



DNSMuxTM

Geographically Separated Site/Server Traffic Management

User Guide

Version 3.1.x

Copyright

Copyright © 2006 CAI Networks, Inc. All Rights Reserved. Printed in USA.

The information contained in this document is the property of CAI Networks, Inc. Neither receipt nor possession hereof confers or transfers any right to reproduce or disclose any part of the contents hereof, without the prior written consent of CAI Networks, Inc. No patent liability is assumed, however, with respect to the use of the information contained herein.

Trademarks

DNSMux and WebMux are trademarks of CAI Networks, Inc.

All other product names and logos are trade or service marks of their respective companies.

Disclaimer

The instructions and descriptions contained in this manual were accurate at the time of printing. However, succeeding products and manuals are subject to change without notice. Therefore, CAI Networks, Inc. assumes no liability for damages incurred directly or indirectly from errors, omissions, or discrepancies between the product and this manual.

CAI Networks, Inc.
1715 Wilshire Ave., Suite 719
Santa Ana, CA 92705

www.cainetworks.com

Table Of Contents

Table Of Contents.....	1
Introduction to DNSMux	4
Domain Name System Basics.....	4
DNSMux Overview	4
Configuration Guidelines	7
Introduction.....	7
Major Steps and Domain NS Record.....	7
Configuration Master and Propagation	7
Propagation Usage	8
Delayed Application	8
Caching	8
Default Cache Duration (TTL)	9
External Caches	9
Load Balancing IP Servers.....	10
Health-Checking IP Servers.....	12
Failover.....	12
Failure of an IP Server Site	13
Failure of a DNSMux.....	13
Preparing for DNSMux Deployment	14
Introduction.....	14
Overview	14
Determine Network Addresses.....	14
Determine Relative Performance of IP Servers	15
Determine Technical Contacts and Their Email Addresses.....	15
Reduce TTL Value	15
Using the Front Panel Controls	16
Introduction.....	16
Layout and Controls	16
Control Panel Functions	17
Security Lockout.....	17
Control Panel Tasks	17
Unlocking the Control Panel.....	17
Determining Throughput.....	18
Setting Network Addresses	18
Disabling the Internal Firewall	19
Rebooting the DNSMux Unit	19
Restoring the Factory Defaults.....	19
Adjusting the Brightness of the LCD	20

Configuring DNSMux.....	21
Introduction.....	21
Configuring Multiple DNSMuxes From A Single Point	21
Configuration Overview.....	21
Initial Setup of a New DNSMux.....	21
Set The IP Address, Netmask, and Gateway Via The Control Panel	22
Ports Utilized by DNSMux	22
Accessing the DNSMux Screens	22
Using The DNSMux Screens	23
Propagation to Other DNSMuxes.....	23
Basic Screen	24
Network.....	24
Time.....	25
Email.....	26
Logging.....	26
Nameservers	27
Security Screen	27
Passwords	27
Control Panel PIN.....	28
Allowed hosts.....	28
Firewall	29
Zones Screen	29
Zone.....	31
FQDN SOA NS.....	31
Delayed Application.....	32
Dynamic Hosts	32
Static records.....	32
Nameservers	33
Site Screen (sub-screen of Zone screen)	34
Servers (sites).....	34
Criteria	35
Firmware Screen	36
Status Screen.....	36
DNSMux Appliance Layout.....	38
Overview	38
Front View	38
Rear View	38
Control Panel LCD Values.....	40
Troubleshooting and Recovery.....	42
Guidelines	42
Ensure you are working on the correct DNSMux.....	42
DNSMux notifications.....	42
Failed/recovered sever.....	43
Failed/recovered DNSMux	43
Firmware version.....	43
Rescue Mode	44

Introduction to DNSMux

Domain Name System Basics

The domain name system's primary function is to convert domain names into IP addresses, needed to connect to Internet services. DNS has numerous secondary uses, for example helping route email.

All of DNS's duties are undertaken by so-called DNS name servers, which are deployed throughout the Internet, using a simple request-answer paradigm. Clients query their ISPs' DNS server, which in turn query an authoritative name server with a domain name, and an answer is given that typically consists of an IP address of the server in the domain name.

DNSMux Overview

DNSMux is an intelligent DNS nameserver, providing an enhanced alternative to ordinary name servers.

Its enhanced features include high-performance and high-availability capabilities to ensure that users are always targeted to servers that are up and running and providing good performance, as well as checking the server's availability and fail-over function to not resolve the down site server addresses.

Peak performance is accomplished via load balancing, whereby DNSMux could select from among multiple content-identical servers the ones that are offering the best performance at any given moment.

Peak uptime is accomplished via health monitoring and failover, whereby DNSMux will monitor the health of each content server and report those that are unresponsive (either because certain processes are inoperative or because a server is down) thus only resolve the available servers' IP addresses.

User can have two or more sites that geographically separated to fail over from each other. By proper settings, DNSMuxes will resolve one location with user defined fail-over sequences that also passed health checking.

At least two DNSMuxes should be deployed for each domain on a different site to accomplish the fail-over detection and function. Multiple DNSMuxes can be deployed in a cluster to efficiently serve users worldwide by automatically targeting them to the servers with the closest geographical proximity

The first step in the DNSMux configuration process of is to use the front-panel controls to set the IP address, netmask, and gateway for one or both of DNSMux's Ethernet interfaces

(the second interface is optional and is intended to connect the DNSMux unit to a private network for management purposes).

Once the DNSMux unit is network-accessible, DNSMux's browser-based configuration interface is used to set host-specific details for each DNSMux. Configurations settings can be automatically propagated to all the DNSMuxes in the cluster so that any can stand in for any other in a failover scenario.

The settings specific to each DNSMux nameserver include:

- The hostname, company name, IP address, subnet mask, and gateway IP address
- Optionally, the IP address and subnet mask of a private network associated with the DNSMux nameserver
- Optionally, the NTP server from which the DNSMux will get the current time
- Optionally, the current time and time zone
- The hostname or IP address of the outgoing email server
- The email address of the technical contact for notifications related to this DNSMux nameserver
- The hostname or IP address of the syslog server to receive logged events
- Which categories of events to log, selected from a drop-down list
- The hostnames or IP addresses of other DNSMux nameservers in this cluster

Each zone within the domain needs to be setup with their related configurations. The settings for each zone include SOA records:

- The zone name (e.g., myzone.com)
- The email address of the technical contract person for the zone
- The default cache time (TTL, or Time To Live), in seconds, for various DNS caches
- The standing time that all DNSMux nameservers in the cluster should activate the configuration changes
- The dynamic hosts for the zone and their settings
- The static DNS records for the zone
- The nameservers to advertise for the zone, selected with checkboxes

Within each zone, all the hosts (e.g. "www", "ftp", "mail", etc) that comprise the zone must be set up.

The settings for each host includes:

- The host name, e.g. "www", "ftp", "mail", etc.
- The servers, by hostname or IP address, which contain the content provided by the host. (They need not be content-identical, because regions will take care of the differing content and who to provide it to)
- The “weight” to assign to each server, based on inherent performance power or fail-over sequence
- Which characteristics should be taken into account for load balancing (weight and/or health), whether the proximity between the client and each server should be considered for performance optimization, and/or whether a round robin scheme should be used
- Which installed protocol(s) to exercise for regular health-checking

There is also a Security screen for:

- Changing the passwords for the Administrator and Observer users
- Specifying which servers, by hostname or IP address, are allowed access to manage the DNSMuxes
- Specifying which other DNSMux nameservers to accept propagated configurations from
- Deny certain IP address access any DNSMux functions, including the DNS functions
- Disabling DNSMux’s internal firewall

An optional configuration can then be set for whether users should be targeted by proximity (to the hosts most closely located to them). Such targeting is done automatically by DNSMux with no configuration required, except an indication of whether users should be restricted to their home regions even if content-identical servers exist in other regions which may offer better performance.

Proximity determinations are implied by the automatic determination of the geographical locations of servers and users based on their respective IP addresses.¹

Once all DNSMuxes, are properly configured, they will:

- Perform address resolution and other functionality expected of any DNS nameserver
- Target users to the best performing servers, within restrictions imposed by proximity and affinity rules
- Direct users away from failed servers

¹ User IP addresses are determined by the geographical locations of their local DNS name servers

Configuration Guidelines

Introduction

In setting up a DNSMux cluster, there are a number of factors to consider:

- Which DNSMux(es) will server as “configuration master(s)”
- The default time of day to post queued configuration changes
- The default cache duration (Time To Live, or TTL) to impose on external caches
- Health-checking methods
- Load balancing methods
- Failover strategy

Each of these is described in the following paragraphs.

