DNSMux™

Global IP Load Balancing / Traffic Management Appliance

User Guide

Version 1.0.3

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.

An attempt has been made to state all allowable values where applicable throughout this manual. Any values or parameters used beyond those stated may have unpredictable results.

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

www.cainetworks.com

Table Of Contents

Chapter 1

Introduction to DNSMux

Overview

DNSMux is an intelligent DNS nameserver, providing an enhanced alternative to ordinary DNS 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 proximity and affinity capabilities to automatically target users to the geographically closest sites and/or those serving the content they are seeking.

Peak performance is accomplished via load balancing, whereby DNSMux will 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 server it manages and report those that are unresponsive (either because certain processes are inoperative or because a server is down).

Multiple DNSMuxes can be deployed in a grid to efficiently serve users worldwide by automatically targeting them to the servers with the closest geographical proximity

DNSMux is also capable of targeting users to specific servers among a group of content-identical and content-disparate servers that have specific content with which they have affinity (based on locality, language, etc.). This matching of users to servers is driven by a customer-defined configuration based on each user's geographical location.

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 network is optional and is intended to be used for management purposes on a private network).

Once the DNSMux is network-accessible, DNSMux's browser-based configuration screens are used to set is used to host-specific details for each DNSMux that will act as a nameserver for the domains under DNSMux management. As configurations settings are made, the information is automatically echoed to all the DNSMuxes in the cluster so that any can stand in for any other in a failover scenario.

The settings for each DNSMux nameserver include:

- The hostname, 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
- 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 need to be setup with their related configurations. The settings for each zone include:

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

Each host within each zone (e.g. "www", "ftp", "mail", etc) need to be setup, and which content-identical servers, by hostname or IP address, are members of each zone needs to be defined. The settings for each host includes:

- The host name, e.g. "www", "ftp", "mail", etc.
- The zone to which the host belongs
- The content-identical servers, by hostname or IP address, that are members of the host
- The performance factor to assign to each server, based on its inherent performance power
- Which characteristics should be taken into account for load balancing (weight and/or health) 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 setup screen for:

- Changing the passwords for the Administrator and Observer users
- Specifying which servers, by hostname or IP address, are allowed and denied access
- Which other DNSMux nameservers in the cluster should be allowed to propagate configurations to this DNSMux nameserver

An optional configuration can then be set for whether users should be targeted by proxmity (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 (user IP addresses are determined by the geographical locations of their local DNS servers).

An optional configuration can also be done for targeting users based on affinity (to the servers that contain content related to them), via a three-step process:

- First, define the group of servers that contain identical content of a particular type
- Second, define classes of users, based on their geographical locations, that are consumers of the various content types, where geographical location can be either a country or something more granular, like a state, province, or city
- Third, associate the user classes with their respective server groups

There is also an option to specify whether or not proximity should be imposed on users who are governed by affinity

Once all DNSMuxes, are properly configured, they will offer the following functionality:

- They will perform address resolution and other functionality expected of any DNS nameserver
- They will target users to the best performing servers, within restrictions imposed by proximity and affinity rules
- They will direct users away from failed servers

Chapter 2

Configuration Guidelines

Introduction

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

- Which DNSMux(es) you will use as the “configuration master”
- When configuration changes should be propagated
- The default cache duration (TTL) to set
- Health-checking methods
- Load balancing methods
- Failover strategy

Each of these is described in the following paragraphs.

Configuration Master

In configuring the various DNSMuxes in a cluster, it is not necessary to configure each one manually: DNSMux is capable of automatically propagating the configuration from one DNSMux to one or more others. It is therefore recommended that you designate one DNSMux as a “configuration master” and perform the configuration settings that will apply to all DNSMuxes on that one.

It is necessary that you enable access on all DNSMux units that will be propagated by the configuration master by specifying the configuration master’s IP address in the “Propagation” field in the Allowed Hosts section of the Security setup screen in the GUI configurator.

