Special-Use Domain Names

Abstract

   This document describes what it means to say that a Domain Name (DNS
   name) is reserved for special use, when reserving such a name is
   appropriate, and the procedure for doing so. It establishes an IANA
   registry for such domain names, and seeds it with entries for some of
   the already established special domain names.

Status of This Memo

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Further information on
   Internet Standards is available in Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc6761.

1. Introduction

   Certain individual IP addresses and IP address ranges are treated
   specially by network implementations and, consequently, are not
   suitable for use as unicast addresses. For example, IPv4 addresses
   224.0.0.0 to 239.255.255.255 are multicast addresses [RFC5735], with
   224.0.0.1 being the "all hosts" multicast address [RFC1112]
   [RFC5771]. Another example is 127.0.0.1, the IPv4 "local host"
   address [RFC5735].

   Analogous to Special-Use IPv4 Addresses [RFC5735], the Domain Name
   System (DNS) [RFC1034][RFC1035] has its own concept of reserved
   names, such as "example.com.", "example.net.", and "example.org.", or
   any name falling under the top-level pseudo-domain "invalid."
   [RFC2606]. However, "Reserved Top Level DNS Names" [RFC2606] does
   not state whether implementations are expected to treat such names
   differently, and if so, in what way.

   This document specifies under what circumstances special treatment is
   appropriate, and in what ways.

2. Terminology

   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 "Key words for use in
   RFCs to Indicate Requirement Levels" [RFC2119].

3. Applicability

   When IP multicast was created [RFC1112], implementations had to be
   updated to understand what an IP multicast address means and what to
   do with it. Adding IP multicast to a networking stack entailed more
   than merely adding the right routing table entries for those
   addresses. Moreover, supporting IP multicast entails some level of
   commonality that is consistent across all conformant hosts,
   independent of what networks those hosts may be connected to. While
   it is possible to build a private isolated network using whatever
   valid unicast IP addresses and routing topology one chooses
   (regardless of whether those unicast IP addresses are already in use
   by other hosts on the public Internet), the IPv4 multicast address
   224.0.0.1 is always the "all hosts" multicast address, and that's not
   a local decision.

   Similarly, if a domain name has special properties that affect the
   way hardware and software implementations handle the name, that apply
   universally regardless of what network the implementation may be
   connected to, then that domain name may be a candidate for having the

   IETF declare it to be a Special-Use Domain Name and specify what
   special treatment implementations should give to that name. On the
   other hand, if declaring a given name to be special would result in
   no change to any implementations, then that suggests that the name
   may not be special in any material way, and it may be more
   appropriate to use the existing DNS mechanisms [RFC1034] to provide
   the desired delegation, data, or lack-of-data, for the name in
   question. Where the desired behaviour can be achieved via the
   existing domain name registration processes, that process should be
   used. Reservation of a Special-Use Domain Name is not a mechanism
   for circumventing normal domain name registration processes.

   As an example, suppose there were to be an IETF document specifying
   that a particular name (or set of names) is guaranteed to produce an
   NXDOMAIN ("Name Error" [RFC1035]) result. Such a document falls
   within the responsibilities of the IETF. The IETF is responsible for
   protocol rules. The IETF defines name character set, length limits,
   syntax, the fact that in DNS "A" is equivalent to "a", etc.
   [RFC1034] [RFC1035]. Portions of the namespace created by those
   rules are given to ICANN to manage, but, due to established DNS
   protocol rules, ICANN is not free to allocate "COM" and "com" to two
   different name servers. The IETF has responsibility for specifying
   how the DNS protocol works, and ICANN is responsible for allocating
   the names made possible by that DNS protocol. Now, suppose a
   developer were to use this special "guaranteed nonexistent" name,
   "knowing" that it's guaranteed to return NXDOMAIN, and suppose also
   that the user's DNS server fails to return NXDOMAIN for this name.
   The developer's software then fails. Who do the user and/or
   developer complain to? ICANN? The IETF? The DNS server operator?
   If the developer can't depend on the special "guaranteed nonexistent"
   name to always return NXDOMAIN, then the special name is worthless,
   because it can't be relied on to do what it is supposed to. For this
   special "guaranteed nonexistent" name to have any use, it has to be
   defined to return NXDOMAIN, BY PROTOCOL, for all installations, not
   just by ICANN allocation on the public Internet. ICANN has no
   jurisdiction over how users choose to configure their own private DNS
   servers on their own private networks, but developers need a protocol
   specification that states that returning positive answers for the
   special "guaranteed nonexistent" name is a protocol violation on
   all networks, not just the public Internet. Hence, the act of
   defining such a special name creates a higher-level protocol rule,
   above ICANN's management of allocable names on the public Internet.

