-----------+          |        +----------------------+ |
      |     ^            |             |           |         |
      |     |            |  Timeout |         | Failed |
  Request V |Response    |             |           |         |
  +-----------+          |             V           V         V
  | Executing |          |        +--------------------+
  |  Command  |  +-------->|      Disconnected    |
  |   (EXE)   |--------------------->|        (DIS)        |
  +-----------+      QUIT      +--------------------+
```
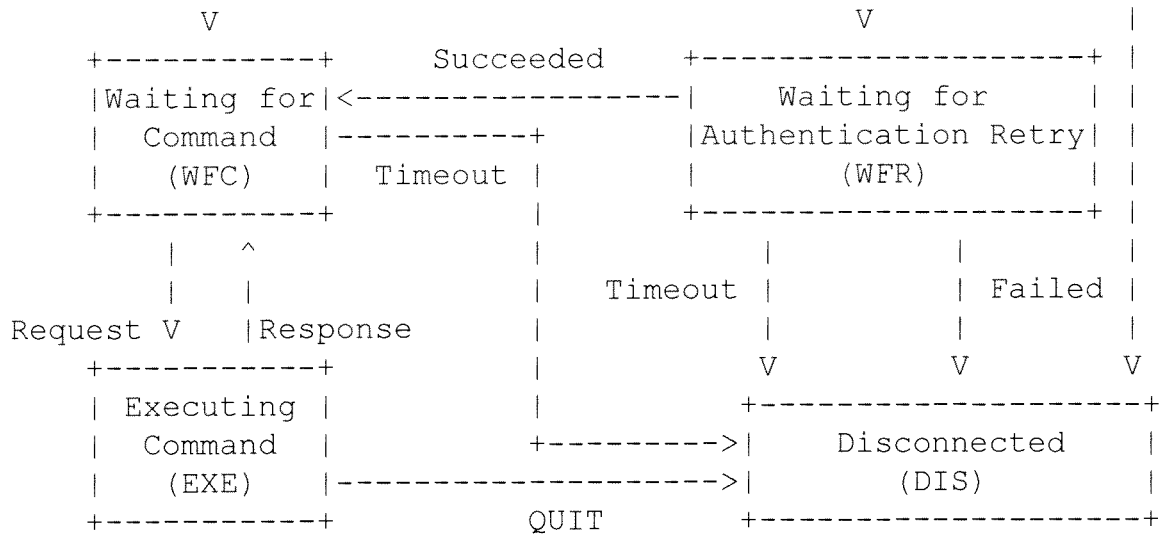
Figure 1: RRP Server Finite State Machine

If the authentication fails, the server gives the client another
chance to identify itself (WFR). If the authentication fails again,
the server disconnects (DIS). Otherwise, the server waits for a
request from the client (WFC). Upon receiving a request, the server
executes it and responds to the client with the result (EXE). The
server then waits again for another request from the client (WFC). If
the client sends a QUIT command, the server ends the session and
disconnects (DIS). To keep its state in sync with that of the server,
the client SHOULD wait for a response from the server before sending
another request on the same connection. The following table
summarizes these states:

Hollenbeck & Srivastava   Informational   [Page 6]

RFC 2832   NSI Registry Registrar Protocol   May 2000

     PRE   Waiting for client connection and authentication
     WFR   Waiting for authentication retry
     WFC   Waiting for a command from an authenticated client
     EXE   Executing a command
     DIS   Disconnected

The WFR and WFC states MAY time out. An implementation SHOULD define
inactivity timeout periods for these states based on System-specific
factors, including (but not limited to) resource availability and
security risk. In the absence of other factors, a default timeout
period of 10 minutes SHOULD be used. The server MAY disconnect if the
server is in one of these states and no message is received from the

client during the timeout period.

4.1 Request Format

An RRP request nominally consists of a command name, an entity block,
command options, and an end-of-command delimiter. Command options and
entity blocks collectively define command parameters and their
specification is order independent; examples provided in this
document specify entity blocks before command options.

    CommandName [EntityBlock] [CommandOptions] EndOfCommand

A command name specifies the type of an RRP request. A command is a
word or abbreviation terminated by a carriage-return linefeed (crlf)
sequence.

    CommandName<crlf>

An entity block specifies the data in an RRP request. It consists of
attribute name-value pairs specifying the entity and all of the
attributes of the entity. Each attribute name-value pair starts with
the attribute name, followed by a colon, the attribute value, and is
finally terminated by a carriage-return linefeed sequence. Entity
blocks are optional for some requests.

    entityName:entityValue<crlf>
    attributeName:attributeValue<crlf>

Command options specify control parameters for an RRP request. A
command option starts with a dash, followed by the option name, a
colon, the option value, and is finally terminated by a carriage-
return linefeed sequence.

    -commandOptionName:commandOptionValue<crlf>

Hollenbeck & Srivastava   Informational   [Page 7]

RFC 2832   NSI Registry Registrar Protocol   May 2000

An EndOfCommand delimiter specifies the end of an RRP request. It
consists of a dot (".") in column one followed by a carriage-return
linefeed sequence.

    .<crlf>

4.2 Response Format

An RRP response starts with a three-digit response code, followed by
a space, an ASCII text description of the response, a carriage-return
linefeed sequence, and zero or more attribute name-value pair lines.
An RRP response is terminated by a dot in column one followed by a
carriage-return linefeed sequence.

```
ResponseCode<space>responseDescription<crlf>
[attributeName:attributeValue<crlf>]
.<crlf>
```

4.3 Protocol Commands

Implementations of RRP commands MUST provide "all or nothing" success
and failure operation. Failed command execution MUST leave the System
in the same state it was in before the command was attempted and
failed.

All RRP commands include features to provide idempotency. Command
features that are not idempotent are explained fully as needed as
part of the appropriate command description.

4.3.1 ADD

This command allows a registrar to register a domain name or a name
server in the System.

4.3.1.1 Registering a Domain Name

The request to register a domain name MUST contain the following
data:

- The "EntityName" parameter set to value "Domain".
- Fully qualified second level domain name in the "DomainName"
  parameter.

Hollenbeck & Srivastava   Informational   [Page 8]

RFC 2832   NSI Registry Registrar Protocol   May 2000

The request to register a domain name MAY contain 1 or more, and a
maximum of 13, fully qualified name servers hosting the domain name
in multiple instances of the "NameServer" parameter. The name servers
MUST have already been registered in the registry. Implementations

MAY allow specification of name servers associated with domains
registered in other TLDs. For example, an implementation MAY allow
use of ccTLD name servers for gTLD domain name registration.

The request to register a domain name MAY contain the initial
registration period in years for the domain being registered in a
single instance of the "Period" parameter. The System MUST provide a
default initial registration period in years if the "Period"
parameter is not provided. The acceptable year values for the
"Period" parameter are implementation specific.

The System will register the domain name to the registrar for the
period specified by the registrar. If the registrar does not specify
a registration period, a System-specified default value MUST be used
for the initial registration period. If the domain name is
successfully registered, the System MUST return the registration
expiration date in the "registration expiration date" attribute in
the response.

Authorized User: All registrars MAY use the ADD command to register
domain names.

Examples

A registrar registers a domain name without specifying name servers:
C:add<crlf>
C:EntityName:Domain<crlf>
C:DomainName:example.com<crlf>
C:-Period:10<crlf>
C:.<crlf>
S:200 Command completed successfully<crlf>
S:registration expiration date:2009-09-22 10:27:00.0<crlf>
S:status:ACTIVE<crlf>
S:.<crlf>

Hollenbeck & Srivastava   Informational   [Page 9]

RFC 2832   NSI Registry Registrar Protocol   May 2000

A registrar registers a domain name using previously-registered name
servers:

C:add<crlf>
C:EntityName:Domain<crlf>
C:DomainName:example2.com<crlf>

```
C:-Period:10<crlf>
C:NameServer:ns1.example.com<crlf>
C:NameServer:ns2.example.com<crlf>
C:.<crlf>
S:200 Command completed successfully<crlf>
S:registration expiration date:2000-09-22 10:27:00.0<crlf>
S:status:ACTIVE<crlf>
S:.<crlf>
```

4.3.1.2 Registering a Name Server

   The request to register a name server MUST contain the following
   data:

   - The "EntityName" parameter set to value "NameServer".
   - Fully qualified server name of the name server in the "NameServer"
     parameter.

   If the name server being registered is the child of a registered
   domain name, the name server registration request MUST include one or
   more, and a maximum of 13, name server IP addresses in multiple
   instances of the "IPAddress" parameter. Name servers associated with
   domains registered in other TLDs SHOULD NOT be specified with IP
   addresses to reduce the possibility of duplicating DNS NS records for
   the name servers in multiple zone files.

   The registrar MUST register the name server in the System before
   using it to host domain names. Further, the name server MUST be
   registered through the same registrar that is the current registrar
   of its parent domain name. The System MAY allow any registrar to use
   the name server to host domain names.

   Authorized User: All registrars MAY use the ADD command to register
   name servers.

Hollenbeck & Srivastava   Informational   [Page 10]

RFC 2832   NSI Registry Registrar Protocol   May 2000

   Examples

   A registrar registers a new name server in an existing domain name:

```
C:add<crlf>
C:EntityName:NameServer<crlf>
```

```
C:NameServer:ns1.example.com<crlf>
C:IPAddress:198.41.1.11<crlf>
C:.<crlf>
S:200 Command completed successfully<crlf>
S:.<crlf>
```

4.3.2 CHECK

This command allows a registrar to determine if a domain name or name server has been registered in the System.

4.3.2.1 Domain Name Check

The request to determine if a domain name is registered MUST contain the following data:
- The "EntityName" parameter set to value "Domain".
  - Fully qualified second level domain name in the "DomainName" parameter.

The System MUST provide a positive or negative response to document domain name availability at the moment the command is executed.

Authorized User: All registrars MAY use the CHECK command to determine if a domain name has been registered or not.

Examples
A registrar checks the availability of a domain name in the System:

```
C:check<crlf>
C:EntityName:Domain<crlf>
C:DomainName:example.com<crlf>
C:.<crlf>
S:211 Domain name not available<crlf>
S:.<crlf>
```

Hollenbeck & Srivastava   Informational   [Page 11]

RFC 2832   NSI Registry Registrar Protocol   May 2000

4.3.2.2 Name Server Check

The request to determine if a name server is registered MUST contain the following data:

- The "EntityName" parameter set to value "NameServer".

- Fully qualified server name in the "NameServer" parameter.

The System MUST provide a positive or negative response to document
name server availability at the moment the command is executed. If
the name server has been registered, the System MUST return the IP
address(es) of the name server.

Authorized User: All registrars MAY use the CHECK command to
determine if a name server has been registered or not.

Examples

A registrar checks the availability of a server name in the System:

```
C:check<crlf>
C:EntityName:Nameserver<crlf>
C:Nameserver:ns1.example.com<crlf>
C:.<crlf>
S:213 Name server not available<crlf>
S:ipAddress:192.10.10.10<crlf>
S:.<crlf>
```

4.3.3 DEL

This command allows a registrar to delete (cancel the registration)
of a domain name or delete a name server.

4.3.3.1 Deleting a Domain Name

The request to cancel the registration of a domain name MUST contain
the following data:

- The "EntityName" parameter set to value "Domain".
- Fully qualified second level domain name in the "DomainName"
  parameter.

A request to delete a domain name SHOULD cause the deletion of all
name servers that are children of the domain name being deleted. The
name servers SHOULD be deleted if they are not actively hosting other
domains. A domain MUST not be deleted if it has child name servers
hosting other domains.

Hollenbeck & Srivastava   Informational   [Page 12]

RFC 2832   NSI Registry Registrar Protocol   May 2000

Authorized User: The current registrar of a domain name MAY use the
DEL command to delete a domain name from the System.

Examples

A registrar deletes a domain name, implicitly deleting all name
servers registered in the domain:

C:del<crlf>
C:EntityName:Domain<crlf>
C:DomainName:example.com<crlf>
C:.<crlf>
S:200 Command completed successfully<crlf>
S:.<crlf>

4.3.3.2 Deleting a Name Server

The request to delete a name server MUST contain the following data:

- The "EntityName" parameter set to value "NameServer".
- Fully qualified name of the name server in the "NameServer"
  parameter.

A name server MUST not be deleted if it is hosting domains. Deleting
such domains or name servers is prohibited because their deletion
WILL result in orphaning the hosted domains.

Authorized User: The current registrar of a name server MAY use the
DEL command to delete a name server from the System.

Examples

A registrar deletes a name server that is not hosting domains:

C:del<crlf>
C:EntityName:NameServer<crlf>
C:NameServer:ns1.registrarA.com<crlf>
C:.<crlf>
S:200 Command completed successfully<crlf>
S:.<crlf>

Hollenbeck & Srivastava   Informational   [Page 13]

RFC 2832   NSI Registry Registrar Protocol   May 2000

A registrar tries to delete a name server that is hosting domains:

```
C:del<crlf>
C:EntityName:NameServer<crlf>
C:NameServer:ns1.registrarA.com<crlf>
C:.<crlf>
S:532 Domain names linked with name server<crlf>
S:.<crlf>
```

4.3.4 DESCRIBE

This command allows a registrar to obtain general information about an RRP implementation. The command MAY contain the following parameters:

- The "Target" parameter set to value "Protocol".

The implementation MUST return the protocol version number whether or not the request contains the "Target" parameter.

Authorized User: All registrars MAY use the DESCRIBE command.

Examples

A registrar obtains general information about an RRP implementation:

```
C:describe<crlf>
C:-Target:Protocol<crlf>
C:.<crlf>
S:200 Command completed successfully<crlf>
S:Protocol:RRP 1.1.0<crlf>
S:.<crlf>
```

4.3.5 MOD

This command allows a registrar to update a registered domain name or a name server. The command allows the following operations on an attribute value for both single-valued and multi-valued attributes:

- Add an attribute value. The value to be added MUST be unique among the values of the attribute. For a single-valued attribute, it replaces the current value.
- Remove an attribute value. The value to be removed MUST exist. Further, an attribute value cannot be removed if it is the only value of a required attribute.

Attribute values to be removed are identified by tagging with an "="
suffix.

Hollenbeck & Srivastava   Informational   [Page 14]

RFC 2832   NSI Registry Registrar Protocol   May 2000

4.3.5.1 Domain Modification

   The request to modify a registered domain name MUST contain the
   following data:

   - The "EntityName" parameter set to value "Domain".
   - Fully qualified second level domain name in the "DomainName"
     parameter.

   The registrar can perform the following update operations on the
   domain name:

   - Update the name servers of the domain name by setting one or more
     instances of the "NameServer" parameter.
   - Update the status of the domain name by setting one or more
     instances of the "Status" parameter. Valid values for the "Status"
     parameter are defined in Section 6.

   Authorized User: The current registrar of a domain name MAY use the
   MOD command to modify the attributes of a domain name.

   Examples

   A registrar removes one name server (ns1) from a domain and adds a
   new name server (ns3) to the same domain:

   C:mod<crlf>
   C:EntityName:Domain<crlf>
   C:DomainName:example.com<crlf>
   C:NameServer:ns3.registrarA.com<crlf>
   C:NameServer:ns1.registrarA.com=<crlf>
   C:.<crlf>
   S:200 Command completed successfully<crlf>
   S:.<crlf>

4.3.5.2 Name Server Modification

   The request to update a name server MUST contain the following data:

- The "EntityName" parameter set to value "NameServer".
- Fully qualified server name of the name server in the "NameServer" parameter.

Hollenbeck & Srivastava   Informational   [Page 15]

RFC 2832   NSI Registry Registrar Protocol   May 2000

The registrar can perform the following update operations on the name server:

- Update the "NameServer" attribute of the name server. This allows a registrar to change the name of a name server while preserving all existing associations.
- Update the IP addresses of the name server by setting one or more instances of the "IPAddress" parameter.

Authorized User: The current registrar of a name server MAY use the MOD command to modify the attributes of a domain name.

Examples

A registrar changes the name and IP address of a name server:

```
C:mod<crlf>
C:EntityName:NameServer<crlf>
C:NameServer:ns1.registrarA.com<crlf>
C:NewNameServer:ns2.registrarA.com<crlf>
C:IPAddress:198.42.1.11<crlf>
C:IPAddress:198.41.1.11=<crlf>
C:.<crlf>
S:200 Command completed successfully<crlf>
S:.<crlf>
```

4.3.6 QUIT

This command allows a registrar to close an RRP connection. A response MUST be sent before closing the connection.

Authorized User: All registrars MAY use the QUIT command.

Examples

A registrar ends an RRP session and closes an existing connection:

```
C:quit<crlf>
C:.<crlf>
S:220 Command completed successfully. Server closing connection<crlf>
S:.<crlf>
```

Hollenbeck & Srivastava   Informational   [Page 16]

RFC 2832   NSI Registry Registrar Protocol   May 2000

4.3.7 RENEW

   This command allows a registrar to renew a domain name in the System.
   The request to renew a domain name MUST contain the following data:

   - The "EntityName" parameter set to value "Domain".
   - Fully qualified second level domain name in the "DomainName"
     parameter.

   The request to renew a domain name MAY contain the renewal period in
   years for the domain being renewed in a single instance of a "Period"
   parameter and a single instance of a "CurrentExpirationYear"
   parameter. These parameters MUST appear together if either is
   specified, though the order in which the parameters appear is
   insignificant. The "Period" parameter identifies the number of years
   to be added to the registration. The "CurrentExpirationYear"
   parameter identifies the current expiration year, and is required to
   ensure that repeated attempts to retry this command do not result in
   multiple successful renewals. The System MUST provide a default
   number of renewal years if the "Period" and "CurrentExpirationYear"
   parameters are not provided. Repeated use of this command without the
   "Period" and "CurrentExpirationYear" parameters may result in
   repeated successful renewals since idempotency is not provided when
   these parameters are not used. The acceptable year values for the
   "Period" parameter are implementation specific subject to syntax
   restrictions.

   The System renews the domain name for a period specified by the
   registrar. If the domain name renewal is completed successfully, the
   System MUST return the new registration expiration date in the
   "RegistrationExpirationDate" attribute in the response.

   Authorized User: The current registrar of a domain name MAY use the
   RENEW command.

Examples

A registrar renews a domain name using a specified renewal period:

```
C:renew<crlf>
C:EntityName:Domain<crlf>
C:DomainName:example.com<crlf>
C:-Period:9<crlf>
C:-CurrentExpirationYear:2001<crlf>
C:.<crlf>
S:200 Command completed successfully<crlf>
S:registration expiration date:2010-09-22 10:27:00.0<crlf>
S:.<crlf>
```

Hollenbeck & Srivastava   Informational   [Page 17]

RFC 2832   NSI Registry Registrar Protocol   May 2000

4.3.8 SESSION

   This command allows a registrar to establish an RRP session. A
   registrar can also use this command to change their password. The
   request to establish an RRP connection MUST contain the following
   command parameters:

   - The "Id" parameter set to the registrar's System user ID.
   - The "Password" parameter set to the registrar's current System
     password.

   The request to establish an RRP session MAY contain a new password
   for the registrar in a single instance of the "NewPassword"
   parameter.

   The registrar MUST send this command to the System before any other
   command. If the command fails due to invalid information (such as an
   invalid registrar ID or password), the registrar can resend this
   request with corrected information. If the command fails a second
   time, the System SHOULD close the connection.

   Authorized User: All registrars MAY use the SESSION command.

   Examples

   A registrar establishes an RRP session:

```
C:session<crlf>
C:-Id:registrarA<crlf>
C:-Password:i-am-registrarA<crlf>
C:.<crlf>
S:200 Command completed successfully<crlf>
S:.<crlf>
```

4.3.9 STATUS

This command allows a registrar to determine the current status of a
domain name or name server.

4.3.9.1 Domain Status

The request to query a domain name MUST contain the following data:

- The "EntityName" parameter set to value "Domain".
- Fully qualified second level domain name in the "DomainName"
  parameter.

Hollenbeck & Srivastava   Informational   [Page 18]

RFC 2832   NSI Registry Registrar Protocol   May 2000

The response from the System MAY contain the following data:

- Fully qualified server names of name servers hosting the domain
  name in multiple instances of the "nameserver" attribute.
- Registration expiration date in the "registration expiration date"
  attribute.
- ID of the current registrar of the domain name in the "registrar"
  attribute.
- Date the domain name was transferred by the current registrar in
  the "registrar transfer date" attribute.
- Current statuses of the domain name in multiple instances of the
  "status" attribute.
- Date the domain name was originally registered in the "created
  date" attribute.
- ID of the registrar that originally registered the domain name in
  the "created by" attribute.
- Date the domain name was last updated in the "updated date"
  attribute.
- ID of the entity (either a registrar or the registry) that last
  updated the domain name in the "updated by" attribute.