Major Steps and Domain NS Record

The first thing to configure is to use push button to set IP address. Once the IP address setup and can be reached, DNSMux can be configured using browser from that point on. Please reference Chapter 4 for the details.

To make DNSMux working properly, first fill up the Basic screen. Make sure enter all the DNSMuxes into the bottom propagation list line. They can be IP addresses, or host-name.domain-name.com format. Next one will add domain for DNSMux to manage. The information on the screen is very important. Leave the mouse cursor on each field will get prompt for the proper format of the entry. Before leaving that page, please make sure add NS record, first for the DNSMux itself, and other DNSMux into the DNSMuxes field separated by comma. Please reference Chapter 5 for details.

To enable DNSMuxes working properly, it will also involve having an existing DNS server entering NS record for their IP addresses. After 24 to 48 hours, the NS records being populated over the Internet, then you can add DNSMux to the domain record as its domain NS records to replace the existing NS records.

Configuration Master and Propagation

In configuring the various DNSMuxes in a cluster, it is not necessary to configure each one individually: DNSMux is capable of propagating its configuration to others. It is therefore recommended that one DNSMux be designated as a “configuration master” and set the configurations common to all DNSMuxes in the cluster there. After testing the configuration, you can instruct DNSMux to propagate the settings to the other DNSMuxes in the cluster.

A primary reason for propagation is to facilitate failover of a DNSMux unit. Each DNSMux in a cluster contains the configurations of all the other DNSMuxes in the cluster, so that if any DNSMux in the cluster fails any other can stand in for it.

DNSMux's propagation feature propagates the following settings between servers:

- Settings from the Zones screen
- Settings from the Hosts subscreen of the Zones screen
- List of DNSMux nameservers from the Basic screen

These settings are described in the following chapters.

To facilitate configuration propagation, each "configuration master" must be listed in the Propagation field in the Security screen on all the other DNSMuxes in the cluster.

Propagation Usage

Configuration set in the browser-based configurator are queued to be propagated to other DNSMuxes in the cluster. An information bar appears beneath the header indicating that changes have been made but not yet propagated. Changes are explicitly propagated by hitting the "Propagate" button in the information bar.

Upon hitting the "Propagate" button, all changes are immediately propagated to other DNSMuxes but not necessarily activated on any DNSMux as each unit has the capability of deferring configuration changes to a specified time. Whether changes are activated immediately or at a later time is governed by DNSMux's "Delayed Application" feature.

Delayed Application

Configuration changes made for a zone can be activated immediately or deferred to a particular time of day. If the latter, DNSMux will defer any configuration activations until that time. Such "standing time" is specified in the Delayed Application section of the Zone screen in the GUI configurator.

The Delayed Activations feature applies to both configuration changes made directly to a DNSMux, as well as via propagation.

Caching

Caching is an important and potentially problematic issue that needs to be taken into account when determining configuration strategies for DNSMux.

A key operational premise of DNS is that DNS name servers are capable of caching DNS answers (i.e., the IP address for a hostname) so that, as a matter of efficiency, clients do not need to request DNS resolutions for every DNS request. This was beneficial behavior when Internet connections were slow and DNS records didn't often change. Traditional DNS name servers would keep resolutions cached for hours or days.

Unlike traditional name servers, DNSMux is more dynamic: users are directed on the fly to the most appropriate server based on ever-changing conditions. It is therefore recommended that the configured TTL value be set short in order to prevent stale resolutions remaining in cache. The shorter the cache time, the more often the client needs to send a query to the authoritative name server and wait for an answer, which typically take a few tenths of a second. Balancing these two priorities is a local decision.

Default Cache Duration (TTL)

DNS answers have an associated value that informs DNS clients and caching DNS servers how long until this answer expires. Clients and caching name servers remember this answer until it expires and then *should* resend the query the next time it is asked once the cache duration has lapsed.

The cache duration, known as TTL (Time To Live) in DNS terminology, is specified in seconds for each zone via the “Default Cache Time” setting in the top section of the Zones screen. If the default cache time is not specified, 15 seconds is imposed. (See the previous section for recommendations on setting the cache duration.)

It is recommended that a relatively short TTL value be imposed so that DNSMux has the most control of where to send users and the most information about the geographic concentration of users.

External Caches

For a Windows client, there are typically three caches that can impede the desired DNS operation, and DNSMux has little or no control over them. These three caches and their behavior are described below.

ISP's Nameserver Cache

Clients normally don't contact authoritative nameservers directly, but use their ISP's DNS name server in order to translate hostnames into their corresponding IP addresses. The ISP's DNS server caches answers and serves them to clients when they make such queries.

When the client queries its ISP's DNS server, the server first looks in its cache for the answer. If the ISP's DNS server does not know the answer it in turn asks another DNS server (which also caches) or the authoritative nameserver (in this case, a DNSMux) directly. Entries in the cache should be deleted when they expire, as suggested by the TTL value. Be forewarned, however, that many ISPs have configured their name servers to ignore the TTL value and keep entries in their cache for up to three days.

Windows

Before querying the client's ISP's nameserver to resolve a hostname, Windows first checks its internal cache for answers. If it knows the answer (from a previous query) and that answer has not yet expired, Windows uses the IP address from the cache instead of querying the local DNS server.

The Windows cache respects the TTL supplied by the ISP's name server, so each answer will expire when the TTL has lapsed. To flush the Windows cache, reboot the machine or run:

```
flushdns.exe
```

Apple Mac OS X

All DNS lookups under OS X go through the lookup cache. This cache respects the TTL set by the nameserver, and unused entries are forgotten after 12 hours. To flush the lookup cache, login as administrator and from the Terminal run:

```
mycomputer# lookupd -flushcache
```

If the client is connecting to your website with a browser, there is another cache to contend with. Browsers rely upon the operating system to resolve domain names, but they do not resend the request on every visit to a site. The durability of the cache varies among browsers, browser versions, and even among the type of data (HTML, images, etc.)

Load Balancing IP Servers

One of the advantages of using DNSMux is its ability to load balance the IP servers for each site under management by DNSMux. This functionality does not replace that of WebMux – in fact, WebMux can do a better job for local servers because it has total control over directing clients and near real-time information about server health – but the two working together can do a better job than either one alone.

Even in the absence of a WebMux, DNSMux is capable of load balancing the IP servers it manages, such that a reasonably equal workload of traffic management is given to each. To accomplish this, DNSMux is able to allocate transactions across the IP servers it manages based on a load-balancing algorithm that ranks qualifying servers to receive transactions. DNSMux's load balancing algorithm can be influenced by up to three factors that determine whether each server's rank will be increased or decreased:

- **Weight:** A static user-assigned value that reflects the inherent power of the server. It also acts as the fail-over sequence when in fail-over mode. The highest weight IP address will be the first to resolve
- **Health:** A dynamic value determined by DNSMux's regular health-check which deduces the server's near-current performance based on how quickly tested protocols execute
- **Round Robin:** A relative value based on the DNSMux's previous allocation of transactions. When this checkbox is unchecked, the host resolution is fail-over based on the weight
- **Proximity** A relative value based on the physical distance between the client (or the client's local DNS server) and each server

These four factors work as described in the following paragraphs.

Weight

The idea behind weight is to generate more transactions on the servers that are better able to handle them. Use normalized number possible for best result.

The weight is imposed manually at configuration time and reflects the relative inherent performance of each server. Weight values are arbitrary; their effect on the load-balancing algorithm is that the literal weight value is added to (for positive weights) or subtracted from (for negative weights) the server's current ranking value.

For example, a standard IP server could be assigned a weight of 0 (neutral) while a slower system could be given a negative value and a faster system a positive value. These values are taken into account in the algorithm so as to cause more transactions to be generated to the more powerful systems.

At the fail over mode, the weight number is the sequence number for the sites being failed over. Highest weight number will be the first to be selected. If that failed health check, next highest weight will be selected.

Health

The health factor reflects the near-current performance of each IP server. It is not able to detect the current performance because by the time the information is gotten the transaction volume and allocation may have changed slightly.

