SOFTWARE REQUIREMENTS SPECIFICATION
“THE PORTAL”

Developed by:

ARDC Technical Advisory (TAC) Members: Zachary Seguin - *VA3ZTS*, Tim Pozar - *KC6GNJ*,
Rob Janssen - *PE1CHL*, and Adam Lewis - *KC7GDY*

ARDC IT Lead: Chris Smith - *G1FEF*

Reviewed by:

TAC Members: Pierre Martel - *VE2PF*, Chip Eckhardt - *W9OQI*

ARDC Executive Director: Rosy Schechter - *KJ7RYV*

Sept. 2022

1. Introduction

1.1. Purpose

This document describes the software requirements and specification for a Portal for ARDC members and administrators to request and manage assignments of IP address space within the 44net address space, manage forward and reverse DNS for the assigned address space and to manage gateways into the network.

This document is intended for developers of the Portal software, the Board of Directors and the Technical Advisory Committee (TAC) of Amateur Radio Digital Communications (ARDC).

1.2. Scope

The Portal will be a web application from ARDC to enable the management of the 44net address space and entry points into the network. The Portal will not offer connectivity to the network; that would be offered through points of presence (PoPs).

1.3. Definitions, Acronyms and Abbreviations

44net	44.0.0.0/9, 44.128.0.0/10

Allocation	One or more consecutive IP addresses that are reserved for a use case; all addresses under an allocation may not be actively in use
Assignment	One or more consecutive IP addresses assigned to a group or member for use.
Gateway	An endpoint which accepts traffic destined to one or more assignments

Abbreviations:

BGP	Border Gateway Protocol.
LOA	Letter of Authorization. A document which authorizes a member to arrange BGP announcement of an assignment for a specific time period.
LoT	Level of Trust - integer value indicating how trustworthy a member is.
RBAC	Role Based Access Control.
UI	User Interface - The web pages presented to the user that they may interact with.

1.4. References

1.4.1. Chris' initial proposal: https://gitlab.ardc.net/ardc/technology/-/blob/main/proposals/portal/Software-Development.txt

1.4.2. Existing portal: https://portal.ampr.org/

1.4.3. New portal: https://new.portal.ampr.org/

1.5. Overview

2. Overall Description

2.1. Product perspective & Features

At a high level, the Portal is intended to provide ARDC and its members with the ability to manage allocations of 44net address space.

2.1.1. The Portal will be released as open source

2.1.1.1. As soon as a functional version is available, code will be published in a public repository

2.1.1.2. Additional development work will be completed in alignment with open source best practices.

2.1.1.3. The project will be under the "GNU General Public License v3.0 or later" license.[1]

[1] https://www.gnu.org/licenses/gpl-3.0-standalone.html

2.1.2. The UI should be easy to use by people with a technical interest but not necessarily an expert.

2.1.2.1. The UI should follow as many accessibility standards as possible:

2.1.3. Interface should be internationalized;

2.1.4. Compatible with modern browsers;

2.1.5. Support sight-impaired clients.

2.1.5.1. Annotated images

2.1.6. Should be extensible, to accommodate new features or localization;

2.1.7. Should have an API - when this is finished, members should be able to manage their resources through both the web interface and the API;

2.1.8. Access to functionality is controlled through RBAC.

2.1.9. Use Cases

2.1.9.1. Members

2.1.9.1.1. Requesting assignment

2.1.9.1.2. Managing assignment

2.1.9.1.2.1. DNS - Resource records

2.1.9.1.2.2. rDNS (automatic or based on LoT)

2.1.9.1.2.3. IPIP Tunnels, ideally to be extended to PoPs

2.1.9.1.3. Submit a ticket

2.1.9.1.3.1. Bugs

2.1.9.1.3.2. Assignment request

2.1.9.1.3.3. Validation request

2.1.9.1.3.4. Includes notification module

2.1.9.2. Administrators

2.1.9.2.1. Ticketing system

2.1.9.2.1.1. Accessible by a group of administrators

2.1.9.2.1.2. Needs to handle development vs help desk tasks.

2.1.9.2.1.2.1. Development tasks need to be tied to internal ARDC project management system.

2.1.9.2.2. Admin removal of members

2.2. User characteristics

2.2.1. There will be multiple types of accounts on the portal based on the member's LoT and RBAC for example:

2.2.1.1. Members:

2.2.1.1.1. Members of the Portal will be licensed Amateur Radio operators from around the world.

2.2.1.1.1.1. Members of the Portal will need to have their callsign verified.

2.2.1.1.2. Members of the Portal are worldwide, and understand a variety of languages.

2.2.1.1.3. Members of the Portal will have a variety of knowledge, ranging from no knowledge of networking to advanced knowledge of networking.