Propagation

Whenever you make configuration changes in the GUI configurator, those changes 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. You explicitly indicate when want to have DNSMux propagate changes 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.

Note The configuration propagation feature can only function for DNSMuxes that can be reached via the network at the time that changes are made. For DNSMuxes that cannot be connected to at configuration time, those settings must be changed manually on the DNSMuxes that were not propagated to; or the configuration changes must be redone at a time when all DNSMuxes are available.

Delayed Application

Configuration changes made in DNSMux's GUI configurator can be activated immediately deferred to a particular time of day. You can set a "standing" time for propagation, and DNSMux will defer any configuration propagations until that time. You can instruct DNSMux to delay applying changes and specify the time for that in the Delayed Application section of the Zones setup screen in the GUI configurator.

Caching

Caching is an important and potentially problemmatic issue that needs to be taken into account when determining your DNSMux configuration strategy.

A key operational premise of DNS is that DNS servers are capable of caching DNS resolutions (hostname to IP address) so that, as a matter of efficiency, they do not need to request the resolution from a higher-level server all the time. While this is fine for static DNS resolutions, DNSMux-based resolutions are dynamic: users are directed on-the-fly to the most appropriate server based on ever-changing conditions. The DNSMux-issued DNS resolution must get all the way to the client application in order for the appropriate server to be accessed. It is therefore important that minimal cache durations are imposed, in DNS servers and elsewhere.

Default Cache Duration (TTL)

DNSMux is able to impose the cache duration for every DNS resolution it performs. In doing so, it instructs all downstream caches to cache the resolution for only the specified period of time. Once the cache duration expires, all caches should flush the resolution and re-request it if asked again.

The default cache duration, known as Time To Live or "TTL" in DNS terminology, can be specified 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.

Other Caches

In addition to DNS server caches, there are other caches external to DNSMux, and in some cases DNSMux may have little or no control over them.

For a Windows client, there are typically three caches that can impede the desired DNS operation. These three caches and their behavior are described below.

Local DNS cache

Each client computer will access a so-called local DNS server in order to translate hostnames into their corresponding IP addresses. The local DNS server caches hostname/IP address resolutions and serves them to clients when they make such requests.

If the local DNS server does not have the resolution in its cache, it in turn asks another DNS server, which in turn may ask another DNS server, etc. until one having the resolution is found. (This may eventually lead to the so-called authoritative DNS server, which, in your case, would be a DNSMux.)

DNS resolution records have a so-called TTL (Time To Live) value, which instructs the DNS server to retain the record for only that amount of time. Once the TTL has lapsed, the DNS server is *supposed* to flush the record from its cache; however, many DNS servers ignore the TTL value and retain the information for up to 3 days or more. For DNSMux configuration, we recommend setting a relatively short TTL value of 15 seconds so that DNSMux is queried frequently to get current information on DNS request resolution; however, that may be defeated by the ignored TTL.

Windows cache

As stated, a client will ask its local DNS server to resolve a hostname-to-IP-address conversion but before doing that, some client systems (like Windows) maintain their own DNS cache and will try to resolve the entry there. If the request can be resolved from the client's DNS cache, it does not ask the local DNS server to do the resolution.

The Windows Resolver Cache respects the value that was specified by the authoritative DNS server, so each resolution entry will remain in the cache only until the TTL has lapsed. The DNS cache is flushed upon reboot or use of the FLUSHDNS command.

Browser cache

The topmost client cache is the browser cache, in which recently-accessed hostnames and their corresponding IP addresses are held. Each time the browser is asked to visit a host by name, it first checks its local cache and if can resolve from there it does so.

If the hostname is not in the local cache, the browser checks the Windows cache and resolves from there. And, in turn, if the resolution is not contained in the Windows Resolver Cache, the local DNS server is queried.

Browser DNS caching rules vary by browser, and different elements of retrieved web pages may be treated differently for caching purposes.