This health factor is determined automatically by DNSMux every 15 seconds, by testing the configured health-check protocols serially against each server to determine its average current performance.

The effect of the health factor on DNSMux's load balancing algorithm is that for every 10 milliseconds of response time (to a maximum of 20 seconds) during protocol checking one is subtracted from the server's ranking value.

If the health check determines that any tested protocol is unresponsive, 10000 is subtracted from the server's rank, effectively taking the server out of service so that it will not be sent any transactions. Once the problem is rectified, DNSMux automatically determines this and the server comes back in service as its ranking value returns to normal competitive levels.

Round Robin

The purpose of the round robin factor is to allocate transactions across all servers that have competitive ranks; i.e. servers with approximately equivalent ranking values will get an even allocation of transactions.

The DNSMux load balancing algorithm's method of imposing round robin is to track a round robin count for each server. Every time a server is given a transaction, its round robin count goes up by one. The round robin count is subtracted from the ranking value each timeservers are ranked for transaction allocation.

When the round robin checkbox is unchecked, DNSMux will resolve one IP address only. It will select the highest weight IP address that also passed health check. When the site with highest weight failed health check, next highest weight site will be resolved.

Proximity

The purpose of the proximity factor is to favor servers that are geographically closer to each client. This feature is not available at this time. It will be added in the future through firmware update.

Proximity is calculated by the geographical location of the client (or the client's local ISP) and each server, based on the differential between each's longitude and latitude. DNSMux's allocation algorithm divides the mileage distance between the client and each candidate server by 100 ms and adds the result to the comparative rating of each

Note Proximity measurements reflect only "as the crow flies" distances and do not take into account variations in network speeds and other factors that may affect performance.

Health-Checking IP Servers

DNSMux regularly monitors the health of all the IP servers it manages to ensure that they are ready to service user requests. Should an IP server become unable to service user requests, DNSMux will automatically divert traffic to functioning IP servers. When the problem machine begins responding reliably, DNSMux automatically puts it back into service.

DNSMux's health check not only determines the responsiveness of each protocol to service requests, it collects performance information which is used in determined how to allocate user requests across the IP servers to ensure peak responsiveness.

The health check is performed every 15 seconds by all DNSMuxes against all servers in the cluster to test availability and performance characteristics.

The health check serially performs the tests configured in the Host screen. As available protocols may vary from server to server, you should take care when configuring the Hosts screen that all the host's servers have services or daemons installed for the tests selected.

If all the tests completed successfully, the load-balancing rank of the server is adjusted by the total time taken, averaged with previous health check runs. Refer to the discussions in Chapter 3 for more information. In addition, the test results are shared with the other DNSMux nameservers in the cluster.

Failover

With DNSMux, there are two types of failovers considered:

- The failure or unresponsiveness of a site
- The failure or unresponsiveness of a DNSMux unit itself

These problem conditions are detected, reported, and handled as described below.

Failure of an IP Server Site

Every 15 seconds, all DNSMuxes in the cluster perform a health check on the servers they manage. The health check tests the protocols configured in the Hosts screen.

When exercising each individual protocol on each IP server, DNSMux waits for up to 20 seconds for the protocol to return. If the server fails any test on three consecutive runs, DNSMux assumes the server is non-functional. While a server is considered non-functional, it must successfully complete three consecutive runs to be considered operational.

In Round Robin mode, rather than taking a non-functional IP server out of service, DNSMux ranks it at the bottom of the candidates for directing clients. This has the effect of excluding the IP server from any transactions for a time.

Once the problem with the protocol is resolved, the IP server is brought back into service automatically with no manual intervention to DNSMux required.

In Fail-Over mode, DNSMuxes only resolve the site IP address that passed the health check also has the highest weight. When the site with highest weight failed, it will resolve to next highest site IP address. This is designed for the need that only has one active site at a time.

Notification of the unresponsive protocol is logged and the technical contacts for the server are notified by email. If no contacts are listed, the technical contact for the zone is notified.

Failure of a DNSMux

All the DNSMuxes in a cluster are in regular communication with each other, and should at any time there be a communication failure, DNSMux may determine that one of its brothers is down. Should that occur, notification of the problem is made.

There is no opportunity or need for the active DNSMuxes to work around its failed brother because of the way that DNS itself functions. To understand why, some explanation of DNS is called for.

As part of the normal functioning of DNS, when clients or caching DNS servers try to resolve a domain name, they first ask one of the root DNS servers. The root servers reply with the IP addresses of the authoritative nameservers (in this case DNSMuxes) for the zone. Then the client or caching DNS server asks each of the authoritative servers in line, trusting the first reply it receives. In this way, when a DNSMux is down, other DNSMuxes in the cluster will continue to service queries, ensuring normal and uninterrupted operation.

For this reason most domain registrars will require you supply the IP address of at least two DNSMuxes, and why it is strongly recommended that they be geographically separated to sufficiently protect against environmental disasters and other events that could cause both DNSMuxes to fail. Should the failure of multiple DNSMuxes be a concern, additional DNSMuxes can be deployed within a domain to provide additional protection.

Preparing for DNSMux Deployment

Introduction

If you are deploying DNSMux in your environment, it is likely that you already have traditional DNS servers that you will be replacing with DNSMuxes. DNSMux supports all the features of traditional nameservers, but introduces several new concepts that should be adequately understood and their utilization planned before deployment.

Overview

Ideally, you should start preparing for your new DNSMux environment several weeks before you actually deploy DNSMux.

There are a number of preparatory steps:

- Record the hostname or IP address for your organization's servers
- Determine the technical contact emails
- Set the TTL value on all your existing DNS servers low so clients will start sending queries to DNSMux soon after the transition.

Determine Network Addresses

When configuring your DNSMuxes, you will need to know the public hostname or IP address for the existing DNS servers that will be replaced by DNSMux. In addition, note the IP address, netmask, and gateway for the local network the nameservers reside upon. This may be a public network or a private network.

- You must also record the hostname or IP address for:
 - All IP servers that will be managed by DNSMux
 - The email server(s) that will be used to route outgoing messages from your DNSMuxes
 - The log server(s) that will log entries generated by your DNSMuxes
 - Optionally, a NTP timeserver to keep the DNSMux clocks in sync

In addition, should you be connecting any DNSMuxes that are not one-to-one replacements for existing DNS servers, or any new servers, their IP addresses will need to be allocated.

DNSMux has two network interfaces. One is directly on the Internet, the other is for intranet. DNSMux has an internal firewall that blocks any unwanted traffic so that it can stay on Internet safely. Its firewall policy blocks any traffic not related to DNS inquiries from the Internet side. It also allows blocking certain IP addresses from reach it on any port.

Determine Relative Performance of IP Servers

DNSMux is capable of load balancing the IP servers it manages, such that a relatively equal workload of incoming traffic is given to each one. To accomplish this, it can use a weighted, round robin, or weighted round robin algorithm. The weighted and weighted round robin algorithms have both a dynamic and static component, where the dynamic component is the current IP server performance and the static component is the inherent performance power of the server.

The inherent power of the server has the effect of skewing the load balancing algorithms to favor more powerful servers, by ranking it higher than other servers for receiving new traffic.

In order to take advantage of that feature, you would need to specify a positive or negative weight value for each server to indicate its inherent performance capabilities relative to the norm, and so you should estimate how many connections each of your servers can handle.

Note CAI Network's WebSpray product can be useful in determining the performance power of any IP-based server.

Determine Technical Contacts and Their Email Addresses

DNSMux is capable of alerting the appropriate people whenever another DNSMux stops working (i.e., it stops sending heartbeat messages). The technical contacts configured on the failed DNSMux nameserver will be notified.

Whenever the state of a server changes between up and down, the technical contacts listed for that host will be notified. If none are listed, the technical contact for the zone is notified.

Reduce TTL Value

Traditional DNS nameservers typically specify TTLs of hours or days because DNS without DNSMux's enhanced behavior is relatively static. DNSMux makes DNS much more dynamic and therefore the TTL value should be shorter in order to prevent stale resolutions to remain in cache. By default the TTL is 15 seconds. Clients will let their DNS answers expire before re-querying the nameserver. This delay will impede the responsiveness of DNSMux to changes in server health.

Rather than wait until you deploy DNSMux to change the TTL, it is recommended that you reduce the TTL before deployment on your current nameservers. The change should be made early enough so records using the old TTL expire before the deployment and it should be set to the TTL to be used on the DNSMuxes. Following this advice, when you deploy DNSMux you can immediately see the change in behavior.