2.2.1.2. Address Coordinator (“Coordinator”):

2.2.1.2.1. Address Coordinators will be knowledgeable in networking, ARDC policies and are familiar with the operations of the intended use of the allocations they are responsible for.

2.2.1.3. BGP Coordinator

2.2.1.3.1. BGP Coordinators will be knowledgeable in networking and BGP, as well as ARDC policy regarding assignment of BGP authorized subnets.

2.2.1.4. DNS Coordinator

2.2.1.4.1. DNS Coordinators are knowledgeable in the management of DNS and ARDC policies around such.

2.2.1.5. Portal Administrator

2.2.1.5.1. Administrators of the Portal will have an advanced knowledge of networking, and the policies of ARDC for management of the address space. Administrators have full Address Coordinator privileges.

2.3. Assumptions and dependencies

2.3.1. The portal’s requirements may change based on the outcomes of the current 44Net assessment. Therefore, this document is written based on the current needs and will need to be revisited based on the outcomes of the assessment.

3. Specific requirements

3.1. External interface requirements

3.1.1. **Web application**
Primary user interface in how members will interact with the portal.

3.1.2. **API**
External systems/clients can interact with the Portal via a RESTful JSON API.

3.1.3. **ampr.org forward DNS zone**
Information from the Portal will be used to generate the ampr.org forward DNS zone. These records will be based on information provided by members for the IP addresses within their allocations.

3.1.4. **Reverse DNS records**
Information from the Portal will be used to generate the reverse DNS records for IP addresses within 44Net.

3.1.5. Gateway

Members may add their public IP address and link their assigned subnet(s) to their gateway to participate in the IPIP mesh.

3.1.6. ENCAP

Information from the Portal will be used to generate the encap file, which will be available via the API, via FTP and automatically populated to the 44RIP daemon running on the UCSD gateway server.

3.2. Functional requirements

3.2.1. Accounts

3.2.1.1. **Register.** Upon accessing the Portal, members are presented the option to register for an account, log in with their existing account, as well as being able to request a password reset or username reminder.

3.2.1.2. **Update PII.** Members will be permitted to update their personal information, including their name, email address, phone number, physical address and amateur radio callsign(s).

3.2.1.3. **Modify email.** Upon initial registration, and upon a user modifying their own email address, a confirmation will be sent to the user's new email address with a validation code. The user's email will be validated only once the user has clicked/entered the validation code. If a user's email has been changed, a notification email is to be sent to the user's previous email address.

3.2.1.4. **Cell conf.** Upon initial registration, and upon a user modifying their cellphone number, a confirmation will be sent to the user's new cellphone number with a validation code. The user's cellphone number will be validated only once the user has entered the validation code.

3.2.1.5. **Unver. Update.** Users with an unverified email address will be provided with the ability to update their own profile or delete their account. Any other access will be read-only.

3.2.1.6. **Unver. Scrubbing.** Accounts created and not verified will be scrubbed after ___ days.

3.2.1.7. **Notification selection.** A user can select which methods of notification (email, SMS message) are enabled for their account.

3.2.1.8. **Notification display.** The portal will also display active notifications on the homepage after logging in. Members can mark notifications as read as well as view/delete old notifications.

3.2.1.9. **2FA.** Members can enable two factor authentication on their account. At a minimum, email, SMS, TOTP and WebAuthn should be supported.

3.2.1.10. **Add maidenhead.** Members must add a maidenhead locator to their profile. In setting the maidenhead locator, members will be presented with a map.

3.2.1.11. **Auto suspension.** Accounts with no activity for a defined period will be automatically suspended at a time frame defined by ARDC policy. Several reminder notices should be sent before suspension to the user’s selected methods of communication.

3.2.1.12. **Admin suspension.** An administrator can suspend an account at any time.

3.2.1.13. **Account suspension.** When an account is suspended, all assignments, DNS entries and gateways are disabled but not removed from the system.

3.2.1.14. **Suspension notification.** Administrators will be notified of accounts which are automatically suspended due to ARDC policy, by their selected notification methods, to review the accounts assignments, DNS entries and gateways for deletion.

3.2.1.15. **Account deletion.** When an account is deleted, all assignments, DNS entries and gateways for that account are removed.

3.2.1.16. **LoT.** A user account contains a Level of Trust associated with it.