```
Authorized User: The current registrar of a domain name MAY use the
STATUS command to view current domain name attributes.

Examples

The current registrar of a domain name queries the domain name:

C:status<crlf>
C:EntityName:Domain<crlf>
C:DomainName:example.com<crlf>
C:.<crlf>
S:200 Command completed successfully<crlf>
S:nameserver:ns2.registrarA.com<crlf>
S:nameserver:ns3.registrarA.com<crlf>
S:registration expiration date:2010-09-22 10:27:00.0<crlf>
S:registrar:registrarA<crlf>
S:registrar transfer date:1999-09-22 10:27:00.0<crlf>
S:status:ACTIVE<crlf>
S:created date:1998-09-22 10:27:00.0<crlf>
S:created by:registrarA<crlf>
S:updated date:2002-09-22 10:27:00.0<crlf>
S:updated by:registrarA<crlf>
S:.<crlf>
```

Hollenbeck & Srivastava   Informational   [Page 19]

RFC 2832   NSI Registry Registrar Protocol   May 2000

   A registrar queries a domain name currently registered by another
   registrar:

```
   C:status<crlf>
   C:EntityName:Domain<crlf>
   C:DomainName:example.com<crlf>
   C:.<crlf>
   S:531 Authorization failed<crlf>
   S:.<crlf>
```

4.3.9.2 Name Server Status

   The request to query a name server MUST contain the following data:

   - The "EntityName" parameter set to value "NameServer".
   - Fully qualified name of the name server in the "NameServer"

```
           parameter.

           The response from the System MAY contain the following data:

           -  Fully qualified name of the name server in the "nameserver"
              attribute.
           -  IP addresses of the name server in multiple instances of the
              "ipaddress" attribute.
           -  ID of the current registrar of the name server in the "registrar"
              attribute.
           -  Date the name server was transferred by the current registrar in
              the "registrar transfer date" attribute.
           -  Date the name server was registered in the "created date"
              attribute.
           -  ID of the entity that registered the name server in the "created
              by" attribute.
           -  Date the name server was last updated in the "updated date"
              attribute.
           -  ID of the entity that last updated the name server in the "updated
              by" attribute.

           Authorized User: The current registrar of a name server MAY use the
           STATUS command to view current domain name attributes.

           Examples

           The current registrar of a name server queries the name server:

           C:status<crlf>
           C:EntityName:NameServer<crlf>
           C:NameServer:ns1.registrarA.com<crlf>
           C:.<crlf>
```

Hollenbeck & Srivastava   Informational   [Page 20]

RFC 2832   NSI Registry Registrar Protocol   May 2000

```
        S:200 Command completed successfully<crlf>
        S:ipaddress:198.42.1.11<crlf>
        S:registrar:registrarA<crlf>
        S:registrar transfer date:1999-09-22 10:27:00.0<crlf>
        S:CreatedDate:1998-09-22 10:27:00.0<crlf>
        S:CreatedBy:registrarA<crlf>
        S:UpdatedDate:2002-09-22 10:27:00.0<crlf>
        S:UpdatedBy:registrarA<crlf>
```

```
S:.<crlf>


A registrar queries a name server that was registered by another
registrar:

C:status<crlf>
C:EntityName:NameServer<crlf>
C:NameServer:ns1.registrarA.com<crlf>
C:.<crlf>
S:531 Authorization failed<crlf>
S:.<crlf>
```

4.3.10 TRANSFER

This command allows a registrar to request transfer of domain name
sponsorship from a second registrar and to approve or reject transfer
requests initiated by other registrars. The request to transfer a
domain name MUST contain the following data:

- The "EntityName" parameter set to value "Domain".
- Fully qualified second level domain name in the "DomainName"
  parameter.

The identity of the requesting registrar is derived from the current
active session. The identity of the current sponsoring registrar (the
registrar who must approve or reject the transfer request) is known
by the registry and does not need to be known by the requesting
registrar in advance of issuing the transfer request.

The System MUST notify the potential losing registrar when a domain
transfer request has been received using an out-of-band transport
mechanism such as electronic mail and/or transaction reporting. The
losing registrar SHOULD then explicitly approve or reject the
transfer. A request to approve or reject a transfer request MUST
contain a single instance of the "Approve" parameter with a value of
"Yes" to approve the transfer or a value of "No" to reject the
transfer. A server implementation MAY provide a default approval or
rejection action to be taken if the losing registrar does not
explicitly approve or reject the transfer request within a fixed
amount of time. The criteria used by registrars to approve or deny

Hollenbeck & Srivastava   Informational   [Page 21]

RFC 2832   NSI Registry Registrar Protocol   May 2000

requested transfers are typically based on business policies that are
beyond the scope of this document.

Approval of a transfer by the current sponsoring registrar results in
a change of sponsorship to the original requesting registrar.
Approval attempts by any other registrar MUST result in explicit
failure of the attempted approval. Rejection of the transfer by the
current sponsoring registrar results in an end to the transfer
request with no change in sponsorship. Rejection attempts by any
other registrar MUST result in explicit failure of the attempted
rejection.

Name servers MUST be implicitly transferred when their parent domain
name is transferred.

Authorized User: All registrars MAY use the TRANSFER command to
request transfer of registration service authority to the requesting
registrar. Only the current sponsoring registrar of a domain name may
explicitly approve or reject a requested transfer. The registry MAY
implicitly approve or reject requested transfers after a fixed amount
of time.

Examples

A registrar requests transfer of a domain name from another
registrar:

C:transfer<crlf>
C:EntityName:Domain<crlf>
C:DomainName:example.com<crlf>
C:.<crlf>
S:200 Command completed successfully<crlf>
S:.<crlf>

The original registrar approves the transfer request:

C:transfer<crlf>
C:-Approve:Yes<crlf>
C:EntityName:Domain<crlf>
C:DomainName:example.com<crlf>
C:.<crlf>
S:200 Command completed successfully<crlf>
S:.<crlf>

Hollenbeck & Srivastava   Informational   [Page 22]

RFC 2832   NSI Registry Registrar Protocol   May 2000

5. Response Codes

   RRP commands may return a variety of response codes to signify normal
   completion or error conditions. This section documents all of the
   defined RRP response codes.

5.1 Response Code Summary

   200 Command completed successfully
   This is the normal response for successful completion of most RRP
   commands.

   210 Domain name available
   This is the normal response for successful completion of an RRP CHECK
   command for a domain name that is not currently registered.

   211 Domain name not available
   This is the normal response for successful completion of an RRP CHECK
   command for a domain name that is currently registered.

   212 Name server available
   This is the normal response for successful completion of an RRP CHECK
   command for a name server that is not currently registered.

   213 Name server not available
   This is the normal response for successful completion of an RRP CHECK
   command for a name server that is currently registered.

   220 Command completed successfully. Server closing connection This is
   the normal response for successful completion of an RRP QUIT command.
   It may also be returned by other RRP commands if a transient
   situation is noted that requires closing the connection after
   successfully completing the RRP command.

   420 Command failed due to server error. Server closing connection A
   transient server error has caused RRP command failure and session
   termination. A new session must be established before continued
   processing can be attempted.

   421 Command failed due to server error. Client should try again A
   transient server error has caused RRP command failure. A subsequent
   retry may produce successful results.

   500 Invalid command name

A client-specified RRP command name was not recognized as a valid RRP command name.

Hollenbeck & Srivastava   Informational   [Page 23]

RFC 2832   NSI Registry Registrar Protocol   May 2000

   501 Invalid command option
   A client-specified RRP command parameter was not recognized as a
   valid RRP command parameter.

   502 Invalid entity value
   The "value" of an entity name-value pair is invalid. Command blocks
   that require an "EntityName" parameter also require a value that
   specifies the entity name, and the provided value is invalid.

   503 Invalid attribute name
   A client-specified RRP command parameter was not recognized as a
   valid RRP command parameter.

   504 Missing required attribute
   A parameter required to execute the RRP command was not provided by
   the client. The command should be retried with all required
   parameters specified.

   505 Invalid attribute value syntax
   A supplied parameter value is syntactically incorrect. For example, a
   year value digit such as "5" may be required but the client provided
   a string of characters such as "five".

   506 Invalid option value
   A client-specified value for an RRP command parameter is out-of-
   bounds or otherwise not within acceptable System limits.

   507 Invalid command format
   The specified command does not resemble a well-formed RRP command.
   The command should be retried using the proper command structure and
   syntax.

   508 Missing required entity
   An entity required for command completion was not provided by the
   client. For example, the CHECK command requires specification of
   either a "Domain" entity or a "Nameserver" entity.

   509 Missing command option

A command parameter that isn't really optional (such as the registrar
ID in a SESSION command) was not provided by the client. The command
should be retried with all needed parameters.

520 Server closing connection. Client should try opening new
connection; <why>
A timeout event has been detected, and the client's session is being
ended. The System SHOULD define timeout periods to begin a client

Hollenbeck & Srivastava   Informational   [Page 24]

RFC 2832   NSI Registry Registrar Protocol   May 2000

command, complete a client command, and for the duration of an open
session. The reason for the timeout MUST be provided at the end of
the response code string.

521 Too many sessions open. Server closing connection
A System-defined limit on the number of open connections has been
exceeded, and it is impossible to establish a new session at the
moment. It may be possible to establish a session by waiting for a
few moments or by closing existing unused sessions.

530 Authentication failed
The client-supplied registrar identifier or password was not
recognized by the System. A subsequent retry with valid values may
produce successful results. Repeated authorization failures MAY
result in termination of the TCP connection.

531 Authorization failed
Registrars may not view or alter data associated with either the
registry or another registrar. This response code is typically
returned when a registrar attempts to view or modify data belonging
to either the registry or another registrar. A typical situation
includes doing a STATUS command for a domain registered to another
registrar.

532 Domain names linked with name server
The name server is hosting active domains. This error occurs when a
registrar is trying to delete a server that is the name server for
active domains. The registry MUST not allow the registrar to delete
this server. All of the domain names using this server MUST be
modified to use a different name server before the name server can be
deleted.

533 Domain name has active name servers
The domain name has active name servers. The registrar is trying to
delete a domain name that is a parent domain of an active name
server, i.e., a server that is hosting active domains. All of the
name servers within the domain MUST be removed from service before
the domain can be deleted.

534 Domain name has not been flagged for transfer
The registrar is trying to approve or reject a domain name transfer
for a domain name that is not pending transfer.

535 Restricted IP address
IANA identifies certain IP address ranges that are not valid for
normal use. The registrar is trying to use an IP address that is in
a restricted IP address range as identified by IANA.

Hollenbeck & Srivastava   Informational   [Page 25]

RFC 2832   NSI Registry Registrar Protocol   May 2000

536 Domain already flagged for transfer
The registrar tried to perform a transfer command for a domain name
that is awaiting approval of an earlier transfer request.

540 Attribute value is not unique
A supplied attribute value is not unique. This occurs when the
registrar is adding a domain name that already exists in the
registry, a server that already exists in the registry, or an IP
address that is already being used by another server in the registry.
Another possibility occurs when performing domain modifications and
the registrar is adding a server that is already in the list of
servers for the domain name or setting a domain name to a status to
which it is already set. The RRP STATUS command MAY be used to
determine current domain name status before attempting to change the
status. When modifying or adding a name server, the IP address of the
name server might not be unique. The registry MUST not allow IP
addresses to be used by more than one server.

541 Invalid attribute value
A supplied parameter value is invalid. Examples of invalid attribute
values include an invalid IP address, an invalid domain name, an
invalid server name, or an invalid renewal period.

542 Invalid old value for an attribute
A current attribute value to be modified is invalid. The registrar is
trying to modify an attribute of a server or a domain name that does
not exist in the registry.

543 Final or implicit attribute cannot be updated
The registrar is attempting to modify an attribute that is only
modifiable by the registry. Registrars can not modify final or
implicit attribute values.

544 Entity on hold
The attempted operation was rejected because the entity is on HOLD
status. If the HOLD status was set by the registrar, the status can
be changed using the MOD command and the requested command can be
retried. If the HOLD status was set by the registry, the registrar
must contact the registry to change the status before the command can
be successful.

545 Entity reference not found
A required entity reference was not found. This occurs when the
registrar tries to add a new name server and the parent domain of the
name server does not exist in the registry. It also occurs when the
user is trying to add a new name server to a domain name when the
name server does not exist in the registry.

Hollenbeck & Srivastava   Informational   [Page 26]

RFC 2832   NSI Registry Registrar Protocol   May 2000

546 Credit limit exceeded
The registrar's credit limit has been exceeded. This is an
implementation specific error that occurs when a potentially billable
operation, such as adding a domain name, renewing a domain name, or
transferring a domain name, is attempted and the registrar does not
have sufficient financial standing with the registry to complete the
operation.

547 Invalid command sequence
RRP commands are issued using a well-formed syntax that requires
entry of command structures in particular sequences. This response
code indicates that an ill-formed command was received and rejected.

548 Domain is not up for renewal
A RENEW command was attempted during a period in which the domain can
not be renewed. Implementations MAY limit renewal periods to
particular time frames, such as within 90 days of the domain's
expiration. This response indicates that the RENEW command was
received outside of the System-defined domain renewal period.

549 Command failed
A System error prevented successful completion of the requested RRP
command. Retrying the command might produce success, but a repeated
failure indicates a System error condition.

550 Parent domain not registered
The parent domain of a name server being registered is not
registered. This occurs when the registrar tries to add a new name
server and the parent domain for the server does not exist in the
registry.

551 Parent domain status does not allow for operation
The status of the parent domain does not allow the requested
operation. This occurs when a registrar tries to modify a server
whose parent domain is flagged as LOCK or HOLD in the registry.

552 Domain status does not allow for operation
The status of the domain does not allow the requested operation. This
occurs when a registrar tries to modify or delete a domain that is
flagged as LOCK or HOLD in the registry.

553 Operation not allowed. Domain pending transfer
The status of the domain does not allow the requested operation. The
registrar is attempting to delete a domain that is pending approval
or denial of a transfer request.

Hollenbeck & Srivastava   Informational   [Page 27]

RFC 2832   NSI Registry Registrar Protocol   May 2000

554 Domain already registered
A registrar tried to register a domain name that has already been
registered by the same registrar.

555 Domain already renewed
A registrar tried to renew a domain using the same parameters as
specified for an earlier, successful renewal. This will commonly
occur when executing the same RENEW command more than once.

556 Maximum registration period exceeded
A registrar tried to renew a domain registration, and the resulting
new registration period exceeds the System-defined maximum
registration period. If there is renewal time available with the
System-defined maximum registration period it may be possible to
retry the RENEW command with specified renewal period parameters.

5.2 Command-Response Correspondence

The session between the client and the server is intended to be an
alternating dialogue. Each command issued by a client MUST be acted
upon by the server, which MUST return a response code to document the
success or failure of command execution. "Success" means that the
command completed normal execution without error. "Failure" means
that the System did not complete the command as requested. Failure
may be due to either syntax, semantic, data, or System errors.

A complete list of response codes for each RRP command is listed
below.

Command: ADD
Success: 200, 220
Failure: 420, 421, 500, 502, 503, 504, 505, 507, 508, 520, 531, 535,
540, 541, 545, 546, 547, 549, 550, 554

Command: CHECK
Success: 210, 211, 212, 213
Failure: 220, 420, 421, 500, 502, 503, 504, 505, 507, 508, 520, 541,
547, 549

Command: DEL
Success: 200, 220
Failure: 420, 421, 500, 502, 503, 504, 505, 507, 508, 520, 531, 532,
533, 541, 544, 545, 547, 549, 551, 552, 553

Command: DESCRIBE
Success: 200, 220
Failure: 420, 421, 500, 501, 506, 507, 509, 520, 547, 549

Hollenbeck & Srivastava   Informational   [Page 28]

RFC 2832   NSI Registry Registrar Protocol   May 2000

Command: MOD
Success: 200, 220
Failure: 420, 421, 500, 502, 503, 504, 505, 507, 508, 520, 531, 535,
540, 541, 542, 543, 544, 545, 547, 549, 550, 551, 552, 553

Command: QUIT
Success: 220
Failure: 420, 421, 500, 507, 520, 547, 549