Using the Front Panel Controls

Introduction

Each DNSMux unit is initially configured via the front-panel keypad and related LCD display, and from time to time it may be necessary to use these controls for other functions. Normally, however, once the networking information is set via the front panel, all configuration operations are performed from the web-based user interface, described in the next chapter.

Layout and Controls

The front panel controls look like this:



There are six keys in the keypad which are referred to by the following names and which have the following behavior:

- ← LEFT Moves between control panel functions and IP address octets
- RIGHT Moves between control panel functions and IP address octets
- ↑ UP Increases an IP address octet
- ↓ DOWN Decreases an IP address octet
- ✓ CHECK Accepts the current value into DNSMux
- X CANCEL Cancels the current function

These keys are used in combination to perform various operations, in conjunction with the LCD display.

Control Panel Functions

Through the control panel you can:

- Display statistics
- Display and set network addresses
- Disable the internal firewall
- Reboot the DNSMux unit
- Reset settings to factory defaults
- Adjust the brightness of the LCD

Values that may be displayed in the LCD and their meanings are shown in Appendix B.

You can cycle through the various control panel functions using the LEFT and RIGHT buttons. Pressing the CANCEL button returns to the status screen. The network settings can be changed by pressing CHECK, then using the arrows to modify the value, and CHECK to accept the changes, or CANCEL to abort. The other functions are activated by pressing and holding the CHECK button.

Security Lockout

For security reasons, the control panel will lock itself after 10 to 20 minutes and require a pre-configured security code to leave the statistics screen. The security code is specified as a keypad sequence via the GUI, and the same keypad sequence must be entered in the control panel to unlock it.

Once unlocked, the control panel remains unlocked for 10 to 20 minutes, and thereafter the security code must be re-entered to leave the statistics screen. This feature can be disabled by browser setup in security screen.

Control Panel Tasks

The various tasks that can be accomplished via the front panel control are described below.

Unlocking the Control Panel

This screen is displayed when the control panel is locked, and a pre-configured keypad sequence (set in the GUI configurator) must be specified to unlock it:

Enter PIN →↑↓←✓→

The unlock sequence uses only the directional keys (LEFT, RIGHT, UP, and DOWN) and the CHECK key. The CANCEL key cancels and returns to the main screen.

Once unlocked, the control panel stays unlocked for 10 to 20 minutes.

Note If you attempt to perform a function when the control panel is locked which starts with the LEFT, RIGHT, or CHECK button, the “Enter PIN” screen will be displayed. Once the PIN is correctly entered, the previously-pressed button (LEFT, RIGHT, or CHECK) action will be executed and you can continue as normal (there is no need to re-press the first button in the desired sequence.)

Determining Throughput

The default screen shows the current load on the unit, including the CPU usage, memory consumption, and incoming and outgoing network throughput, in megabytes per second.

<i>0.0 0.0 MB/s</i> <i>cpu 0% mem 3%</i>

Setting Network Addresses

To set the IP address or netmask for either the network 1 or network 2 interface, or to set the default gateway used by both interfaces:

1. Advance to the function you want to set
2. Press the CHECK button to begin modification
3. Use LEFT/RIGHT to step between the octets comprising an IPv4 address
4. Press UP/DOWN to increase/decrease the value of an octet
5. Press the CHECK button to accept the changes

At any time you can press CANCEL to abort and discard any changes

This function sets the IP address for the first network card:

<i>←Net 1 IP→</i> <i>nnn.nnn.nnn.nnn</i>

This function sets the IP address of the netmask for the first network card:

<i>←Net 1 Netmask→</i> <i>nnn.nnn.nnn.nnn</i>
--

This function sets the IP address of the gateway for both network interfaces:

<i>←Net 1 Gateway→</i> <i>nnn.nnn.nnn.nnn</i>
--

This function sets the IP address for the second network card:

<i>←Net 2 IP →</i> <i>nnn.nnn.nnn.nnn</i>
--

This function sets the IP address of the gateway for the second network card:

←Net 2 Gateway→
nnn.nnn.nnn.nnn

Disabling the Internal Firewall

When the control panel is in this mode, pressing the CHECK button for four seconds will remove firewall protection and open all ports on the DNSMux unit.

← hold ✓ to →
open firewall

After the defaults have been reset, a confirmation screen is displayed.

← SUCCESS →
open firewall

The DNSMux unit's firewall can be re-enabled via the Security screen in DNSMux's browser-based configurator or by restoring the factory defaults via the control panel.

Rebooting the DNSMux Unit

When the control panel is in this mode, pressing the CHECK button for four seconds will reboot the DNSMux unit.

← hold ✓ to →
reboot

After the DNSMux unit has rebooted, a confirmation message is displayed.

← SUCCESS →
reboot

This message remains displayed until the control panel daemon restarts.

Restoring the Factory Defaults

When the control panel is in this mode, pressing the CHECK button for four seconds will restore the DNSMux unit's control panel settings to its default values.

← hold ✓ to →
restore defaults

After the defaults have been reset, a confirmation message is displayed:

← SUCCESS →
restore defaults

Adjusting the Brightness of the LCD

You may wish to adjust the brightness of the LCD, particularly in brightly lit settings where the LCD may be hard to read with default brightness.

The LCD brightness can be adjusted from the statistics screen on the LCD. Use the UP and DOWN buttons to make the LCD brighter and dimmer.

Note The LCD brightness may not be adjusted when the control panel is locked. You must first unlock it before adjusting the LCD brightness.

Configuring DNSMux

Introduction

DNSMux serves as a replacement for an ordinary DNS server. You configure it with the same kind of information as any DNS server but some additional information to facilitate advanced DNSMux functionality. This additional information includes:

- Criteria to use when load balancing among various IP servers for load balancing purposes
- Protocols to use for health-checking IP servers to determine if they are up and, if so, their performance characteristics

Before configuring your DNSMuxes, collect all the relevant configuration information required and plan out the usage of the DNSMuxes in your environment.

Configuring Multiple DNSMuxes From A Single Point

Although basic Setup screen needs to be configured individually, there is no need to configure zones/hosts on every DNSMux. DNSMuxes have a peer-to-peer relationship with each other such that you can specify shared configuration information and propagate those settings to all DNSMuxes in the cluster.

Note Propagation can only succeed for DNSMuxes that can be reached via the network at the time that changes are propagated. For DNSMuxes that cannot be connected to at propagation time, propagation can be repeated at a later time by hitting the “Propagate” button. The propagation message bar will remain until all DNSMuxes in the cluster have been successfully propagated

Configuration Overview

DNSMux setup is done via a browser-based interface that requires authentication.

The predefined user Administrator can view configurations and make changes; the predefined user Observer can view configurations, except passwords, but not make changes.

Initial Setup of a New DNSMux

If you are setting up a DNSMux for the first time, you will need to assign it an IP address via the front-panel controls. Once that is done, you can access the setup pages via that IP address.

Set The IP Address, Netmask, and Gateway Via The Control Panel

Use the front panel to set the IP address for the network 1 interface of the DNSMux unit.

If replacing an existing DNS Server with a DNSMux, use the same IP address.

To set the IP address and netmask of the DNSMux unit:

1. Press the CHECK button, and then use the LEFT and RIGHT buttons to switch between octets and the UP and DOWN buttons to change the value of the octet.
2. When complete press the CHECK button twice, then set the gateway address
3. When complete press the CHECK button twice, then set the gateway address

You should now be able to access the DNSMux screens via the web-based interface.

Note Refer to Chapter 4 for more information about using the control panel

Ports Utilized by DNSMux

The following ports are used by DNSMux with the protocols and for the functions described:

22 (TCP)	SSH port for DNSMux configuration propagation
51 (UDP)	Health daemon collaboration protocol
53 (UDP)	Used for accepting and sending DNS queries
80 (TCP)	Used for HTTP access to the GUI configurator
433 (TCP)	Used for HTTPS (secured) access to the GUI configurator

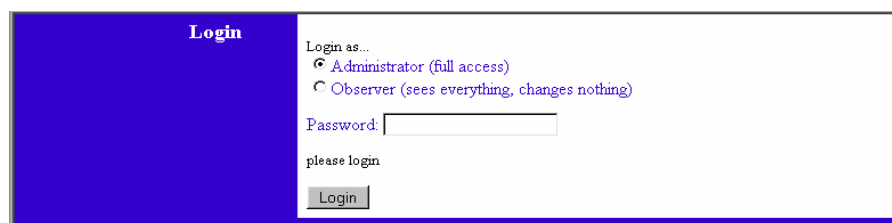
If the DNSMux unit is located behind a firewall, the first three ports above must be kept open to allow the various DNSMuxes in the cluster to communicate. Additionally, if you want to use DNSMux's GUI configurator from outside the firewall, the last two ports must also be kept open. DNSMux built-in firewall drop all the packets come to any other ports.