4. Procedure

   If it is determined that special handling of a name is required in
   order to implement some desired new functionality, then an IETF
   "Standards Action" or "IESG Approval" specification [RFC5226] MUST be
   published describing the new functionality.

   The specification MUST state how implementations determine that the
   special handling is required for any given name. This is typically
   done by stating that any fully qualified domain name ending in a
   certain suffix (i.e., falling within a specified parent pseudo-
   domain) will receive the special behaviour. In effect, this carves
   off a sub-tree of the DNS namespace in which the modified name
   treatment rules apply, analogous to how IP multicast [RFC1112] or IP
   link-local addresses [RFC3927] [RFC4862] carve off chunks of the IP
   address space in which their respective modified address treatment
   rules apply.

   The specification also MUST state, in each of the seven "Domain Name
   Reservation Considerations" categories below, what special treatment,
   if any, is to be applied. If in all seven categories the answer is
   "none", then possibly no special treatment is required and requesting
   reservation of a Special-Use Domain Name may not be appropriate.

5. Domain Name Reservation Considerations

   An IETF "Standards Action" or "IESG Approval" document specifying
   some new naming behaviour, which requires a Special-Use Domain Name
   be reserved to implement this desired new behaviour, needs to contain
   a subsection of the "IANA Considerations" section titled "Domain Name
   Reservation Considerations" giving answers in the seven categories
   listed below. In the case of algorithmically generated DNS names,
   the specifying document needs to clearly identify the set of names
   generated by the algorithm that would require the proposed special
   treatment.

   1. Users:

       Are human users expected to recognize these names as special and
       use them differently? In what way?

   2. Application Software:

       Are writers of application software expected to make their
       software recognize these names as special and treat them
       differently? In what way? (For example, if a human user enters
       such a name, should the application software reject it with an
       error message?)

3. Name Resolution APIs and Libraries:

    Are writers of name resolution APIs and libraries expected to
    make their software recognize these names as special and treat
    them differently? If so, how?

4. Caching DNS Servers:

    Are developers of caching domain name servers expected to make
    their implementations recognize these names as special and treat
    them differently? If so, how?

5. Authoritative DNS Servers:

    Are developers of authoritative domain name servers expected to
    make their implementations recognize these names as special and
    treat them differently? If so, how?

6. DNS Server Operators:

    Does this reserved Special-Use Domain Name have any potential
    impact on DNS server operators? If they try to configure their
    authoritative DNS server as authoritative for this reserved name,
    will compliant name server software reject it as invalid? Do DNS
    server operators need to know about that and understand why?
    Even if the name server software doesn't prevent them from using
    this reserved name, are there other ways that it may not work as
    expected, of which the DNS server operator should be aware?

7. DNS Registries/Registrars:

    How should DNS Registries/Registrars treat requests to register
    this reserved domain name? Should such requests be denied?
    Should such requests be allowed, but only to a specially-
    designated entity? (For example, the name "www.example.org" is
    reserved for documentation examples and is not available for
    registration; however, the name is in fact registered; and there
    is even a web site at that name, which states circularly that the
    name is reserved for use in documentation and cannot be
    registered!)

6. Initial Registry

   The initial IANA "Special-Use Domain Names" registry shall contain
   entries for the private-address [RFC1918] reverse-mapping domains and
   for the existing Reserved Top Level DNS Names [RFC2606].