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 because it has access to more relevant information than DNSMux – 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 one of the following methods:

- Weight
- Round Robin
- Weighted Round Robin

These methods work as follows:

Weight

The weight method generates more transactions to the IP servers which are best able to handle them. This determination is made by a static factor and a dynamic factor.

The static factor is the weight of a system imposed manually at configuration time which reflects the relative inherent performance of each server to one another. For example, a standard IP server would have a weight of 0 while a slower system would have some negative value and a faster system some positive value. Those values are taken into account in the algorithm so as to cause more transactions to be generated to the more powerful systems.

The dynamic factor is the current performance of each IP server. This is determined automatically by DNSMux every few seconds, by testing a series of protocols specified at configuration time against each server to determine its average current performance.

The dynamic performance factor, when combined with the static weight, are used to rank each DNSMux's IP servers to determine which is the best candidate to receive the next transaction.

Specifically, the way the algorithm works is to concurrently perform the sequential protocol checks on each IP server and track the total time (in milliseconds) for each server and add to it the configured weight * 100 for each server. This determines the ranking factors which are used to rank the IP servers from best to worst candidate.

Round Robin

Unlike the weight method, the round robin method does not take system power or current performance into account at all when assigning transactions to the IP servers. It simply sends each transaction to a different IP server in sequence, such that each IP server gets the same number of transactions.

Weighted Round Robin

The third method combines the other two methods into a single method. The result of that transactions are allocated in roughly a round robin sequence but with more transactions assigned to the better performing servers (whether they are performing better because they are more powerful or less loaded, or both).

So, for example, with Weighted Round Robin, if there were three servers and two of them were fast and one twice as slow as the others, the transactions might be allocated two to the first fast system, one to the slow system, and two to the other fast system, in sequence.

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 be in a state that it is unable to service user requests, DNSMux will automatically divert traffic to reliable IP servers until the problem machine is back in normal service, whereupon the problem machine is automatically put 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 performs a serial series of tests using the protocols that are configured in the Host setup screen. As available protocols may vary from server to server, you should take care when configuring the Hosts setup screen to ensure that the specified protocols to use for testing the servers in that host are installed.

The health check tracks the millisecond count for each protocol to return, and passes the total along to another DNSMux process which determines the state of each IP server and instructs each DNSMux to behave accordingly.

Refer to the discussions in Chapter 3 for information about how the health check affects DNSMux behavior.

Failover

With DNSMux, there are two types of failovers considered:

- The failure or unresponsivness of a DNSMux-managed server
- 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

Every 15 seconds, all DNSMuxes in the cluster perform a health check on the servers they manage. This health check performs a serial series of tests using the protocols that are configured in the Hosts setup screen.

When exercising each individual protocol on each IP server, DNSMux waits for up to 20 seconds for the protocol to return. If the protocol does not respond after three consecutive attempts, DNSMux assumes that protocol is non-functional. If the protocol responds correctly for three consecutive attempts, DNSMux considers it to be ok.

Rather than taking the IP server out of service, DNSMux ranks it below a certain threshold at the bottom of the candidate server list when new transactions are released, which has the effect of that IP server being excluded from receiving any transactions for a time.

This dynamic method works such that once the problem with the protocol is resolved, the IP server is brought back into service automatically with no manual intervention to DNSMux required.

Notification of the unresponsive protocol is optional and can be made in two ways:

- A DNSMux log entry is generated
- The configured technical contact for the IP server experiencing the problem is notified by email

Failure of a DNSMux

All the DNSMuxes in a grid 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, the World Wide Web has a series of 13 root DNS servers deployed worldwide which service all unresolved DNS lookups and regularly send queries to a huge volume of authoritative DNS servers that make up the World Wide Web. For domains that have multiple nameservers, these master servers query them all and take the first response that comes back, ignoring the others. In the event any DNSMux is down, its brothers are able to service these queries and thereby ensure normal and uninterrupted operation.