DNSMux has built-in firewall to drop any host not on the propagation list to access port 22. To block external access to the GUI configurator, block both HTTP (80) and HTTPS (433) ports in your firewall, or alternatively use the "Allow Hosts" feature on the GUI configurator Security screen. If by accident the management ports locked out, use the LCD keyboard panel to temporarily open the firewall to allow administrator correcting the setup.

Accessing the DNSMux Screens

To access the GUI configurator screens for a DNSMux from your web browser:

1. Navigate to the IP address assigned to the DNSMux you want to configure, like "http://<DNSMux IP>/" or "https://<DNSMux IP>/".
2. The login screen will be displayed:



The screenshot shows a web-based login interface. The top part has a blue background with the word "Login" in white. Below that, there's a "Login as..." section with two radio button options: "Administrator (full access)" which is selected, and "Observer (sees everything, changes nothing)". Below the radio buttons is a "Password:" label followed by a text input field. At the bottom, there's the text "please login" and a "Login" button.

3. Enter the Administrator password to make changes or the Observer password to view configurations. The default password is:
123456
4. Once you have logged in, your user name is displayed in the header and a logout button is provided:



Note If browser cookies are not disabled, login information will not need to be re-entered until logging out or staying idle for eight hours.

Using The DNSMux Screens

DNSMux has three screens – Basic, Zones, and Security – which can be used to configure the various functionality within DNSMux.

At the top of each screen is a series of identical buttons that provide access to the various screens, which looks like this:



The recommended sequence for configuring DNSMux is as follows:

1. Complete the Basic screen, which must be set for each DNSMux individually
2. Complete the Security screen, to set the passwords and firewall values
3. Use the Zones screen to configure the DNS zones and hosts for the zone

Note The settings made in the DNSMux Zones screens will be propagated to other DNSMux nameservers in the cluster.

Propagation to Other DNSMuxes

Once you have changed any configuration settings in the GUI, a message bar appears beneath the header indicating that changes have been made and that those changes have not yet been propagated to other DNSMuxes in the cluster:



Hitting the “Propagate” button will immediately propagate all queued configuration changes to the other DNSMuxes listed in the nameservers field of the Basic screen. If the propagation was successful, the bar disappears until more changes are made.

Basic Screen

The Basic screen configures basic settings for all DNSMuxes in the cluster.

From the Basic screen, you can configure the following:

- Outgoing email server
- Server to send log files to
- What to log
- Nameserver(s)

The Basic screen looks like this:

Network	Hostname: <input type="text" value="ns8"/> Company: <input type="text" value="CAI Networks, Inc."/> IP Address: <input type="text" value="69.82.176.103"/> Netmask: <input type="text" value="255.255.255.0"/> Gateway: <input type="text" value="69.82.176.1"/> An optional private network on the second ethernet port Internal IP Address: <input type="text" value="192.168.82.112"/> Netmask: <input type="text" value="255.255.255.0"/>
Time	<input checked="" type="checkbox"/> NTP Server: <input type="text" value="152.4.20.3"/> Time: <input type="text" value="Tue Nov 28 12:30:06 20"/> Time zone: <input type="text" value="(-8:00) Los Angeles, Vancouver, Dawson, Tijuana"/>
Email	Outgoing email server: <input type="text" value="192.168.82.98"/> Technical contact(s): <input type="text" value="someone@your-domain.com"/> Allow Bug Report <input type="checkbox"/>
Logging	Logging server: <input type="text" value="192.168.82.28"/> Log classification: <input type="text" value="Informative messages, warnings, and errors"/>
DNSMuxes	DNSMux name servers: <input type="text" value="dnsmux3.dnsmux.com, ns8.dnsmux.com"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Network

These are the networking-related settings for the DNSMux nameserver you are configuring.

Hostname

This is the hostname for this DNSMux. If specified, email notifications sent from other DNSMuxes will contain this value.

IP Address

This is the IP address assigned to this DNSMux unit on the Internet side.

Netmask

This is the netmask assigned for devices on this network.

Gateway

This is the IP address of the upstream gateway, router address.

Internal IP address

This is the IP address assigned for the second network interface in the DNSMux, generally used for intranet private access, or access the email server on that network.

Netmask

This is the netmask for the second network.

Company Name

This value will identify the DNSMux in the upper left corner of the GUI configurator

Time

You can explicitly set the time for this DNSMux or have DNSMux source it from a specified NTP server. You may also optionally specify the time zone this DNSMux is located in (or in which you would like it to be seen in).

NTP Server

Tick the checkbox if you want this DNSMux to get the current time from an NPT server. If the checkbox is ticked, specify the hostname or IP address of the NTP server.

Note If you do not have your own NTP server, you can reference pool.ntp.org, which hosts contains hundreds of servers all with perfectly synchronized clocks

Time

This is the current date and time setting for this DNSMux. The current time is shown, and you may override it if desired in YYYY-MM-DD HH:MM:SS format.

Time Zone

Select the time zone for this DNSMux by selecting from the drop-down list. Timezones are shown relative to GMT (Greenwich Mean Time).

Email

When another DNSMux in the cluster has detected that this DNSMux has failed, it will send notification to this email address.

Outgoing email server

Host name or IP address of the outgoing email server. Please make sure your email server allowing sending email by the DNSMux IP addresses.

Technical contact(s)

The email address of the technical contact person for the zone. To specify more than one technical contact, delimit multiple email addresses by commas (“,”).

Allow bug report

When this checkbox is checked, DNSMux will send any error report to CAI Networks’ support. In normal operation, this option is unchecked.

Logging

The settings govern the handling of logging information generated by DNSMux.

DNSMux uses its own logging daemon that uses the syslog protocol for sending log files to a nominated server, optionally on a designated port. You can specify the level of logging, which determines which events will be included in the log files. Logged events can include internal errors, errors encountered when sending email notifications, and errors encountered by related subsystems.

Logging server

Host name or IP address of the system to which syslogd notifications will be sent. Please make sure the system at this address accept the syslogd messages from DNSMux. The default syslogd port is being used. To specify a port number, append it to the host name or IP address separated by a colon (“:”).

Log classification

Select from the drop-down list which level of logging should be performed. The possible levels are:

- Errors
- Warnings and errors
- Informative messages, warnings, and errors

Nameservers

If this is the first DNSMux you are configuring for your network, the Nameservers field will be blank. Specify the hostnames or IP addresses of the DNSMux nameserver(s). To specify multiple nameservers, delimit each by a comma (“,”) or space. It is important this field is not left blank.

This value will be propagated along with the zones.

Note If you specify an IP address for a nameserver, a temporary name will be created for every zone in which it is contained, as required by the DNS protocol. This temporary name will be exposed via DNS queries for NS records.

Security Screen

The Security screen lets you configure the user passwords and access controls for each DNSMux-managed server.

From the Security screen, you can configure the following:

- Administrator and Observer user passwords
- DNSMux zone to which server belongs
- Hosts to which access is allowed and denied
- Whether DNSMux’s internal firewall is enabled or disabled

The Security screen looks like this:

The screenshot shows a web-based configuration interface for the Security screen. It features a dark blue sidebar on the left with three main sections: "Passwords", "Control Panel PIN", and "Allowed Hosts".

- Passwords:** Contains two sets of input fields. The first set is for the "ADMINISTRATOR" password, with a "confirmation:" field. The second set is for the "OBSERVER" password, also with a "confirmation:" field.
- Control Panel PIN:** A single input field containing the text "NO PIN SET".
- Allowed Hosts:** This section includes a radio button interface for the firewall status, currently set to "enabled". Below this are three input fields: "Allow" (containing "192.168.12.0/255.255.255.0" and "10.1.1.0/255.255.255.0"), "Deny" (empty), and "Propagation" (containing "1.2.3.4 5.6.7.8 192.168.12.111"). At the bottom of this section are "Apply" and "Cancel" buttons.