```
Command: RENEW
Success: 200, 220
Failure: 420, 421, 500, 502, 503, 504, 505, 507, 508, 520, 531, 541,
545, 546, 547, 548, 549, 552, 553, 555, 556

Command: SESSION
Success: 200, 220
Failure: 420, 421, 500, 501, 506, 507, 508, 509, 520, 521, 530, 531,
547, 549

Command: STATUS
Success: 200, 220
Failure: 420, 421, 500, 501, 502, 503, 504, 505, 506, 507, 508, 520,
531, 541, 545, 547, 549

Command: TRANSFER
Success: 200, 220
Failure: 420, 421, 500, 501, 502, 503, 504, 505, 506, 507, 508, 520,
531, 534, 536, 541, 544, 545, 546, 547, 549, 552, 553
```

6. Domain Status Codes

   The status of a domain can be viewed using the RRP STATUS command and
   modified using the RRP MOD command. Both the registry and the
   sponsoring registrar MAY view and change the status of a domain. The
   criteria for status changes are highly dependent on registry and
   registrar business models and are thus beyond the scope of this
   specification.

   The domain's status SHOULD have a direct bearing on whether or not
   the domain appears in the appropriate TLD zone file and whether or
   not the domain can be modified. A domain can have more than one
   assigned status, e.g., REGISTRAR-HOLD and REGISTRAR-LOCK. If a domain
   is in ACTIVE status, then the domain name can only be in this status.
   When a registrar sets a domain name to REGISTRAR-LOCK, the registry
   MUST automatically remove the ACTIVE status. When the registrar
   removes the REGISTRAR-LOCK and other domain statuses, the registry
   MUST automatically set the domain name status to ACTIVE.

Hollenbeck & Srivastava   Informational   [Page 29]

RFC 2832   NSI Registry Registrar Protocol   May 2000

6.1 Domain Status Code Description

ACTIVE: This is the default status of a domain at registration time. The registry sets the domain to this status. The domain is modifiable by the registrar. The domain can be renewed. The domain SHALL be included in the zone file when in this status if the domain has at least one associated name server.

REGISTRY-LOCK: The registry sets the domain to this status. The domain cannot be modified or deleted by the registrar. The registry MUST remove the REGISTRY-LOCK status for the registrar to modify the domain. The domain can be renewed. The domain SHALL be included in the zone file when in this status if the domain has at least one associated name server.

REGISTRY-HOLD: The registry sets the domain to this status. The domain cannot be modified or deleted by the registrar. The registry MUST remove the REGISTRY-HOLD status for the registrar to modify the domain. The domain can be renewed. The domain SHALL NOT be included in the zone file when in this status.

REGISTRAR-HOLD: The registrar of the domain sets the domain to this status. The domain can not be modified or deleted when in this status. The registrar MUST remove REGISTRAR-HOLD status to modify the domain. The domain can be renewed. The domain SHALL NOT be included in the zone file when in this status.

REGISTRAR-LOCK: The registrar of the domain sets the domain to this status. The domain cannot be modified or deleted when in this status. The registrar MUST remove REGISTRAR-LOCK status to modify the domain. The domain can be renewed. The domain SHALL be included in the zone file when in this status.

REGISTRY-DELETE-NOTIFY: A domain is set on this status if it has expired and has child name servers that are hosting other domains. Only the registry may set this status. The domain SHALL be included in the zone file when in this status if the domain has at least one associated name server.

7. Formal Syntax

The following syntax specification uses the augmented Backus-Naur Form (BNF) as described in [ABNF].

; ABNF specification for Registry Registrar Protocol (RRP) v1.1.0
; Note that character string literals are case insensitive.

Hollenbeck & Srivastava   Informational   [Page 30]

RFC 2832   NSI Registry Registrar Protocol   May 2000

```
; Lexical tokens
space = %x20 ; " "
dot = %x2E ; "."
dash = %x2D ; "-"
underscore = %x5F ; "_"
colon = %x3A ; ":"
cr = %x0D ; ASCII carriage return
lf = %x0A ; ASCII linefeed
crlf = cr lf
alpha = %x41-5A / %x61-7A ; A-Z / a-z
digit = %x30-39 ; 0-9
dns-char = alpha / digit / dash
id-char = alpha / digit / underscore / dash
id-prefix = alpha / digit
id-word = id-prefix *id-char
printable-char = %x20-7E ; ASCII " " - "~"