6.1. Domain Name Reservation Considerations for Private Addresses

   The private-address [RFC1918] reverse-mapping domains listed below,
   and any names falling within those domains, are Special-Use Domain
   Names:

     10.in-addr.arpa.   21.172.in-addr.arpa.   26.172.in-addr.arpa.
     16.172.in-addr.arpa.   22.172.in-addr.arpa.   27.172.in-addr.arpa.
     17.172.in-addr.arpa.   30.172.in-addr.arpa.   28.172.in-addr.arpa.
     18.172.in-addr.arpa.   23.172.in-addr.arpa.   29.172.in-addr.arpa.
     19.172.in-addr.arpa.   24.172.in-addr.arpa.   31.172.in-addr.arpa.
     20.172.in-addr.arpa.   25.172.in-addr.arpa.   168.192.in-addr.arpa.

   These domains, and any names falling within these domains, are
   special in the following ways:

   1. Users are free to use these names as they would any other
       reverse-mapping names. However, since there is no central
       authority responsible for use of private addresses, users SHOULD
       be aware that these names are likely to yield different results
       on different networks.

   2. Application software SHOULD NOT recognize these names as special,
       and SHOULD use these names as they would other reverse-mapping
       names.

   3. Name resolution APIs and libraries SHOULD NOT recognize these
       names as special and SHOULD NOT treat them differently. Name
       resolution APIs SHOULD send queries for these names to their
       configured caching DNS server(s).

   4. Caching DNS servers SHOULD recognize these names as special and
       SHOULD NOT, by default, attempt to look up NS records for them,
       or otherwise query authoritative DNS servers in an attempt to
       resolve these names. Instead, caching DNS servers SHOULD, by
       default, generate immediate (positive or negative) responses for
       all such queries. This is to avoid unnecessary load on the root
       name servers and other name servers. Caching DNS servers SHOULD
       offer a configuration option (disabled by default) to enable
       upstream resolution of such names, for use in private networks
       where private-address reverse-mapping names are known to be
       handled by an authoritative DNS server in said private network.

5. Authoritative DNS servers SHOULD recognize these names as special
    and SHOULD, by default, generate immediate negative responses for
    all such queries, unless explicitly configured by the
    administrator to give positive answers for private-address
    reverse-mapping names.

6. DNS server operators SHOULD, if they are using private addresses,
    configure their authoritative DNS servers to act as authoritative
    for these names.

7. DNS Registries/Registrars MUST NOT grant requests to register any
    of these names in the normal way to any person or entity. These
    names are reserved for use in private networks, and fall outside
    the set of names available for allocation by registries/
    registrars. Attempting to allocate one of these names as if it
    were a normal DNS domain name will probably not work as desired,
    for reasons 4, 5 and 6 above.

6.2. Domain Name Reservation Considerations for "test."

   The domain "test.", and any names falling within ".test.", are
   special in the following ways:

1. Users are free to use these test names as they would any other
    domain names. However, since there is no central authority
    responsible for use of test names, users SHOULD be aware that
    these names are likely to yield different results on different
    networks.

2. Application software SHOULD NOT recognize test names as special,
    and SHOULD use test names as they would other domain names.

3. Name resolution APIs and libraries SHOULD NOT recognize test
    names as special and SHOULD NOT treat them differently. Name
    resolution APIs SHOULD send queries for test names to their
    configured caching DNS server(s).

4. Caching DNS servers SHOULD recognize test names as special and
    SHOULD NOT, by default, attempt to look up NS records for them,
    or otherwise query authoritative DNS servers in an attempt to
    resolve test names. Instead, caching DNS servers SHOULD, by
    default, generate immediate negative responses for all such
    queries. This is to avoid unnecessary load on the root name
    servers and other name servers. Caching DNS servers SHOULD offer
    a configuration option (disabled by default) to enable upstream
    resolving of test names, for use in networks where test names are
    known to be handled by an authoritative DNS server in said
    private network.

   5. Authoritative DNS servers SHOULD recognize test names as special
       and SHOULD, by default, generate immediate negative responses for
       all such queries, unless explicitly configured by the
       administrator to give positive answers for test names.

   6. DNS server operators SHOULD, if they are using test names,
       configure their authoritative DNS servers to act as authoritative
       for test names.

   7. DNS Registries/Registrars MUST NOT grant requests to register
       test names in the normal way to any person or entity. Test names
       are reserved for use in private networks and fall outside the set
       of names available for allocation by registries/registrars.
       Attempting to allocate a test name as if it were a normal DNS
       domain name will probably not work as desired, for reasons 4, 5,
       and 6 above.