Passwords

DNSMux has two pre-configured users, “Administrator” and “Observer”, for which you can change the passwords using this screen. It is recommended that passwords be at least six characters in length and contain mixed-case letters, numbers, and special symbols. DNSMux GUI configurator passwords are case-sensitive.

Administrator

To change the Administrator password, enter the same new password value in both side-by-side fields.

Observer

To change the Observer password, enter the same new password value in both side-by-side fields.

Control Panel PIN

To set or change the keypad sequence used to unlock the control panel, specify the sequence as a string using the following abbreviations: “L” = LEFT, “R” = RIGHT, “U” = UP, “D” = DOWN, and “C” = CHECK. (The CANCEL key is used to cancel code entry and therefore cannot be used in the keypad sequence.) Leave it empty will delete the PIN.

Allowed hosts

When this field is empty, any host can connect to DNSMux through browser to manage it. 0.0.0.0 entry also servers as all host can access DNSMux management console. DNSMux can be configured to allow access from specified hosts. In configuring this, you either specify a host is allowed or which is denied (but not both). If allowed hosts are specified, only those hosts are granted access to management console through HTTP/HTTPS ports, all other hosts will be dropped; if denied hosts are specified, those hosts being specified are dropped on any ports. You can also specify which DNSMux(es) in a cluster are allowed to propagate changes to the current DNSMux.

For the first two fields, you may enter a list of IP addresses, hostnames, or networks. Hostnames will be resolved only when first configured. Networks should be entered either as prefix-addr/netmask-length or prefix-addr/netmask. Multiple values in a field need to be separated by spaces, commas, or line-breaks.

Allow

Specify the host(s) or network(s) to allow access to manage this DNSMux unit. This does not permit propagation. When there is no entry in this field, all hosts (except in the Deny list) can manage DNSMux through browser. Once you have an entry in this field, only hosts on the list are allowed to manage the DNSMux, all other hosts are dropped. Its format is: 216.200.50.0/255.255.255.0 216.200.51.1/255.255.255.255

Deny

Specify the host(s) or network(s) to deny access to this DNSMux unit on all ports, including the DNS services. When this field is empty, no hosts are denied access to DNS services. This field is for blocking those hosts trying to attack DNSMux in anyway. Format: 1.2.3.4 5.6.7.8

Propagation

Specify the DNSMux(es) that are allowed to propagate configurations from and to this DNSMux. Only those host(s) or network(s) listed here may connect using SSH protocol. All other IP address not on the list will be dropped at the DNSMux network interfaces.

The format for specifying a DNSMux is by IP address, like 192.168.10.100. To specify multiple DNSMuxes, delimit them with commas or space.

Firewall

This option enables and disables DNSMux's internal firewall. When disabling the firewall, the configuration is preserved but disabled. Re-enabling the firewall will reactivate the saved configuration.

Note DNSMux's internal firewall may also be disabled via the control panel on the front of the DNSMux unit.

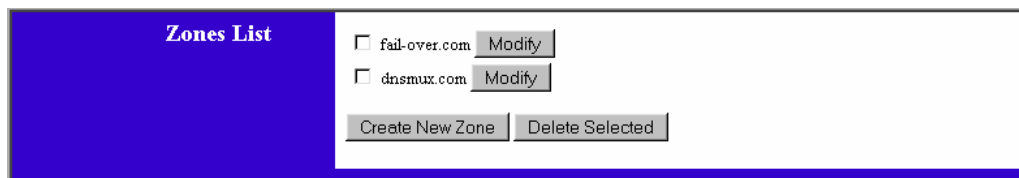
Zones Screen

The Zone screen lets you configure the various options for each zone.

From the Zone screen, you can configure the following:

- The name of the zone
- Email address of technical contact for the zone
- Default duration for objects in this zone to remain in cache
- Delay duration until zone changes should post to all other DNSMuxes
- Dynamic hosts related to this zone
- Static DNS records related to this zone
- Nameserver(s) for this zone

The Zone screen looks like this:



Click the “Create New Zone” to create the first zone:

New Zone	Zone Name: <input type="text" value="your-domain.com"/> FQDN SOA NS: <input type="text" value="dnsmux.your-domain.com"/> Technical Contact Email: <input type="text" value="hostmaster@your-domain.com"/> Default Cache Time: <input type="text" value="15"/> (seconds)																								
Delayed Application	<input type="checkbox"/> Delay any changes until <input type="text" value="17:00"/> local time (PST).																								
Dynamic Hosts	You must create and save this zone before adding hosts																								
Static Records	Standard DNS records: <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Hostname</th> <th>Class</th> <th>Type</th> <th>Priority</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td><input type="text" value="host1"/></td> <td>IN</td> <td>A</td> <td><input type="text"/></td> <td><input type="text" value="1. 2. 3. 4"/></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="text" value="smtp"/></td> <td>IN</td> <td>A</td> <td><input type="text"/></td> <td><input type="text" value="5. 6. 7. 8"/></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="text" value="your-domain.com"/></td> <td>IN</td> <td>MX</td> <td><input type="text" value="10"/></td> <td><input type="text" value="smtp.your-domain.com"/></td> </tr> </tbody> </table> Checked Records: delete duplicate	<input type="checkbox"/>	Hostname	Class	Type	Priority	Value	<input type="checkbox"/>	<input type="text" value="host1"/>	IN	A	<input type="text"/>	<input type="text" value="1. 2. 3. 4"/>	<input type="checkbox"/>	<input type="text" value="smtp"/>	IN	A	<input type="text"/>	<input type="text" value="5. 6. 7. 8"/>	<input type="checkbox"/>	<input type="text" value="your-domain.com"/>	IN	MX	<input type="text" value="10"/>	<input type="text" value="smtp.your-domain.com"/>
<input type="checkbox"/>	Hostname	Class	Type	Priority	Value																				
<input type="checkbox"/>	<input type="text" value="host1"/>	IN	A	<input type="text"/>	<input type="text" value="1. 2. 3. 4"/>																				
<input type="checkbox"/>	<input type="text" value="smtp"/>	IN	A	<input type="text"/>	<input type="text" value="5. 6. 7. 8"/>																				
<input type="checkbox"/>	<input type="text" value="your-domain.com"/>	IN	MX	<input type="text" value="10"/>	<input type="text" value="smtp.your-domain.com"/>																				
DNSMuxes	DNSMux name servers: <input checked="" type="checkbox"/> dnsmux.dnsmux.com. <input checked="" type="checkbox"/> ns2.dnsmux.com.																								
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>																									

Every field on this page should be filled with proper information, replacing the part says “your-domain.com” with your actual domain name that is being configured. Static Records part must have all the new DNSMux host name and IP addresses. In the DNSMuxes section, it may list all the hosts in the propagation list from “Basic” screen. Please note NS records should not be entered into the Static records, instead, check all the proper DNSMux name servers. Those DNSMux name servers are defined in the Basic screen DNSMuxen field. Then press the “Apply” button to create the first zone.

Clicking the “Modify” button next to a zone name will bring up a screen to configure that zone:

your-domain.com

Zone Name:

FQDN SOA NS:

Technical Contact Email:

Default Cache Time: (seconds)

Delayed Application

Delay any changes until local time (PST).

Dynamic Hosts

Hostname Modify

Checked Hosts: [delete](#) [duplicate](#)

Static Records

Standard DNS records:

<input type="checkbox"/>	Hostname	Class	Type	Priority	Value
<input type="checkbox"/>	ns1	IN	A		1.2.3.4
<input type="checkbox"/>	ns2	IN	A		5.6.7.8
<input type="checkbox"/>	<input type="text"/>	IN	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	IN	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	IN	<input type="text"/>	<input type="text"/>	<input type="text"/>

Checked Records: [delete](#) [duplicate](#)

DNSTMuxes

DNSTMux name servers: dnsmux.dnsmux.com. ns1.dnsmux.com.

Form Submitted Successfully

If making changes to an existing zone, the zone name is shown in the upper left. If setting up a new zone, “New Zone” is shown.

Zone

The name of the zone being configured is displayed in the upper left corner.

Zone Name

To change the name of the zone, enter it here.

FQDN SOA NS

The name of this DNSTMux appliance. Please notice its format and terminated with a ‘.’.