; Start of basic grammar.
year = 4digit
month = 2digit
day = 2digit
ymd = year dash month dash day
hour = 2digit
minute = 2digit
second = 2digit
split-second = 1digit
hms = hour colon minute colon second dot split-second
time-stamp = ymd space hms
ip-address = 1*3digit dot 1*3digit dot 1*3digit dot 1*3digit
password = 4*16printable-char
option-name = 1*128id-word
option-tag = dash option-name
option-value = 1*128id-word
attribute-name = 1*128id-word
attribute-value = 1*128printable-char
attribute-line = attribute-name colon attribute-value crlf
response = 3digit space 1*printable-char crlf
version-number = "RRP" space 1*digit dot 1*digit dot 1*digit
label = id-prefix [*61dns-char id-prefix]
sldn = label dot label
servername = *(label dot) sldn
period = %x31-39 / (%x31-39 %x30-39) ; "1" - "9" or "10" - "99"
```

```
period-option = dash "Period" colon period crlf
yesno = "Yes" / "No"
domainstatus = "Active" / "Registry-Lock" / "Registry-Hold" /
               "Registrar-Lock" / "Registrar-Hold" /
               "Registry-Delete-Notify"
```

Hollenbeck & Srivastava   Informational   [Page 31]

RFC 2832   NSI Registry Registrar Protocol   May 2000

```
; RRP commands and responses.
rrp = add / check / delete / describe / mod / quit / renew /
      session / status / transfer

add = add-request add-response
check = check-request check-response
delete = del-request del-response
describe = describe-request describe-response
mod = mod-request mod-response
quit = quit-request quit-response
renew = renew-request renew-response
session = session-request session-response
status = status-request status-response
transfer = transfer-request transfer-response

; ADD command.
add-request = add-domain-request / add-nameserver-request
add-response = add-domain-response / add-nameserver-response
add-domain-request = "add" crlf
 "EntityName" colon "Domain" crlf
 "DomainName" colon sldn crlf
 [period-option]
 0*13("NameServer" colon servername crlf)
 dot crlf
add-nameserver-request = "add" crlf
 "EntityName" colon "NameServer" crlf
 "NameServer" colon servername crlf
 1*("IPAddress" colon ip-address crlf)
 dot crlf
add-domain-response = response
 "RegistrationExpirationDate" colon time-stamp crlf
 "status" colon domainstatus crlf
 dot crlf
add-nameserver-response = response
 dot crlf
```

```
; CHECK command.
check-request = check-domain-request / check-nameserver-request
check-response = check-domain-response / check-nameserver-response
check-domain-request = "check" crlf
 "EntityName" colon "Domain" crlf
 "DomainName" colon sldn crlf
 dot crlf
check-nameserver-request = "check" crlf
 "EntityName" colon "NameServer" crlf
 "NameServer" colon servername crlf
 dot crlf
check-domain-response = response
```

Hollenbeck & Srivastava   Informational   [Page 32]

RFC 2832   NSI Registry Registrar Protocol   May 2000

```
 dot crlf
check-nameserver-response = available-check-nameserver-response /
                            notavailable-check-nameserver-response
available-check-nameserver-response = response
 dot crlf
notavailable-check-nameserver-response = response
 1*("IPAddress" colon ip-address crlf)
 dot crlf

; DEL command.
del-request = del-domain-request / del-nameserver-request
del-response = response
 dot crlf
del-domain-request = "del" crlf
 "EntityName" colon "Domain" crlf
 "DomainName" colon sldn crlf
 dot crlf
del-nameserver-request = "del" crlf
 "EntityName" colon "NameServer" crlf
 "NameServer" colon servername crlf
 dot crlf

; DESCRIBE command.
describe-request = "describe" crlf
 [target-option]
 *(option-tag colon option-value crlf)
 dot crlf
```

```
describe-response = response
 "Protocol" colon version-number crlf
 *attribute-line
 dot crlf
target-option = dash "Target" colon "Protocol" crlf

; MOD command.
mod-request = mod-domain-request / mod-nameserver-request
mod-response = response
 *attribute-line
 dot crlf
mod-domain-request = "mod" crlf
 "EntityName" colon "Domain" crlf
 "DomainName" colon sldn crlf
 *(add-attribute-value-line /
 remove-attribute-value-line /
 replace-attribute-value-line)
```

Hollenbeck & Srivastava   Informational   [Page 33]

RFC 2832   NSI Registry Registrar Protocol   May 2000

```
 dot crlf
mod-nameserver-request = "mod" crlf
 "EntityName" colon "NameServer" crlf
 "NameServer" colon servername crlf
 ["NewNameServer" colon attribute-value crlf]
 *(add-attribute-value-line /
 remove-attribute-value-line /
 replace-attribute-value-line)
 dot crlf
add-attribute-value-line =
 attribute-name colon new-attribute-value
remove-attribute-value-line =
 attribute-name colon old-attribute-value "="
replace-attribute-value-line =
 attribute-name colon old-attribute-value "="
 new-attribute-value
old-attribute-value = attribute-value
new-attribute-value = attribute-value

; QUIT command.
quit-request = "quit" crlf
 dot crlf
quit-response = response
```

```
dot crlf

; RENEW command.
renew-request = "renew" crlf
 "EntityName" colon "Domain" crlf
 "DomainName" colon sldn crlf
 [renew-period-option]
 dot crlf
expiration-year-option = dash "CurrentExpirationYear" colon year crlf
renew-period-option = period-option expiration-year-option /
                       expiration-year-option period-option
renew-response = response
 "RegistrationExpirationDate" colon time-stamp crlf
 dot crlf

; SESSION command.
session-request = "session" crlf
 registrar-id-option
 registrar-password-option
 [registrar-newpassword-option]
 dot crlf
session-response = response
 dot crlf
registrar-id-option = dash "Id" colon option-value crlf
registrar-password-option =
```

Hollenbeck & Srivastava   Informational   [Page 34]

RFC 2832   NSI Registry Registrar Protocol   May 2000

```
 dash "Password" colon password crlf
registrar-newpassword-option =
 dash "NewPassword" colon password crlf

; STATUS command.
status-request = status-domain-request /
                 status-nameserver-request
status-response = response
 *attribute-line
 dot crlf
status-domain-request = "status" crlf
 "EntityName" colon "Domain" crlf
 "DomainName" colon sldn crlf
 dot crlf
status-nameserver-request = "status" crlf
```

```
"EntityName" colon "NameServer" crlf
"NameServer" colon servername crlf
dot crlf

; TRANSFER command.
transfer-request = "transfer" crlf
 [approve-option]
 "EntityName" colon "Domain" crlf
 "DomainName" colon sldn crlf
 dot crlf
transfer-response = response
 "RegistrationExpirationDate" colon time-stamp crlf
 dot crlf
approve-option = dash "Approve" colon yesno crlf