6.3. Domain Name Reservation Considerations for "localhost."

   The domain "localhost." and any names falling within ".localhost."
   are special in the following ways:

   1. Users are free to use localhost names as they would any other
       domain names. Users may assume that IPv4 and IPv6 address
       queries for localhost names will always resolve to the respective
       IP loopback address.

   2. Application software MAY recognize localhost names as special, or
       MAY pass them to name resolution APIs as they would for other
       domain names.

   3. Name resolution APIs and libraries SHOULD recognize localhost
       names as special and SHOULD always return the IP loopback address
       for address queries and negative responses for all other query
       types. Name resolution APIs SHOULD NOT send queries for
       localhost names to their configured caching DNS server(s).

   4. Caching DNS servers SHOULD recognize localhost names as special
       and SHOULD NOT attempt to look up NS records for them, or
       otherwise query authoritative DNS servers in an attempt to
       resolve localhost names. Instead, caching DNS servers SHOULD,
       for all such address queries, generate an immediate positive
       response giving the IP loopback address, and for all other query
       types, generate an immediate negative response. This is to avoid
       unnecessary load on the root name servers and other name servers.

5. Authoritative DNS servers SHOULD recognize localhost names as
    special and handle them as described above for caching DNS
    servers.

6. DNS server operators SHOULD be aware that the effective RDATA for
    localhost names is defined by protocol specification and cannot
    be modified by local configuration.

7. DNS Registries/Registrars MUST NOT grant requests to register
    localhost names in the normal way to any person or entity.
    Localhost names are defined by protocol specification and fall
    outside the set of names available for allocation by registries/
    registrars. Attempting to allocate a localhost name as if it
    were a normal DNS domain name will probably not work as desired,
    for reasons 2, 3, 4, and 5 above.

6.4. Domain Name Reservation Considerations for "invalid."

   The domain "invalid." and any names falling within ".invalid." are
   special in the ways listed below. In the text below, the term
   "invalid" is used in quotes to signify such names, as opposed to
   names that may be invalid for other reasons (e.g., being too long).

1. Users are free to use "invalid" names as they would any other
    domain names. Users MAY assume that queries for "invalid" names
    will always return NXDOMAIN responses.

2. Application software MAY recognize "invalid" names as special or
    MAY pass them to name resolution APIs as they would for other
    domain names.

3. Name resolution APIs and libraries SHOULD recognize "invalid"
    names as special and SHOULD always return immediate negative
    responses. Name resolution APIs SHOULD NOT send queries for
    "invalid" names to their configured caching DNS server(s).

4. Caching DNS servers SHOULD recognize "invalid" names as special
    and SHOULD NOT attempt to look up NS records for them, or
    otherwise query authoritative DNS servers in an attempt to
    resolve "invalid" names. Instead, caching DNS servers SHOULD
    generate immediate NXDOMAIN responses for all such queries. This
    is to avoid unnecessary load on the root name servers and other
    name servers.

5. Authoritative DNS servers SHOULD recognize "invalid" names as
    special and handle them as described above for caching DNS
    servers.

   6. DNS server operators SHOULD be aware that the effective RDATA for
       "invalid" names is defined by protocol specification to be
       nonexistent and cannot be modified by local configuration.

   7. DNS Registries/Registrars MUST NOT grant requests to register
       "invalid" names in the normal way to any person or entity. These
       "invalid" names are defined by protocol specification to be
       nonexistent, and they fall outside the set of names available for
       allocation by registries/registrars. Attempting to allocate a
       "invalid" name as if it were a normal DNS domain name will
       probably not work as desired, for reasons 2, 3, 4, and 5 above.

6.5. Domain Name Reservation Considerations for Example Domains

   The domains "example.", "example.com.", "example.net.",
   "example.org.", and any names falling within those domains, are
   special in the following ways:

   1. Users SHOULD understand that example names are reserved for use
       in documentation.

   2. Application software SHOULD NOT recognize example names as
       special and SHOULD use example names as they would other domain
       names.

   3. Name resolution APIs and libraries SHOULD NOT recognize example
       names as special and SHOULD NOT treat them differently. Name
       resolution APIs SHOULD send queries for example names to their
       configured caching DNS server(s).