3.2.1.17. **Validation request.** A user can request validation, using methods to be defined by ARDC, to increase their Level of Trust. Upon submitting a request, Level of Trust Administrators are notified of the request via their selected notification methods.

3.2.1.18. **Validation record.** Level of Trust Administrator, after performing the validation process, will record a “Validation succeeded” or “Validation failed” result. The user will be informed of the result via their selected notification methods.

3.2.2. Allocations

3.2.2.1. **Division.** The 44net address space can be divided into one or more allocations.

3.2.2.2. **Assignment**. Each allocation may be assigned one or more address coordinator(s), or may be assigned to the standard pool.

3.2.2.3. **Subassignment.** Each allocation may have further sub-allocations.

3.2.3. Assignments Features

3.2.3.1. **List Assignments.** Members are presented with a list of their assignments.

3.2.3.2. **Assignments list.** Administrators are presented with a list of all assignments.

3.2.3.3. **Assignments view.** The address coordinator(s) can view all assignments within their allocation.

3.2.3.4. **Add comments.** A coordinator and/or an administrator may add additional comments to an assignment. Only coordinators and administrators may see those comments.

3.2.3.5. **CSV export.** An export function exists to output all assignments as a CSV file.

3.2.4. Assignment Request Workflow

3.2.4.1. **Request.** Members can submit a request for a new assignment, this will take the form of a ticket. A request for a new assignment will include the target allocation, the desired network size and a description of the intended use of the assignment.

3.2.4.2. **Notified.** Upon receiving an assignment request, the address coordinators for the target allocation will be notified of the request via the notification methods selected for their accounts.

3.2.4.3. **Ownership.** One address coordinator must take ownership of the request.

3.2.4.4. **Escalation**. If no-one takes ownership within a defined time period, repeat notifications are sent to the address coordinators. If, after 2 repeat notifications, a request is still pending ownership then it is automatically escalated to the administrators.

3.2.4.5. **Request Info.** When reviewing an assignment request, the coordinator can request additional information from the requestor. When a request is made, a notification is sent to the requestor via their selected notification methods.

3.2.4.6. **Response.** When additional information is requested, the requestor will be able to provide their response. Upon providing a response, a notification is sent to the assigned address coordinator via their selected notification methods.

3.2.4.7. **Display.** Requests and responses are displayed within the assignment request.

3.2.4.8. **Approval Notification.** Upon a coordinator approving an assignment, the requestor will be notified of the assignment via their selected notification methods. The assignment is recorded in the target allocation and the request is closed.

3.2.4.9. **Rejection Notification.** Upon a coordinator rejecting an assignment, the requestor will be notified of the decision via their selected notification methods. The request is then closed.

3.2.4.10. **Appeals.** A requester can appeal the decision to reject an assignment. Upon submitting an appeal, the request is re-opened, assigned to a defined person or role based on ARDC policy for review. The assigned person is notified via their selected notification methods.

3.2.4.11. **Final closure.** An assignment request that was closed following an appeal cannot be appealed again.

3.2.4.12. **Reminders.** If an address coordinator does not action an assignment request (request additional information or approve/reject the request) that is not pending further information from the requestor within a defined time period, a reminder notification is sent to them via their selected notification methods. If, after 2 reminders, the request is not actioned then the other address coordinators are notified. If there are no other address coordinators in the target allocation, then the request is escalated to the administrators.

3.2.4.13. **Second reminders.** If a requester has not responded to a request for additional information within a defined time period, then a reminder notification is sent to the requestor via their selected notification methods. If, after 2 notifications, the requestor has not responded then the request is automatically closed and a notification of such is sent to the requestor via their selected notification methods.

3.2.4.14. **View history.** Address coordinators and administrators can see a history of all assignment requests, whether accepted or closed, within an allocation.

3.2.5. BGP Assignments

3.2.5.1. **BGP permit.** BGP assignment requests are only permitted in allocations authorized for BGP use.

3.2.5.2. **Additional info.** When submitting an assignment request in a BGP allocation, the requestor will be prompted for the additional information that is required. The request will then follow the normal address assignment process.

3.2.5.3. **Download LOA.** Members with an approved BGP assignment will be able to download a LOA for that assignment.

3.2.5.4. **RADB objects** need to be created and propagated.

3.2.6. DNS

3.2.6.1. **DNS manage.** Members will be able to manage DNS resource records for all addresses within their assignments, which must be in the format of <callsign>.ampr.org or *.<callsign>.ampr.org.

