DNS Subdomain Policy (ampr.org)

Contents

Introduction

The ampr.org domain has never had a unified DNS domain naming scheme; as a result, records have been added inconsistently over the years, often with old / stale records not removed. As a result, the ampr.org DNS zone file currently has circa 50,000 domain records. This follows many years wherein users of 44Net were allowed to make their own entries. As of Q3 2024, the majority of these records are likely no longer in use, nor do the IPs associated with many of those domain names have a link back to a user's account IP resources in the AMPRNet Portal.

In order to solve this problem, ARDC needs to:

- Define which of these subdomains are currently in use, and by whom.
- Create a system that will prevent future bloating of the DNS zone file.
- Provide a clear unified DNS domain naming scheme.

This document outlines:

- How users may claim their DNS records, and
- An updated policy aimed to reduce future bloating of the zone file.

Following the date of implementation of the policy and official notice sent to 44Net mailing list (board approval date -TBD):

- Members will have a **total of 19.5 months** to claim their records.
    - Any records unclaimed after 45 days will be deactivated, but not deleted.
    - Any records still unclaimed following 18 months of deactivation, will be deleted.

Identifying DNS Ownership, Reducing Zone Size, and Stale Entry Clean-up

To help solve the ownership of DNS records problem, reduce the ampr.org zone size, and clean up the stale entries, the new Portal allows users and organizations to add and remove resource records directly. This will link their resource records to their accounts, where their other IP resources are also maintained.

With this new account / call sign / DNS association, any future stale records can then be cleaned up much more easily when accounts are closed.

In creating standardization and to reunite still live DNS resource records with their owners, a new DNS best practice naming scheme is implemented that relies on the user's call sign as the subdomain record, i.e., hostname.callsign.ampr.org.

Initially, to help alleviate the manual process of approving thousands of user ticket requests, any user with a verified subdomain based on their call sign will automatically have any existing resource records pulled into their account.

Concurrently, users will also be able to “Claim” orphaned DNS records that don’t follow the call sign subdomain record naming scheme into their accounts.

Following the date of implementation of the policy and official notice sent to 44Net mailing list (board approval date -TBD):

- Members will have a **total of 19.5 months** to claim their records.
    - Any records unclaimed after 45 days will be deactivated, but not deleted.
    - Any records still unclaimed following 18 months of deactivation, will be deleted.

Subdomain Format

Standard Naming Convention

- Subdomains should follow the format: `callsign.ampr.org`
- Second level subdomain names should be descriptive and meaningful; such as relevant to the amateur radio or digital communications project they represent.
    - e.g., `tower42.<callsign>.ampr.org`
    - **You can use:** lowercase letters, numbers, and hyphens (-) in second-level subdomains.
    - **The system will not allow:** Uppercase letters, spaces, underscores (_), or any other special characters.

Automatically Approved Subdomain Syntax

Automatically approved call sign subdomains are ones that match a pre-validated callsign associated with your account.

- e.g., if the user’s call sign is QZ9ABC, their subdomain of qz9abc.ampr.org will be automatically approved.
- Users are free to add any resource record to such subdomains.
- If a call sign is removed from an account, the user will be warned that any associated resource records will automatically be removed as well.

Second-Level Subdomains

Once a user has an approved subdomain, they can create up to 100 second-level subdomains, such as: `tower5.qz9abc.ampr.org.` For more details on how to format subdomain names, please refer to the Standard Naming Convention section above.

Non-Standard Naming Exceptions

In special cases, users may be allowed to use an alternative subdomain instead of a call sign, such as the name of an organization. These exceptions will be granted on a case-by-case basis.

- To request an exception, “Request a subdomain” on the portal as normal.
- When ham clubs apply for a subdomain exception, please provide justification for why you would prefer to use their club’s name in the ticket.
- **Exceptions reviewed by committee (See Exception Review Process)**

Review

Exception Review process

- The user makes a request for a subdomain via the Portal
- The request goes to a subcommittee consisting of three (3) members:
    - 1 TAC member
    - 1 regional coordinator (who may also be a TAC member)
    - 1 member of staff must (ideally a Portal administrator).
    - If possible, the active regional coordinator associated with the requesters region (in addition to regional coordinator committee).
- The subcommittee may decide through a unanimous written decision (email) or via a vote at a TAC meeting.

Subcommittee selection

- Subcommittee would be selected by the TAC at the beginning of their annual tenure
- For more information about our advisory committees: https://www.ardc.net/about/legal/advisory-committee-policy/

Periodic subdomain & policy review

- ARDC will conduct periodic reviews of subdomain usage to ensure compliance with the policy.
- Policy will be adjusted as needed by the committee.

Non-Standard Legacy Subdomains

Non-Standard Legacy Subdomains (“legacy subdomains”) are first-level subdomains created prior to the implementation of the new Portal on April 3, 2024, that use a format other than `callsign.ampr.org`. Though legacy subdomains without callsigns will be asked to choose callsign subdomain, legacy subdomain users may continue use of legacy subdomains, which must be claimed through the new portal. ARDC reserves the right to revoke access to legacy subdomains as described in the Revocation and Reserved Subdomain sections below.

To verify prior ownership, ARDC will confirm that the requested DNS entry points to the requester’s IP address block.