Technical Contact Email

Specify the email address of the technical contact person for the zone. Example: root@your-domain.com

Default Cache Time (TTL)

Specify how long answers should be cached with clients or caching nameservers before expiring. The default cache time is specified in seconds, and defaults to 15 seconds. See “Caching” in Chapter 3 for a discussion of caching and guidelines in setting this value.

Note Many DNS servers ignore the TTL specified in DNS records and instead assign a TTL up to 3 days.

Delayed Application

Configuration changes can be activated immediately, or delayed until a specified time. See “Delayed Application” in Chapter 2.

Delay any changes until

Select the desired time from the drop-down list. This time is governed by whatever time zone was configured for this DNSMux.

Dynamic Hosts

This area is used to create, modify, and delete dynamic site/host DNS entries. Dynamic DNS entries only serve the purposes of CNAME, A, and AAAA records, i.e., they map domain names to IP addresses or other names.

Host

Specify the name of a sever on each line.

Actions

There are also some actions available for managing dynamic hosts:

- | | |
|------------------------|---|
| Modify | To modify a host entry, tick its checkbox and hit the ‘Modify’ button |
| Delete | To delete a host entry, tick its checkbox and hit the ‘Delete’ button |
| Create new host | To create a new host entry, hit the ‘Create new host’ button |

Static records

This area is used to create, modify, and delete static DNS records. Static record information is validated after the “Apply” button is hit and any errors detected are reported.

Hostname

This is a display field containing the name of a created host

Class

This is the class for the host entry (usually IN)

Type

This is the type of host entry. Common record types are A, CNAME and MX.

Priority

This is the priority of the host entry (for MX and SRV records only)

Value

This is the value of the host entry

Static records are configured in DNSMux the same as for a regular DNS server with the following exceptions:

- “A” records may not be configured, as DNSMux automatically sets the proper A record as a dynamic host. There is no need to specify multiple A records, as normal DNSMux behavior provides this functionality
- “AAAA” records may not be configured as they are not supported at this time
- “NS” records should not be configured, as DNSMux automatically sets the proper NS configuration for other DNSMux nameservers in the cluster. Non-DNSMux nameservers should not serve the same zone(s) served by DNSMuxes
- “SOA” records may not be configured, as DNSMux automatically sets the proper SOA configuration based on the technical contact email(s) specified for the zone
- “MX” records require to have “A” records setup first. In the MX line, enter the domain name followed by a period in the hostname entry part, like “mine.com.”, enter the fully qualified A record in the value field, like “smtp.mine.com.”. Please note the period following the .com is needed

Tip DNSMux can perform load balancing and failover on the origin of a zone. For example, for the zone “my-domain.com” it would be desirable for users be able to type “<http://my-domain.com>” (without the “www”) and still be targeted properly. To enable this setup, create a dynamic host of any name (for example, “www”) and alias the origin to that host using a CNAME record.

Actions

There are also some actions available for managing dynamic hosts:

Delete	To delete a host entry, tick its checkbox and hit the ‘Delete’ button
Duplicate	To duplicate a host entry, tick its checkbox and hit the ‘Duplicate’ button

Nameservers

This lists the nameservers for all DNSMuxes that have been configured for the current domain. Tick the checkbox of all the nameservers you want to advertise for this zone.

Site Screen (sub-screen of Zone screen)

The Host screen lets you configure the hosts/sites managed by DNSMux and the servers that comprise them. Geographically separated sites are dynamic records mapping domain names to IP addresses or other names. The Host screen is accessible from the Zones screen: select the modify or create new host.

From the Host/site screen, you can configure the following for each host:

- Each host by name
- The zone to which each host belongs
- Servers that contain the host data
- Criteria used in selecting among various IP servers
- Health checks to be performed to determine the responsiveness of each IP server

The Host screen looks like this:

The screenshot shows a web interface for configuring a host. It has a dark blue sidebar on the left with two main sections: 'Servers' and 'Criteria'. The main content area is white with a blue header. At the top, there are two input fields: 'Hostname: www' and 'belongs to zone: your-domain.com'. Below this is a table with columns for 'IP address', 'Weight', and 'Tech Email'. The table contains two rows: one with IP '2.3.4.5', weight '1', and email 'root@your-domain.com'; the other with IP '3.4.5.6', weight '2', and email 'root@your-other-domain.com'. Below the table are links for 'Checked records: delete duplicate'. Under the 'Criteria' section, there are checkboxes for 'performance factor weight', 'health', and 'round robin'. Below that, there is a section for 'Server health checks to perform:' with a 'Uncheck All' button and checkboxes for 'ftp', 'http', 'https', 'ntp', 'ping', 'pop3', 'smtp', 'tcp', and 'udp'. At the bottom are 'Apply' and 'Cancel' buttons.

IP address	Weight	Tech Email
2.3.4.5	1	root@your-domain.com
3.4.5.6	2	root@your-other-domain.com

The hostname of the host being configured is shown in the upper left.

Hostname

Hostname of the host being configured is displayed

Zone

Zone to which this host belongs is displayed.

Servers (sites)

This lets you specify all the sites' IP addresses for the host and to assign them to various DNSMuxes for management. When this screen is initially displayed, three blank entries are shown, and when those are full, another three are added each time the previous three fill up.

The fields in this section are:

IP address	The IP address of the server
Weight	The assigned weight for comparative purposes against other sites for the host. The weight is a representation of the relative power of each server. Use normalized number possible. More powerful servers should be assigned higher numbers, while less powerful servers lower numbers. 0 is neutral and the default value assigned. In the fail-over mode, the weight will determine the fail-over sequence.
Tech Email	Specify the email address of the technical contact for the host

Criteria

This determines that factors that will be used in determining how the various IP servers for the host will be treated by DNSMux.

Enable one or more factors by ticking its corresponding checkbox. The factors are:

weight	This causes DNSMux to use the assigned weight for each server. A negative value is deducted from the total ranking; a positive value is added. A weight of zero is neutral.
health	This causes DNSMux to use the response time of each server, as determined by the last health check performed by DNSMux
round robin	This causes DNSMux to allocate requests across the various IP servers in a one-after-the-other fashion (e.g., if there are 5 servers and 5 requests, each server would receive one request). When this field is unchecked, DNSMux will resolve the name to one IP address ONLY that has highest weight and passed health check.
proximity	This causes DNSMux to use the physical distance between the client's location (or the location of the client's local DNS server) and each server. This feature is not available in current release.

Health check

DNSMux is able to use various protocols to determine the health (whether a site is up or not, and its performance characteristics) of IP servers. The available protocols are:

FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol – used for web transfers
HTTPS	Secure HTTP protocol (using SSL) – used for secure web transfers
NTP	Network Time Protocol – used to synchronize the clock of a computer to a reference time source...
PING	Packet Internet Groper – send ICMP echos (often blocked by firewalls)
POP3	Post Office Protocol – used for email receipt from server to client

SMTP	Simple Mail Transfer Protocol – used for email receipt by server from client, and between email servers
TCP	Transmission Control Protocol – low-level transport protocol
UDP	User Datagram Protocol – low-level transport protocol

Firmware Screen

The Firmware screen lets you update the DNSMux’s firmware, from a file. You can explicitly specify the pathname of the file or browse to it.

The Firmware screen looks like this:



Browse to the file and hit “Update Firmware”. Upload time depends on your Internet connection speed. After uploading and checksum verification, the screen will display “Upgrade successfully started”. Then DNSMux copies the new firmware and reboots. This process takes about one minute.

Warning DNSMux will be unresponsive after sending the “upgrade successfully started” message. This will not affect users since DNS servers do not hold connections and the workload will be handled by other DNSMuxes in the cluster during the firmware update.

Status Screen

The Status screen shows the status of the DNSMux nameserver, including.

- The revision and build date of the installed firmware
- The serial number of the DNSMux unit
- The elapsed time since the last reboot.

Recent log entries are also shown, listed in reverse-chronological order.