3.2.6.2. **Subdomain assignment.** Members are assigned a subdomain of <callsign>.ampr.org, for which they can create any resource records.

3.2.6.3. **Transfer option.** Based on a user’s callsign, existing DNS records will populate giving them an option to claim and transfer the records over to the new portal as part of the migration process.

3.2.6.4. **rDNS PTR record.** PTR records pointing to other subdomains, or DNS entries in other subdomains, must be approved by a DNS administrator.

3.2.6.5. **Add record types.** Able to add Record Types: A, AAAA, CNAME, TXT, MX, SRV, DNSKEY, DS, LOC, PTR, NS etc.

3.2.6.5.1. **Record help.** Provide help text for more difficult entries like SRV, DNSKEY, DS, LOC etc.

3.2.6.6. **RDNS request.** Members with a BGP IPv4 assignment of /24 or larger can submit a request to have the reverse DNS servers delegated to their own DNS servers.

3.2.6.7. **RDNS notification.** Upon a reverse DNS delegation request, the DNS administrators will be notified via their selected notification method(s) and one of them must take ownership of the request.

3.2.6.8. **RDNS approval/rejection.** The DNS administrators can approve or reject a reverse DNS delegation request. Upon a decision being made by a DNS administrator, the requestor will be notified of the decision via their selected notification method(s).

3.2.7. Gateways

3.2.7.1. **Gateway type list.** Users are presented with a list of gateway types.

3.2.7.2. **Gateway registration list.** Users are presented with a list of their gateways registered within a gateway type.

3.2.7.3. **Gateway registration.** Users are able to register a new gateway within a gateway type, and they will be asked for:

- 3.2.7.3.1. **Assignment routing.** The assignment(s) to be routed to this gateway
- 3.2.7.3.2. **Gateway info.** Any additional information required by the gateway type (e.g., IP address, credentials, etc.)

3.2.7.4. **Gateway approval.** If a gateway type requires administrator approval, then the administrator(s) are notified of the new request via their selected notification method(s).

3.2.7.5. **Route requests.** Users are able to request that another user route their assignment(s) through another user's gateway.

3.2.7.6. **Gateway edit.** Users should be able to edit or delete their gateway.

3.3. Performance requirements

3.3.1. The Portal must support 30 regular concurrent users, and 100 peak concurrent users.

3.4. Design constraints

3.4.1. Legal requirements

3.4.1.1. The portal must meet the requirements of the Americans with Disabilities Act (ADA)[2] for website accessibility and comply with the WCAG standard.

3.4.1.2. General Data Protection Regulation (GDPR)

3.4.1.3. ARDC Privacy Policy (pending) on handling Personal Identifiable Information (PII) and requests from external persons and/or agencies.

3.5. Quality attributes

[2] https://www.accessibilitychecker.org/guides/ada-compliance/

3.5.1. At the beginning of any process (e.g., registration, requesting an assignment, etc), information is presented to the user which outlines the process steps, the prerequisites including any required documentation, and sets the user’s expectations (e.g., estimated processing time).

3.6. Software system attributes

3.6.1. Reliability

3.6.1.1. The frequency of non-scheduled full portal outages would not exceed x outages per month, as defined through a feasibility study.

3.6.2. Availability

3.6.2.1. Need 99.9% of uptime over 1 year

3.6.3. Security

3.6.3.1. Follow OWASP[3] guidelines

3.6.3.2. The Portal must be available over a currently acceptable level of TLS.

3.6.3.3. The Portal must implement login security to prevent brute force attacks on user accounts.

3.6.3.4. The Portal’s infrastructure will follow industry best practices.

3.6.4. Maintainability

3.6.4.1. Written in a modular form that allows addition of new (sub) functions.

3.6.4.2. Written using modern programming language(s) and frameworks that are easily maintainable by a wide variety of developers.

3.6.4.2.1. Preference for modern languages such as Python, JavaScript, HTML5

3.6.4.2.2. All code should be clean, with clear comments for every module as well as a README.md with inputs, outputs, expected behavior, and dependencies

~~3.6.4.3. Maintenance of any part of the system will not affect the overall functionality of the service.~~

3.6.4.4. Developer-facing documentation to be provided, as well as reviewed by ARDC’s Technical Director prior to publication. Documentation may need to be updated during the process of implementation and following release.

3.6.5. Portability*-

3.6.5.1. Should be supportable by multiple operating systems and deployment environments.

3.6.5.2. Should work with multiple browsers across multiple devices, including mobile devices.

[3] https://owasp.org/www-project-web-security-testing-guide/stable/