It is for this reason that every DNSMux installation must have 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

Chapter 3

Preparing for DNSMux Deployment

Introduction

If you are deploying DNSMux in your environment, it is likely that you already have one or more traditional DNS servers that you will be replacing with two or more DNSMuxes While the DNS concepts between ordinary DNS servers and DNSMux are the same, DNSMux 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:

- Determine the cities in which each of your hosts will be located under DNSMux
- Get and record the hostname, IP address, subnet, and gateway values for various servers
- Determine who the Technical Contact persons will be for each host and each DNSMux and their email addresses
- Set the TTL value on all your existing DNS servers to be the same as the value you will assign for DNSMux

Determine DNSMux City Locations

If you will be using the proximity and affinity features of DNSMux, it is important for that functionality to work properly that you accurately identify the city in which of your IP hosts will be located. (If you get this wrong, you can easily change it later.)

Determine Network Addresses

When configuring your DNSMuxes, you will need to know the hostname, IP address, netmask, and gateway for:

- Your existing DNS servers which will be replaced by DNSMux
- 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
- The timeserver(s) that may be used to supply the current time for your DNSMuxes

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.

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 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 would need to determine that.

Determine Technical Contacts and Their Email Addresses

DNSMux is capable of alerting the appropriate people whenever a DNSMux stops working (i.e., it stops sending heartbeat messages). There are two levels of contact people that should be configured:

- The technical contact for each host
- The technical contact for each DNS

If there are multiple users who should be notified, it is recommended to set up an email group address that includes those users so they are all notified and make that the technical contact email.

Reduce TTL Value

Typically, regular DNS nameservers specify a TTL value of several minutes if not hours (if not days). This is because DNS, without its enhanced behavior via DNSMux, is relatively static. DNSMux makes DNS much more dynamic, and therefore the TTL value must be quite short in order to prevent stale resolutions to remain in cache.

Since at any given moment, based on generally unpredictable user behavior, there may be cached resolutions with whatever TTL value you are using on dozens if not hundreds or thousands of DNS servers, you will need to let these resolutions expire before expecting to get any changed behavior by using DNSMux. This will impede the propagation of DNSMux-controlled DNS resolutions.

Rather than wait until you deploy DNSMux to change the TTL, it is recommended that you reduce the TTL in your current environment so that when you deploy DNSMux you can immediately see whether it is behaving as expected based on your configurations. This change should be made in advance of your DNSMux deployment by at least the value of the current TTL.

The default TTL value imposed by DNSMux is 15 seconds, which you may override as desired. Whatever that desired value is is the value you should set for your current nameservers (or use the default of 15 seconds).

Chapter 4

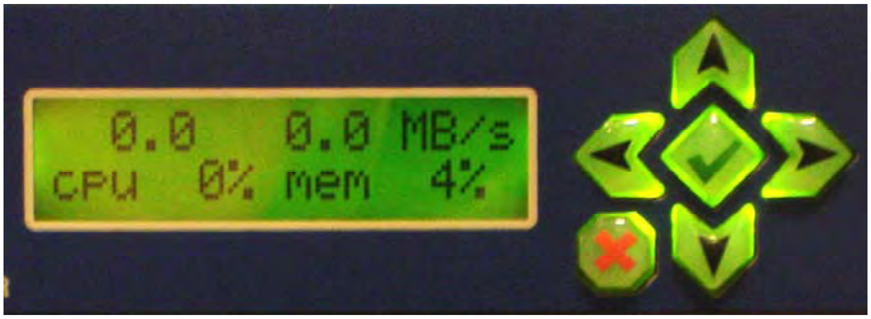
Using the Front Panel Controls

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 t:he following behavior:

←	LEFT	Moves between control panel functions and IP address octets
→	RIGHT	Moves between control panel functions and IP address octets
↑	UP	Cycles between valus in a function or increases a numeric value
↓	DOWN	Cycles between values in a function or decreases a numeric value
✓	CHECK	Accepts the current value into DNSMux, or cancel in unlock function
X	CANCEL	Cancels the current function, or backspace in unlock 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
- Open all ports on the firewall
- Reset settings to factory defaults
- Reboot the DNSMux unit

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, and you can stop on any operational function to use it. There are two types of operational functions that work as described below.