   4. Caching DNS servers SHOULD NOT recognize example names as special
       and SHOULD resolve them normally.

   5. Authoritative DNS servers SHOULD NOT recognize example names as
       special.

   6. DNS server operators SHOULD be aware that example names are
       reserved for use in documentation.

   7. DNS Registries/Registrars MUST NOT grant requests to register
       example names in the normal way to any person or entity. All
       example names are registered in perpetuity to IANA:

        Domain Name: EXAMPLE.COM
        Registrar: RESERVED-INTERNET ASSIGNED NUMBERS AUTHORITY
        Whois Server: whois.iana.org
        Referral URL: http://res-dom.iana.org
        Name Server: A.IANA-SERVERS.NET
        Name Server: B.IANA-SERVERS.NET
        Status: clientDeleteProhibited
        Status: clientTransferProhibited
        Status: clientUpdateProhibited
        Updated Date: 26-mar-2004
        Creation Date: 14-aug-1995
        Expiration Date: 13-aug-2011

   IANA currently maintains a web server providing a web page explaining
   the purpose of example domains.

7. Security Considerations

   This document outlines the circumstances in which reserving a domain
   name for special use is appropriate, and the procedure for having
   that Special-Use Domain Name recorded by IANA. Any document
   requesting such a Special-Use Domain Name needs to contain an
   appropriate "Security Considerations" section which describes any
   security issues relevant to that special use.

8. IANA Considerations

   IANA has created a new registry of Special-Use Domain Names,
   initially populated with the private-address reverse-mapping domains
   and the Reserved Top Level DNS Names outlined above in Section 6.

   When IANA receives a request to record a new "Special-Use Domain
   Name", it should verify, in consultation with the IESG, that the IETF
   "Standards Action" or "IESG Approval" document [RFC5226] includes the
   required "Domain Name Reservation Considerations" section stating how
   the special meaning of this name affects the behavior of hardware,
   software, and humans in the seven categories. If IANA and the IESG
   determine that special handling of this "Special-Use Domain Name" is
   appropriate, IANA should record the Special-Use Domain Name, and a
   reference to the specification that documents it, in the registry.

9. References

9.1. Normative References

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

   [RFC1034]   Mockapetris, P., "Domain names - concepts and facilities",
               STD 13, RFC 1034, November 1987.

   [RFC1035]   Mockapetris, P., "Domain names - implementation and
               specification", STD 13, RFC 1035, November 1987.

   [RFC5226]   Narten, T. and H. Alvestrand, "Guidelines for Writing an
               IANA Considerations Section in RFCs", BCP 26, RFC 5226,
               May 2008.

9.2. Informative References

   [RFC1112]   Deering, S., "Host extensions for IP multicasting", STD 5,
               RFC 1112, August 1989.

   [RFC1918]   Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and
               E. Lear, "Address Allocation for Private Internets",
               BCP 5, RFC 1918, February 1996.

   [RFC2606]   Eastlake, D. and A. Panitz, "Reserved Top Level DNS
               Names", BCP 32, RFC 2606, June 1999.

   [RFC3927]   Cheshire, S., Aboba, B., and E. Guttman, "Dynamic
               Configuration of IPv4 Link-Local Addresses", RFC 3927,
               May 2005.

   [RFC4862]   Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless
               Address Autoconfiguration", RFC 4862, September 2007.

   [RFC5735]   Cotton, M. and L. Vegoda, "Special Use IPv4 Addresses",
               BCP 153, RFC 5735, January 2010.

   [RFC5771]   Cotton, M., Vegoda, L., and D. Meyer, "IANA Guidelines for
               IPv4 Multicast Address Assignments", BCP 51, RFC 5771,
               March 2010.

Authors' Addresses

    Stuart Cheshire
    Apple Inc.
    1 Infinite Loop
    Cupertino, CA 95014
    USA

    Phone: +1 408 974 3207
    EMail: cheshire@apple.com

    Marc Krochmal
    Apple Inc.
    1 Infinite Loop
    Cupertino, CA 95014
    USA

    Phone: +1 408 974 4368
    EMail: marc@apple.com