The status screen looks like this:

```
Firmware: v3.1.1 ( Nov 21 2006 16:42:17 )  
  
Serial Number: DM16A0678  
  
Uptime: 6 days 20 hours 53 minutes  
  
Latest Log Entries  
  
Nov 23 11:21:12 /usr/sbin/ntpd[146]: peer 204.17.42.202 now valid  
Nov 23 03:40:24 -- MARK --  
Nov 23 04:00:24 -- MARK --  
Nov 23 04:20:23 /usr/sbin/ntpd[145]: adjusting local clock by 0.128486s  
Nov 23 04:20:24 -- MARK --  
Nov 23 04:40:24 -- MARK --  
Nov 23 05:00:24 -- MARK --  
Nov 23 05:18:25 /usr/sbin/ntpd[145]: adjusting local clock by 0.128682s  
Nov 23 05:20:25 -- MARK --  
Nov 23 05:40:25 -- MARK --
```

To invoke the Status screen, hit the Status button on the header.

DNSMux Appliance Layout

Overview

DNSMux is a rack-mounted appliance that uses industrial-grade components and which is designed for years of trouble-free use. It interfaces with your network via two Ethernet interfaces, and can be initially configured and controlled via a control panel on its face, while detailed operational configurations are made via a web-based GUI interface.

Front View

The picture below shows the front view of a DNSMux appliance:



- On the front of the DNSMux unit, you will find:
- A reset button, which when pressed resets the DNSMux unit
- A power toggle, which must be held down for several seconds to power the unit off
- A LCD, which gives status and operational messages
- A six-key control panel for performing configuration and operational functions

Rear View

The picture below shows the front view of a DNSMux appliance:



On the rear of the DNSMux unit, you will find:

- A fan exhaust which must be kept clear
- A power port connected to a universal power supply
- A DB9 interface for factory testing.
- Two 100BaseT Ethernet interface ports

Control Panel LCD Values

The table below shows all possible values of the control panel LCD screen and their meanings.

Front Panel LCD Screen Values and Meanings

LCD value	Meaning
CAI Networks DNSMux <i>n.n.n</i>	Boot-up screen. Shows the vendor name and the firmware version.
<i>0.0 0.0 MB/s</i> cpu 0% mem 3%	Main screen. The first line shows the throughput, in megabytes per second, of input and output. The second line shows the current CPU and memory usage as a percentage of maximum.
Enter PIN: →↑↓←✓→	Control panel is locked, and a pre-configured keypad sequence must be specified to unlock it. (This keypad sequence is set via the GUI configurator.)
←Net 1 IP → <i>nnn.nnn.nnn.nnn</i>	The IP address for the first network card is shown and can be set.
←Net 1 Netmask→ <i>nnn.nnn.nnn.nnn</i>	The Netmask for the first network card is shown and can be set.
←Net 1 Gateway→ <i>nnn.nnn.nnn.nnn</i>	The gateway IP address for the first and second network cards is shown and can be set
←Net 2 IP → <i>nnn.nnn.nnn.nnn</i>	The IP address for the second network card is shown and can be set.
←Net 2 Netmask→ <i>nnn.nnn.nnn.nnn</i>	The Netmask for the second network card is shown and can be set.
← hold ✓ to → open firewall	In this mode, holding down the CHECK button for four seconds will remove firewall protection and open all ports. The firewall can be re-enabled by doing “restore defaults” or through the GUI by modifying firewall settings.

LCD value	Meaning
← hold ✓ to → reboot	In this mode, holding down the CHECK button for four seconds will reboot the DNSMux unit.
← hold ✓ to → restore defaults	In this mode, holding down the CHECK button for four seconds will reset all control-panel settings to factory defaults.
performing restore defaults	This message is displayed while DNSMux's factory defaults are being reset.
← SUCCESS → open firewall	This message is displayed after DNSMux's firewall has been opened.
← SUCCESS → reboot	This message is displayed after reboot. The LCD remains in this state until the DNSMux unit has successfully rebooted and the control panel daemon has restarted.
← SUCCESS → restore defaults	This message is displayed after DNSMux's factory defaults have been successfully restored.

Troubleshooting and Recovery

DNSMux is designed for a lifetime of trouble-free operation, but should problems occur this chapter should be helpful in diagnosing and understanding them.

Guidelines

The following guidelines should be following in troubleshooting potential DNSMux-related problems.

Ensure you are working on the correct DNSMux

As much of the configuration of and interaction with DNSMux is done by a browser-based configurator that is capable of accessing any DNSMux in a cluster, you should ensure that you are accessing the DNSMux you think you are. The DNSMux being accessed by the configurator is identified in the header on upper left corner of the screen, by its assigned name and hostname or IP address. [???

DNSMux notifications

DNSMux sends notifications via email when certain events occur, for example when a server managed by DNSMux or a DNSMux unit becomes operational. Such notifications are sent to the configured Technical Contact(s), which vary based on function.

Below is a sample email notification sent by DNSMux:

```
Date: Wed, 9 Jun 2004 23:01:46 +0000
To: support@cainetworks.com
From: "DNSMux" <dnsmux@dnsmux>
Subject: DNSMux host ping.fail-over.com: site
207.46.130.108
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit

dnsmux v1.9.0

The tcp service failed.
```

In this example, the PING protocol is non-responsive on the DNSMux at IP address 207.46.130.108, causing DNSMux's health-check to conclude that TCP/IP is non-operational.

DNSMux cannot send notifications if the outgoing email (SMTP) server configured for DNSMux is inoperative or is configured to not accept messages from DNSMux, so it is important to ensure that the email server configured for DNSMux notifications is accessible to DNSMux and working properly.

Should DNSMux be unable to send notifications because an SMTP server is inoperative, those notifications will be queued and sent when the SMTP server becomes operational.

The following are the most common events for which DNSMux will send notifications:

Failed/recovered sever

The notification is sent by the first DNSMux in the cluster that detects the failure (as indicated by DNSMux's health checking). It is possible that due to timing issues related to DNSMux inter-communication that more than one DNSMux will report the condition.

When an inoperative server comes back into operation, all DNSMuxes in the cluster will detect this and the first one to do so sends the notification. It is possible that due to timing issues related to DNSMux inter-communication that more than one DNSMux will report the condition.

In both cases, notification is sent to the configured Technical Contact(s) configured for the server, as configured via the Hosts screen of the browser-based configurator.

Failed/recovered DNSMux

The notification is sent by the first DNSMux in the cluster that detects the failure (as indicated by the heartbeat between DNSMuxes in the cluster not resolving). Notification can take up to five minutes after the problem is first detected, while DNSMux attempts to determine whether the problem is persistent or may be a case of flapping. It is possible that due to timing issues related to DNSMux inter-communication that more than one DNSMux will report the condition.

In both cases, notification is sent to the Technical Contact(s) configured for the affected DNSMux unit, as configured via the Basic screen of the browser-based configurator.

Firmware version

DNSMux ships with the then-current firmware version, and from time to time firmware updates may be made available to address certain issues. Updated firmware can be supplied to you from CAI Networks, and may be updated via the Firmware screen of the browser-based configurator.

The firmware version installed in your DNSMux can be identified via the Firmware screen, and you should include this in any problem reports to CAI Networks. The format of the firmware version is *major release version.minor release version.patch level*.

Note Updating the DNSMux firmware causes a reboot of the DNSMux unit, so this should ideally be done during periods of low activity.

Rescue Mode

Should DNSMux's data structures become corrupted, DNSMux maintains a rescue partition on its media that contains information that can be used to recover the normal data structures.

DNSMux will automatically detect such corruption and automatically go into rescue mode to recover, and will display the following screen when access via the browser-based configurator is attempted:

DNSMux Rescue

Your DNSMux has failed to boot correctly. You can try rebooting it, and if it fails again, this page will come back. Some of the basic information can be set below. You can also make some changes using the control panel.

IP Address:

NetMask:

Gateway:

An optional private network on the second ethernet port

Internal IP Address:

NetMask:

Upload new firmware:

Factory Reset:

Power Management:

The Resuce screen will populate the latest saved addressing configuration, and this can be revised using the same method as in the Basic screen of the browser-based configurator.

In addition, the following functionality is available from the Rescue screen:

Upload new firmware

This is the same functionality as provided in the Firmware screen of the browser-based configurator. Enter the name of the file containing the DNSMux firmware to upload, or browse to it using the "Browse..." button.

Factory Reset

Pressing the “Overwrite all configuration” button will reset all DNSMux configuration settings to their factory values. It would then be necessary to use the control panel found on the front of the DNSMux unit to reset IP addresses in order to be able to access the DNSMux via the browser-based configurator.

Power Management

The “Reboot” button reboots the DNSMux unit while the “Shutdown” button shuts it down.