; End of grammar.
```

8. Internationalization

    RRP is defined using 7-bit US-ASCII characters. Other character sets
    and character codes are not currently supported.

9. Known Issues

    RRP was not designed to provide bulk data query features. The primary
    goal of the original protocol designers was to provide a fast, light
    weight transactional protocol that could be implemented with minimal
    need for database queries that would take a "long" time to complete
    or that would return a "large" amount of data. Implementers SHOULD
    consider developing offline reporting features to provide bulk data
    for registrar reporting in a fashion suitable for the given
    registry-registrar operating environment.

Hollenbeck & Srivastava   Informational   [Page 35]

RFC 2832   NSI Registry Registrar Protocol   May 2000

    This version of RRP does contain a few limitations noted over the
    course of several months of operational experience with live domain
    name registrars. Later versions of this protocol or its successors
    should strive to resolve or address each of the following issues:

    The DESCRIBE command should return information describing System-
    defined default implementation values.

Use of the RENEW command without the "CurrentExpirationYear" and
"Period" parameters does not provide idempotency. Repeated execution
of a RENEW command without these parameters can result in multiple
successful RENEW commands, which may not be the desired action if a
registrar is retrying a RENEW command due to network connectivity
problems.

Time stamps returned by RRP do not include time zone identifiers and
SHOULD be interpreted as local registry time.

The protocol does not provide features for a registrar to become
aware of domain transfer requests and responses. Systems must rely on
means outside of the protocol, such as electronic mail and/or
registry-provided reports, to inform registrars of transfer requests
and responses.

The protocol does not provide features for a registrar to determine
all of the domains served by a name server. Systems must provide this
information using a method outside of the protocol, such as through
periodic extracts from a System database.

The protocol does not provide features to manage lame delegation of
name servers. Any registrar may "use" name servers registered by
another registrar. When a registrar tries to delete a domain or name
server it is quite possible that name servers in the domain to be
deleted or the name server to be deleted will be associated with
other live domains, precluding immediate deletion. Systems must rely
on means outside of the protocol to manage lame delegation of name
servers.

The use of "=" within the MOD command to indicate a value to be
removed is somewhat confusing. A more explicit means of identifying
old and new attribute values within the protocol syntax could make
this feature more obvious.

The CHECK command also returns name server IP addresses when
returning positive confirmation of the registration of a name server.
This extra information may be useful, but it is inconsistent with the
limited function of the command. The command should return a
positive or negative response and nothing more.

Hollenbeck & Srivastava   Informational   [Page 36]

RFC 2832   NSI Registry Registrar Protocol   May 2000

The formal protocol syntax described in this document requires a
specific order for the elements of a command entity block and command
options. The NSI Registry's server-side implementation of the
protocol provides the additional flexibility of allowing order
independent specification of options and entity block elements.
Client-side implementers are strongly urged to observe the order of
command elements as specified here to ensure compliance if the more
restricted form is enforced in the future.

RRP does not return time stamps or transaction identifiers to track
transactions. The NSI Registry provides registrars with daily and
weekly reports that include time stamps in local registry time to
document and synchronize data on a per-registrar basis.

10. Security Considerations

Misuse of the Registry Registrar Protocol can have catastrophic
operational consequences for registrants, registrars, and registries.
As such, all registrars must be authenticated prior to all
interactions with the registry. In addition, all data exchanged
between the registrar and the registry must be protected to avoid
unintended disclosure of information.

11. IANA Considerations

IANA assigned TCP port 648 for RRP use in November 1998. No other
action is required of IANA to support operation of this protocol.

IANA has reserved certain IPv4 address ranges as described in
[ALLOCATION]. Implementers MUST ensure that name server IP addresses
do not fall into one of the reserved address ranges to avoid
operational DNS errors.

12. References

[ABNF]   Crocker, D. (Editor) and P. Overell, "Augmented BNF for
              Syntax Specifications: ABNF", RFC 2234, November 1997.

[ALLOCATION] Hubbard, K., Kosters, M., Conrad, D., Karrenberg, D. and
              J. Postel, "Internet Registry IP Allocation Guidelines",
              BCP 12, RFC 2050, November 1996.

[MUSTSHOULD] Bradner, S., "Key Words for Use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

Hollenbeck & Srivastava   Informational   [Page 37]

RFC 2832   NSI Registry Registrar Protocol   May 2000

    [SSL]   A. Frier, P. Karlton, and P. Kocher, "The SSL 3.0
                  Protocol", Netscape Communications Corp., November 18,
                  1996.

    [TLS]   Dierks T. and C. Allen, "The TLS Protocol Version 1.0",
                  RFC 2246, January 1999.

13. Acknowledgments

Many people have contributed significantly to this document and the
protocol it describes. Brad McMillen and Neeran Saraf deserve special
mention as co-authors of an earlier internal protocol specification.
Other content contributors to the earlier internal specification
include Aristotle Balogh, Chris Bason, Mark Kosters, Jasdip Singh,
and Yibing Wu. Finally, significant contributors to the review of
this document include Steve Mahlstedt and Chris Smith.

14. Authors' Addresses

Scott Hollenbeck
Network Solutions, Inc. Registry
505 Huntmar Park Dr.
Herndon, VA 20170
USA

EMail: shollenb@netsol.com

Manoj Srivastava
Network Solutions, Inc. Registry
505 Huntmar Park Dr.
Herndon, VA 20170
USA

EMail: manojs@netsol.com

Hollenbeck & Srivastava   Informational   [Page 38]

RFC 2832   NSI Registry Registrar Protocol   May 2000

15. Full Copyright Statement

Acknowledgement

Hollenbeck & Srivastava   Informational   [Page 39]

2. <u>Supported initial and renewal registration periods</u>

a. Initial registrations of Registered Names (where available according to functional specifications and
other requirements) may be made in the registry for a minimum of one year or in multiples of one-year
increments up to ten years.

b. Renewal registrations of Registered Names (where available according to functional specifications
and other requirements) may be made in the registry in multiples of one-year increments, provided that
the maximum unexpired (i.e. into the future) term of the registration of an unexpired name shall not
exceed ten years.

c. Upon change of sponsorship of the registration of a Registered Name from one registrar to another,
according to Part A of Exhibit B to Appendix F of the registry agreement, the term of registration of the

Registered Name shall be extended by one year, provided that the maximum unexpired (i.e. into the future) term of the registration of an unexpired name shall not exceed ten years.

d. The change of sponsorship of registration of Registered Names from one registrar to another, according to Part B of Exhibit B to Appendix F of the registry agreement shall not result in the extension of the term of the registrations.

3. <u>Grace period policy</u>

1. Introduction

This document describes VeriSign Global Registry Services (VGRS) practices for operational "Grace" and "Pending" periods, including relationships among sequential operations that occur within given time frames. A *Grace Period* refers to a specified number of calendar days following a Registry operation in which the domain may be deleted and a credit may be issued to a registrar. Relevant registry operations in this context are:

- Registration of a new domain,
- Extension of an existing domain,
- Auto-Renew of an existing domain;
- Transfer of an existing domain, and
- Deletion of an existing domain.

Extension of a registration period is accomplished using the RRP RENEW command or by auto-renewal; registration is accomplished using the RRP ADD command; deletion/removal is accomplished using the RRP DEL command; and transfer is accomplished using the RRP TRANSFER command or, where ICANN approves a bulk transfer under Part B of Exhibit B to the Registry-Registrar Agreement, using the procedures specified in that Part .

There are four grace periods provided by the VGRS Shared Registration System: *Add Grace Period, Renew/Extend Grace Period, Auto-Renew Grace Period,* and *Transfer Grace Period.*

A *Pending Period* refers to a specified number of calendar days following a Registry operation in which final Registry action is deferred before the operation may be completed. Relevant Registry operations in this context are:

- Transfer of an existing domain, and
- Deletion of an existing domain.

2. Grace Periods

2.1 Add Grace Period

The *Add Grace Period* is a specified number of calendar days following the initial registration of a domain. The current value of the *Add Grace Period* for all registrars is five calendar days. If a Delete, Extend (RRP Command Renew), or Transfer operation occurs within the five calendar days, the following rules apply:

> *Delete.* If a domain is deleted within the *Add Grace Period*, the sponsoring Registrar at the time of the deletion is credited for the amount of the registration. The domain is deleted from the Registry database and is immediately available for registration by any Registrar. See Section 3 for a description of overlapping grace period exceptions.

> *Extend (RRP Command "Renew").* If a domain is extended within the *Add Grace Period*, there is no credit for the add. The account of the sponsoring Registrar at the time of the extension will be charged for the initial add plus the number of years the registration is extended. The expiration date of the domain is extended by the number of years, up to a total of ten years, as specified by the registrar's requested Extend operation.

> *Transfer (other than ICANN-approved bulk transfer).* Transfers under Part A of Exhibit B to the Registry-Registrar Agreement may not occur during the *Add Grace Period* or at any other time within the first 60 days after the initial registration. Enforcement is the responsibility of the Registrar sponsoring the domain name registration and is currently enforced by the SRS.

> *Bulk Transfer (with ICANN approval).* Bulk transfers with ICANN approval may be made during the *Add Grace Period* according to the procedures in Part B of Exhibit B to the Registry-Registrar Agreement. The expiration dates of transferred registrations are not affected. The losing Registrar's account is charged for the initial add.

2.2 Renew/Extend Grace Period

The *Renew/Extend Grace Period* is a specified number of calendar days following the renewal/ extension of a domain name registration period through an RRP Command Renew. The current value of the *Renew/Extend Grace Period* is five calendar days. If a Delete, Extend, or Transfer occurs within that five calendar days, the following rules apply:

> *Delete.* If a domain is deleted within the *Renew/Extend Grace Period*, the sponsoring Registrar at the time of the deletion receives a credit of the renew/extend fee. The domain is deleted from the Registry database and is immediately available for registration by any Registrar. See Section 3 for a description of overlapping grace period exceptions.

> *Extend (RRP Command "Renew").* A domain can be extended within the *Renew/Extend Grace Period* for up to a total of ten years. The account of the sponsoring Registrar at the time of the additional extension will be charged for the additional number of years the registration is extended.

> *Transfer (other than ICANN-approved bulk transfer).* If a domain is transferred within the *Renew/Extend Grace Period*, there is no credit. The expiration date of the domain is

extended by one year and the years added as a result of the Extend remain on the domain name up to a total of 10 years.

Bulk Transfer (with ICANN approval). Bulk transfers with ICANN approval may be made during the *Renew/Extend Grace Period* according to the procedures in Part B of Exhibit B to the Registry-Registrar Agreement. The expiration dates of transferred registrations are not affected. The losing Registrar's account is charged for the Renew/Extend operation.

2.3 Auto-Renew Grace Period

The *Auto-Renew Grace Period* is a specified number of calendar days following an auto-renewal. An auto-renewal occurs if a domain name registration is not renewed by the expiration date; in this circumstance the registration will be automatically renewed by the system the first day after the expiration date. The current value of the *Auto-Renew Grace Period* is 45 calendar days. If a Delete, Extend, or Transfer occurs within the *Auto-Renew Grace Period*, the following rules apply:

Delete. If a domain is deleted within the *Auto-Renew Grace Period*, the sponsoring Registrar at the time of the deletion receives a credit of the Auto-Renew fee. The domain is deleted from the Registry database and is immediately available for registration by any Registrar. See Section 3 for a description of overlapping grace period exceptions.

Extend (RRP Command "Renew"). A domain can be extended within the *Auto-Renew Grace Period* for up to a total of ten years. The account of the sponsoring Registrar at the time of the additional extension will be charged for the additional number of years the registration is extended.

Transfer (other than ICANN-approved bulk transfer). If a domain is transferred under Part A of Exhibit B to the Registry-Registrar Agreement within the *Auto-Renew Grace Period*, the losing Registrar is credited with the Auto-Renew charge and the year added by the Auto-Renew operation is cancelled. The expiration date of the domain is extended by one year up to a total maximum of ten by virtue of the transfer and the gaining Registrar is charged for that additional year, even in cases where a full year is not added because of the 10-year maximum limitation.