Gateway Operator's DNS Entries

A 44Net user may be acting as a Gateway Operator or Regional Coordinator for one or more subnets, wherein they are managing DNS entries on behalf of other users. Though unique user registration with the portal is highly encouraged, this practice is permissible, in line with this policy, as well as the terms as outlined in our End User License Agreement (EULA). Please note that these terms may include providing ARDC with basic information about the users in the subdomains and their associated DNS entries.

1. DNS Entry Management: Gateway Operators or Regional Coordinators must ensure that all DNS entries they manage comply with this DNS Subdomain Policy.

2. Responsibility: If claiming the DNS subdomains on behalf of their users that don't have portal accounts, the managing user (such as Gateway Operator or Regional Coordinator) takes full responsibility for all DNS entries they create and manage.

3. Record Keeping: Managers must maintain accurate records of the DNS entries they manage, including the associated callsigns and contact information for the end users. This information is to be provided to ARDC.

4. Compliance: All DNS entries, regardless of who manages them, must comply with this policy and the terms outlined in our End User License Agreement (EULA).

5. Claiming: Gateway operators wishing to claim DNS entries on behalf of their users must set up an Organization Account and pull these entries under the Organization umbrella instead of claiming the DNS entries under Gateway Operator or RC's personal accounts. These DNS claims should be done via Portal API, but if their DNS list is extensive, contact the portal admin, sending an agreed upon document format with information to be uploaded to Portal in bulk.

This approach allows for the continued management of DNS entries by Gateway Operators and Regional Coordinators while ensuring compliance with the overall DNS policy and encouraging individual user engagement with the portal system.

Revocation

ARDC reserves the right to revoke or reassign subdomains or individual DNS entries that:

- Violate policies
- Become inactive for extended periods
- Do no align with Amateur Radio philosophies or ARDC's mission and goals
- Pose security risks
- Cause infrastructure issues
- Have been brought to committee for review

Reserved Subdomains

- Certain subdomains may be reserved for ARDC's official use, such as www, mail, portal, etc.
- Initial reservation list to be created by TAC & Staff.

Reverse DNS

- The system automatically generates a PTR record in the reverse zone file for every A record in the forward zone file that points to a 44Net IP address.
- Reverse DNS delegation is possible, upon request, for assignments of /24 or larger.
    - This can be requested by raising a "Help with DNS" support ticket on the portal.

Zone Transfers

- For now, it is possible for users to carry out zone transfers from the primary nameserver (ns.ardc.net) if the source IP is within 44Net.
    - Users should be encouraged to move away from this practice and zone transfers eventually deprecated in favor of using the portal API.
    - If zone transfer functionality is ultimately found to be beneficial and a wanted feature by the community, a separate machine should be set up that sources zone records off the primary nameserver, which is then used to offer zone transfers.

Security

- Subdomain owners are responsible for maintaining the security of any services hosted within their subdomains.
- ARDC reserves the right to suspend or terminate subdomains such as those that pose security or infrastructure risks

Technical Requirements

- DNS Management
    - ARDC will maintain the primary & secondary DNS servers
- Subdomain owners are granted portal access to manage specific records associated with their accounts
    - E.g. “A” , “CNAME” etc from their subdomain

Glossary

- **DNS (Domain Name System):** is a hierarchical and distributed name service that provides a naming system for computers, services, and other resources on the Internet or other Internet Protocol (IP) networks.
- **Domain names:** is a string that identifies a realm of administrative autonomy, authority or control. Domain names are often used to identify services provided through the Internet, such as websites, email services and more.
- **Top-level domains (TLDs)**: are root domains like: .com, .org, .net, etc.
- **Second-level domains (SLDs):** are like “ampr” in “ampr.org” (under the TLDs such as “.org”)
- **Subdomains (SD):** like callsign.ampr.org are under the SLDs like ampr.org
- **Second-level Subdomains (Sub-Subdomains):** are like tower5.qz9abc.ampr.org
- **Resource Records (RRs):** Resource records are discrete items of data relating to a specific type of record, that the DNS server uses to resolve name resolution queries. Common resource records are “A”, “CNAME”, “MX” and “NS” (see below).
- **Zone file:** This is a file that contains the resource records for a domain name for which the DNS server is authoritative. Only records for one domain are contained within a particular zone file.
- **Authoritative name server:** A DNS name server that has authority to respond to name request lookups for a particular domain name.
- **Primary name server:** This is the authoritative name server for a domain name that is the “source of truth” for all resource records belonging to the domain name.
- **Secondary name server:** This is an authoritative nameserver for a domain name that responds to name request lookups for a particular domain, but which obtains its resource records from a Primary name server. For redundancy a domain name will often have multiple secondary name servers, on different networks, ideally geographically dispersed.
- **Recursive name server:** These servers are used by computers to lookup resource records. Typically (but not always), they are open to the public, and they will cache lookups (according to the TTL) to speed up subsequent lookups. Recursive name servers are typically not authoritative and therefore hold no intrinsic resource records themselves; instead, they will do the “leg work” of looking up a resource record for an end user. Some well known public recursive name servers are Cloudflare’s 1.1.1.1, Quad9’s 9.9.9.9 and Google’s 8.8.8.8 and 8.8.4.4
- **TTL**: Time To Live - how long a recursive name server should cache a resource record for, before it removes it from its cache.