Bulk Transfer (with ICANN approval). Bulk transfers with ICANN approval may be made during the *Auto-Renew Grace Period* according to the procedures in Part B of Exhibit B to the Registry-Registrar Agreement. The expiration dates of transferred registrations are not affected. The losing Registrar's account is charged for the Auto-Renew.

2.4 Transfer Grace Period

The *Transfer Grace Period* is a specified number of calendar days following the transfer of a domain according to Part A of Exhibit B to the Registry-Registrar Agreement. The current value of the *Transfer Grace Period* is five calendar days. If a Delete, Extend, or Transfer occurs within that five calendar days, the following rules apply:

Delete. If a domain is deleted within the *Transfer Grace Period*, the sponsoring Registrar at the time of the deletion receives a credit of the transfer fee. The domain is deleted from the Registry database and is immediately available for registration by any Registrar. See Section 3 for a description of overlapping grace period exceptions.

Extend (RRP Command "Renew"). If a domain is extended within the *Transfer Grace Period*, there is no credit for the transfer. The Registrar's account will be charged for the number of years the registration is extended. The expiration date of the domain is extended by the number of years, up to a maximum of ten years, as specified by the registrar's requested Extend operation.

Transfer (other than ICANN-approved bulk transfer). If a domain is transferred within the *Transfer Grace Period*, there is no credit. The expiration date of the domain is extended by one year up to a maximum term of ten years.

Bulk Transfer (with ICANN approval). Bulk transfers with ICANN approval may be made during the *Transfer Grace Period* according to the procedures in Part B of Exhibit B to the Registry-Registrar Agreement. The expiration dates of transferred registrations are not affected. The losing Registrar's account is charged for the Transfer operation that occurred prior to the Bulk Transfer.

2.5 Bulk Transfer Grace Period

There is no grace period associated with Bulk Transfer operations according to Part B of Exhibit B to the Registry-Registrar Agreement. Upon completion of the Bulk Transfer, any associated fee is not refundable.

3. Overlapping Grace Periods

If an operation is performed that falls into more that one grace period, the actions appropriate for each grace period apply (with some exceptions as noted below).

- If a domain is deleted within the Add Grace Period and the Extend Grace Period, then the Registrar is credited the registration and extend amounts, taking into account the number of years for which the registration and extend were done.
- If a domain is auto-renewed, then extended, and then deleted within the Extend Grace Period, the registrar will be credited for the Auto-Renew and the number of years for the extension.

3.1 Overlap Exception

- If a domain is deleted within one or several Transfer Grace Periods, then only the current sponsoring Registrar is credited for the transfer amount. For example if a domain is transferred from Registrar A to Registrar B and then to Registrar C and finally deleted by Registrar C within the Transfer Grace Period of the first, second and third transfers, then only the last transfer is credited to Registrar C.
- If a domain is extended (through the RRP command "Renew") within the Transfer Grace Period,

then the current Registrar's account is charged for the number of years the registration is extended.

Note: If several billable operations, including transfers, are performed on a domain and the domain is deleted within the grace periods of each of those operations, only those operations that were performed after the latest transfer, including the latest transfer, are credited to the current Registrar.

4. Pending Periods

4.1 Transfer Pending Period

The *Transfer Pending Period* is a specified number of calendar days following a request from a registrar (registrar A) to transfer a domain in which the current registrar of the domain (registrar B) may explicitly approve or reject the transfer request. The current value of the *Transfer Pending Period* is five calendar days for all registrars. The transfer will be finalized upon receipt of explicit approval or rejection from the current registrar (registrar B). If the current registrar (registrar B) does not explicitly approve or reject the request initiated by registrar A, the registry will approve the request automatically after the end of the *Transfer Pending Period*. During the *Transfer Pending Period*:

a. RRP TRANSFER request or RRP RENEW request is denied.
b. AUTO-RENEW is allowed.
c. RRP DELETE request is denied.
d. Bulk Transfer operations are allowed.

4.2 Delete Pending Period

The *Delete Pending Period* is a specified number of calendar days following a request to delete a domain in which the domain is placed in REGISTRY-HOLD status without removing the domain from the Registry database. The current value of the *Delete Pending Period* for all registrars is five calendar days. Registrars may request retraction of a Delete request by calling the VGRS Customer Support staff within the *Delete Pending Period*. Retraction requests processed during the *Delete Pending Period* will be at no cost to the registrar. If no action is taken within the *Delete Pending Period*, the domain will be deleted from the Registry database and returned to the pool of domain names available for registration by any Registrar. During the *Delete Pending Period*:

a. RRP RENEW or AUTO-RENEW request is ignored.
b. RRP TRANSFER request is denied.
c. Bulk Transfer operations are allowed.

4. <u>Nameserver functional specifications</u>

Nameserver operations for the Registry TLD shall comply with <u>RFC 1034</u>, <u>1035</u>, and <u>2182</u>.

5. Patch, update, and upgrade policy

VeriSign Global Registry Services (VGRS) may issue periodic patches, updates or upgrades to the Software, RRP or APIs ("Licensed Product") licensed under the Registry-Registrar Agreement (the "Agreement") that will enhance functionality or otherwise improve the Shared Registration System under the Agreement. For the purposes of this Part 5 of Appendix C, the following terms have the associated meanings set forth herein. (1) A "Patch" means minor modifications to the Licensed Product made by VGRS during the performance of error correction services. A Patch does not constitute a Version. (2) An "Update" means a new release of the Licensed Product which may contain error corrections, minor enhancements, and, in certain circumstances, major enhancements, and which is indicated by a change in the digit to right of the decimal point in the version number of the Licensed Product. (3) An "Upgrade" means a new release of the Licensed Product which involves the addition of substantial or substantially enhanced functionality and which is indicated by a change in the digit to the left of the decimal point in the version of the Licensed Product. (4) A "Version" means the Licensed Product identified by any single version number. Each Update and Upgrade causes a change in Version. Patches do not require corresponding changes to client applications developed, implemented, and maintained by each registrar. Updates may require changes to client applications by each registrar in order to take advantage of the new features and/or capabilities and continue to have access to the Shared Registration System. Upgrades require changes to client applications by each registrar in order to take advantage of the new features and/or capabilities and continue to have access to the Shared Registration System.

VGRS, in its sole discretion, will deploy Patches during scheduled and announced Shared Registration System maintenance periods.

For Updates and Upgrades, VGRS will give each registrar notice prior to deploying the Updates and Upgrades into the production environment. The notice shall be at least sixty (60) days, except that if ICANN's registry agreements with all other unsponsored TLDs provide that the operators of those TLDs will provide at least ninety (90) days' notice, then VGRS will provide at least ninety (90) days' notice. Such notice (whether 60 or 90 days) will include an initial thirty (30) days' notice before deploying the Update that requires changes to client applications or the Upgrade into the Operational Test and Evaluation ("OT&E") environment to which all registrars have access. VGRS will maintain the Update or Upgrade in the OT&E environment for at least thirty (30) days, to allow each registrar the opportunity to modify its client applications and complete testing, before implementing the new code in the production environment.

6. Migration to provreg standard

VeriSign Global Registry Services (VGRS) is committed to participating in and supporting the work of the IETF's provreg working group. VeriSign intends to migrate the current Shared Registration System to the new standard if: (1) The IETF working group defines a protocol standard; (2) the standard can be implemented in a way that minimizes disruption to customers; and (3) the standard provides a solution for which the potential advantages are reasonably justifiable when weighed against the costs that VGRS and its registrar customers would incur in implementing the new standard.

Comments concerning the layout, construction and functionality of this site
should be sent to webmaster@icann.org.

Page Updated 16-April-2001

Exhibit C

Site Map | Site Index | Quick Links | Select a link below:

Search

Submit Query

Internet Corporation for Assigned Names and Numbers

| Home | About | News | Policy | In Focus | Meetings | Resources | Documents | Press Room | Careers |

Contact

Resources

Information for Registrars and Registrants

List of Accredited Registrars

Become an ICANN Accredited Registrar

Changes to an Existing Accreditation

Governing Agreements and Policies

ICANN Registrar Advisories

ICANN Internal Procedure for Handling Conflicts with Privacy Law

Policy on Transfer of Registrations between Registrars

12 July 2004

This Policy was modified by ICANN's Board of Directors on 7 November 2008 with an Effective Date of 15 March 2009.

See modified version of Policy

A. Holder-Authorized Transfers

1. Registrar Requirements

Registered Name Holders must be able to transfer their domain name registrations between Registrars provided that the Gaining Registrar's transfer process meets the minimum standards of this policy and that such transfer is not prohibited by ICANN or Registry policies. Inter-Registrar domain name transfer processes must be clear and concise in order to avoid confusion. Further, Registrars should make reasonable efforts to inform Registered Name Holders of, and provide access to, the published documentation of the specific transfer process employed by the Registrars.

1.1 Transfer Authorities

The Administrative Contact and the Registered Name Holder, as listed in the Losing Registrar's or applicable Registry's (where available) publicly accessible WHOIS service are the only parties that have the authority to approve or deny a transfer request to the Gaining Registrar. In the event of a dispute, the Registered Name Holder's authority supersedes that of the Administrative Contact.

Registrars may use Whois data from either the Registrar of Record or the relevant Registry for the purpose of verifying the authenticity of a transfer request; or from another data source as determined by a consensus policy.

2. Gaining Registrar Requirements

For each instance where a Registered Name Holder requests to transfer a domain name registration to a different Registrar, the Gaining Registrar shall:

2.1 Obtain express authorization from either the Registered Name Holder or the Administrative Contact (hereafter, "Transfer Contact"). Hence, a transfer may only proceed if confirmation of the transfer is received by the Gaining Registrar from the Transfer Contact.

2.1.1 The authorization must be made via a valid Standardized Form of Authorization (FOA). There are two different FOA's available at the ICANN website. The FOA labeled "Initial Authorization for Registrar Transfer" must be used by the Gaining Registrar to request an authorization for a registrar transfer from the Transfer Contact. The FOA labeled "Confirmation of Registrar Transfer Request" may be used by the Registrar of Record to request confirmation of the transfer from the Transfer Contact.

The FOA shall be communicated in English, and any dispute arising out of a transfer request shall be conducted in the English language. Registrars may choose to communicate with the Transfer Contact in additional languages. However, Registrars choosing to exercise such option are responsible for the accuracy and completeness of the translation into such additional non-English version of the FOA.

2.1.2 In the event that the Gaining Registrar relies on a physical process to obtain this authorization, a paper copy of the FOA will suffice insofar as it has been signed by the Transfer Contact and further that it is accompanied by a physical copy of the Registrar of Record's Whois output for the domain name in question.

2.1.2.1 If the Gaining Registrar relies on a physical authorization process, then the Gaining Registrar

assumes the burden of obtaining reliable evidence of the identity of the Transfer Contact and maintaining appropriate records proving that such evidence was obtained. Further the Gaining Registrar also assumes the burden for ensuring that the entity making the request is indeed authorized to do so. The acceptable forms of physical identity are:

- Notarized statement
- Valid Drivers license
- Passport
- Article of Incorporation
- Military ID
- State/Government issued ID
- Birth Certificate

2.1.3 In the event that the Gaining Registrar relies on an electronic process to obtain this authorization the acceptable forms of identity would include:

- Electronic signature in conformance with national legislation, in the location of the Gaining Registrar (if such legislation exists).
- Consent from an individual or entity that has an email address matching the Transfer Contact email address.

The Registrar of Record may not deny a transfer request solely because it believes that the Gaining Registrar has not received the confirmation set forth above.

A transfer must not be allowed to proceed if no confirmation is received by the Gaining Registrar. The presumption in all cases will be that the Gaining Registrar has received and authenticated the transfer request made by a Transfer Contact.

2.2 Request, by the transmission of a "transfer" command as specified in the Registrar Tool Kit, that the Registry Operator database be changed to reflect the new Registrar.

2.2.1 Transmission of a "transfer" command constitutes a representation on the part of the Gaining Registrar that the requisite authorization has

been obtained from the Transfer Contact listed in the authoritative Whois database.

2.2.2 The Gaining Registrar is responsible for validating the Registered Name Holder requests to transfer domain names between Registrars. However, this does not preclude the Registrar of Record from exercising its option to independently confirm the Registered Name Holder's intent to transfer its domain name to the Gaining Registrar in accordance with Section 3 of this policy.

3. Obligations of the Registrar of Record

A Registrar of Record can choose independently to confirm the intent of the Registered Name Holder when a notice of a pending transfer is received from the Registry. The Registrar of Record must do so in a manner consistent with the standards set forth in this agreement pertaining to Gaining Registrars. In order to ensure that the form of the request employed by the Registrar of Record is substantially administrative and informative in nature and clearly provided to the Transfer Contact for the purpose of verifying the intent of the Transfer Contact, the Registrar of Record must use the FOA.

The FOA shall be communicated in English, and any dispute arising out of a transfer request, shall be conducted in the English language. Registrars may choose to communicate with the Transfer Contact in additional languages. However, the Registrar choosing to exercise such option is responsible for the accuracy and completeness of the translation into such additional non-English version of the FOA. Further, such non-English communications must follow the processes and procedures set forth in this policy. This includes but is not limited to the requirement that no Registrar shall add any additional information to the FOA used to obtain the consent of the Transfer Contact in the case of a transfer request.

This requirement does not preclude the Registrar of Record from marketing to its existing customers through separate communications.

The FOA should be sent by the Registrar of Record to the Transfer Contact as soon as operationally possible, but must be sent not later than twenty-four (24) hours after receiving the transfer request from the Registry Operator.

Failure by the Registrar of Record to respond within five (5) calendar days to a notification from the Registry regarding a transfer request will result in a default "approval" of the transfer.

In the event that a Transfer Contact listed in the Whois has not confirmed their request to transfer with the Registrar of Record and the Registrar of Record has not explicitly denied the transfer request, the default

action will be that the Registrar of Record must allow the transfer to proceed.

Upon denying a transfer request for any of the following reasons, the Registrar of Record must provide the Registered Name Holder and the potential Gaining Registrar with the reason for denial. The Registrar of Record may deny a transfer request only in the following specific instances:

1. Evidence of fraud
2. UDRP action
3. Court order by a court of competent jurisdiction
4. Reasonable dispute over the identity of the Registered Name Holder or Administrative Contact
5. No payment for previous registration period (including credit card charge-backs) if the domain name is past its expiration date or for previous or current registration periods if the domain name has not yet expired. In all such cases, however, the domain name must be put into "Registrar Hold" status by the Registrar of Record prior to the denial of transfer.
6. Express written objection to the transfer from the Transfer Contact. (e.g. - email, fax, paper document or other processes by which the Transfer Contact has expressly and voluntarily objected through opt-in means)
7. A domain name was already in "lock status" provided that the Registrar provides a readily accessible and reasonable means for the Registered Name Holder to remove the lock status.
8. A domain name is in the first 60 days of an initial registration period.
9. A domain name is within 60 days (or a lesser period to be determined) after being transferred (apart from being transferred back to the original Registrar in cases where both Registrars so agree and/or where a decision in the dispute resolution process so directs).

Instances when the requested change of Registrar may not be denied include, but are not limited to:

- Nonpayment for a pending or future registration period
- No response from the Registered Name Holder or Administrative Contact.
- Domain name in Registrar Lock Status, unless the Registered Name Holder is provided with the reasonable opportunity and ability to unlock the domain name prior to the Transfer Request.
- Domain name registration period time constraints, other than during the first 60 days of initial registration or during the first 60 days after a registrar transfer.
- General payment defaults between Registrar and business partners / affiliates in cases where the Registered Name Holder for the domain in question has paid for the registration.

The Registrar of Record has other mechanisms available to collect payment from the Registered Name Holder that are independent from the Transfer process. Hence, in the event of a dispute over payment, the Registrar of Record must not employ transfer processes as a mechanism to secure payment for services

from a Registered Name Holder. Exceptions to this requirement are as follows:

(i) In the case of non-payment for previous registration period(s) if the transfer is requested after the expiration date, or

(ii) In the case of non-payment of the current registration period, if transfer is requested before the expiration date.

4. Registrar Coordination

Each Registrar is responsible for keeping copies of documentation, including the FOA and the Transfer Contacts response thereto, that may be required for filing and supporting a dispute under the dispute resolution policy. Gaining Registrars must maintain copies of the FOA as received from the Transfer Contact as per the standard document retention policies of the contracts. Copies of the reliable evidence of identity must be kept with the FOA.

Both the Gaining Registrar and the Registrar of Record must provide the evidence relied on for the transfer during and after the applicable inter-registrar domain name transaction(s). Such information must be provided when requested by, and only by, the other Registrar that is party to the transfer transaction. Additionally, ICANN, the Registry Operator, a court or authority with jurisdiction over the matter or a third party dispute resolution panel may also require such information within five (5) days of the request.

The Gaining Registrar must retain, and produce pursuant to a request by a Losing Registrar, a written or electronic copy of the FOA. In instances where the Registrar of Record has requested copies of the FOA, the Gaining Registrar must fulfill the Registrar of Records request (including providing the attendant supporting documentation) within five (5) calendar days. Failure to provide this documentation within the time period specified is grounds for reversal by the Registry Operator or the Dispute Resolution Panel in the event that a transfer complaint is filed in accordance with the requirements of this policy.

If either a Registrar of Record or a Gaining Registrar does not believe that a transfer request was handled in accordance with the provisions of this policy, then the Registrar may initiate a dispute resolution procedure as set forth in Section C of this policy.

For purposes of facilitating transfer requests, Registrars should provide and maintain a unique and private email address for use only by other Registrars and the Registry:

   i. This email address is for issue related to transfer requests and the procedures set forth in this policy only.

   ii. The email address should be managed to ensure messages are received by someone

who can respond to the transfer issue.

iii. Messages received at such email address must be responded to within a commercial reasonable timeframe not to exceed seven (7) calendar days.

5. EPP - based Registry Requirements for Registrars

In EPP-based gTLD Registries, Registrars must follow the requirements set forth below.

Registrars must provide the Registered Name Holder with the unique "AuthInfo" code within five (5) calendar days of the Registered Name Holder's initial request if the Registrar does not provide facilities for the Registered Name Holder to generate and manage their own unique "AuthInfo" code.

Registrars may not employ any mechanism for complying with a Registered Name Holder's request to obtain the applicable "AuthInfo Code" that is more restrictive than the mechanisms used for changing any aspect of the Registered Name Holder's contact or name server information.

The Registrar of Record must not refuse to release an "AuthInfo Code" to the Registered Name Holder solely because there is a dispute between the Registered Name Holder and the Registrar over payment.

Registrar-generated "AuthInfo" codes must be unique on a per-domain basis.

The "Auth-Info" codes must be used solely to identify a Registered Name Holder, whereas the FOA's still need to be used for authorization or confirmation of a transfer request, as described in Section 2 and Section 4 of this policy.

6. Registry Requirements

Upon receipt of the "transfer" command from the Gaining Registrar, Registry Operator will transmit an electronic notification to both Registrars. In the case of those Registries that use electronic mail notifications, the response notification may be sent to the unique email address established by each Registrar for the purpose of facilitating transfers.

The Registry Operator shall complete the requested transfer unless, within five (5) calendar days, Registry Operator receives a NACK protocol command from the Registrar of Record.

When the Registry's database has been updated to reflect the change to the Gaining Registrar, Registry Operator will transmit an electronic notification to both Registrars. The notification may be sent to the unique email address established by each Registrar for the purpose of facilitating transfers or such other email address agreed to by the parties.

The Registry Operator shall undo a transfer if, after a transfer has occurred, the Registry Operator receives one of the notices as set forth below. In such case, the transfer will be reversed and the domain name reset to its original state. The Registry Operator must undo the transfer within five (5) calendar days of receipt of the notice except in the case of a Registry dispute decision, in which case the Registry Operator must undo the transfer within fourteen calendar days unless a court action is filed. The notice required shall be one of the following:

    i. Agreement of the Registrar of Record and the Gaining Registrar sent by email, letter or fax that the transfer was made by mistake or was otherwise not in accordance with the procedures set forth in this policy;

    ii. The final determination of a dispute resolution body having jurisdiction over the transfer; or

    iii. Order of a court having jurisdiction over the transfer.

7. Records of Registration

Each Registrar shall require its customer, the Registered Name Holder, to maintain its own records appropriate to document and prove the initial domain name registration date.

8. Effect on Term of Registration

The completion by Registry Operator of a holder-authorized transfer under this Part A shall result in a one-year extension of the existing registration, provided that in no event shall the total unexpired term of a registration exceed ten (10) years.

B. ICANN-Approved Transfers

Transfer of the sponsorship of all the registrations sponsored by one Registrar as the result of (i) acquisition of that Registrar or its assets by another Registrar, or (ii) lack of accreditation of that Registrar or lack of its authorization with the Registry Operator, may be made according to the following procedure:

    (a) The gaining Registrar must be accredited by ICANN for the Registry TLD and must have in effect a Registry-Registrar Agreement with Registry Operator for the Registry TLD.

    (b) ICANN must certify in writing to Registry Operator that the transfer would promote the community interest, such as the interest in stability that may be threatened by the actual or imminent business failure of a Registrar.

Upon satisfaction of these two conditions, Registry Operator will make the necessary one-time changes in the Registry

database for no charge, for transfers involving 50,000 name registrations or fewer. If the transfer involves registrations of more than 50,000 names, Registry Operator will charge the gaining Registrar a one-time flat fee of US$ 50,000.

C. Transfer Dispute Resolution Policy

Procedures for handling disputes concerning inter-registrar transfers are set forth in the Transfer Dispute Resolution Policy. Procedures in this policy must be followed by the applicable Registry Operators and ICANN accredited Registrars.

About	News	Policy	In Focus	Resources	Governance Documents	General Documents
FAQs	Announcements	Policy Update	Affirmation of Commitments	Accredited Registrars	Articles of Incorporation	Meetings
IANA	Blog	At-Large	Contractual Compliance	Dispute Resolution Options	Bylaws	Press Room
Mission	Newsletter	ASO	DNSSEC	E-Learning	Board Meeting Minutes and Resolutions	Careers
Structure	News Releases	ccNSO	Fellowship Program	Photos	Board Code of Conduct	Contact
	RSS Feeds	GAC	Internationalized Domain Names (IDNs)	Videos	Board Conflicts of Interest Policy	
		GNSO	IDN ccTLD Fast Track Process	Speeches and Presentations	Summary of Board Statements of Interest	
		RSSAC	IPv6	Whois Search		
		SSAC	New gTLD Program			

ICANN

This file last modified 13-Aug-2010

© 2011 Internet Corporation For Assigned Names and Numbers