Setting Network Addresses

Functions that accept input are for setting network addresses. In those functions:

- Press the CHECK button to enter the function for modification
- Use the LEFT and RIGHT buttons to step between the four octets that comprise an IP address
- Use the UP and DOWN buttons while positioned in any group to increase or decrease the numeric value
- Press the CHECK button to accept the value into DNSMux

Opening the Firewall, Resetting Settings, and Rebooting

There are three operational functions that require no parameters: opening the firewall, resetting the settings to factory defaults, and rebooting the DNSMux unit. To invoke those functions:

- Press the CHECK button and hold it for four seconds

If you press the CHECK button and hold it for less than four seconds, the function will not be invoked.

If you enter an operational function and decide you do not want to invoke it, press the CANCEL button to cancel it.

Security Lockout

For security reasons, the control panel will lock itself after 10 to 20 minutes and require a pre-configured security code to unlock it. 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 unlock it.

Control Panel Tasks

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

Determining Throughput

The default screen shows the current throughput of the DNSMux unit. The first line shows the throughput, in megabytes per second, of input and output.

```
  0.0   0.0 MB/s
cpu  0% mem  3%
```

Setting Network Addresses

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

1. Advance to the function you want to set
2. Press the CHECK button to enter modification mode, and then use the LEFT and RIGHT buttons to switch between octets, and the UP and DOWN buttons to change the value of an octet.
3. When complete, press the CHECK button to accept the new value into DNSMux

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

```
←Net 1 IP→
 nnn.nnn.nnn.nnn
```

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

```
←Net 1 Netmask→
 nnn.nnn.nnn.nnn
```

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

```
←Net 1 Gateway→
  nnn.nnn.nnn.nnn
```

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

```
←Net 2 IP     →
 nnn.nnn.nnn
```

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

```
←Net 2 Gateway→
 nnn.nnn.nnn.nnn
```

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 LCD Pin:
→↑↓←→
```

The unlock sequence uses only the directional keys (LEFT, RIGHT, UP, and DOWN). In unlock mode, the CANCEL (“X”) button acts as a backspace key and the CHECK button cancels and returns to the main screen.

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

Rebooting the DNSMux Unit

When the control panel LCD 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 LCD daemon restarts.

Restoring the Factory Defaults

When the control panel LCD 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
```

Removing and Reinstating Firewall Protection

When the control panel LCD 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 by doing restoring the factory defaults (per the above) or via the GUI by adding a port to the firewall.

Chapter 5

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 DNSMux(es), collect all the relevant configuration information required and plan out the usage of the DNSMux(es) in your environment.

Ordinary DNS Servers Versus DNSMux

Whereas with ordinary DNS servers, you simply determine which DNS servers will manage which IP servers; with DNSMux, you additionally need to determine which DNS servers will service which geographies.

You also need to determine a load-balancing and failover plan across your various DNSMuxes to ensure that users get the best performance and uptime.

Refer to Chapter 3 for more information about planning your DNSMux environment.

Configuring Multiple DNSMuxes From A Single Point

If configuring multiple DNSMuxes, there is no need to specify full configuration information for each one: DNSMuxes have a peer-to-peer relationship with each other such that you can specify global configuration information (settings that are common between all DNSMuxes in a network) and those configuration settings will automatically be applied to all DNSMuxes in the network.

This feature works by propagating all the configuration settings on any DNSMux to all others whenever a screen is completed. Although the configuration changes are propagated immediately, you may specify a delay for the new settings to be activated on the other DNSMux units (as well as the current unit).

Note The configuration propagation feature can only function for DNSMuxes that can be reached via the network at the time that changes are made. For DNSMuxes that cannot be connected to at configuration time, those settings must be changed manually on the DNSMuxes that were not propagated to; or the configuration changes must be redone at a time when all DNSMuxes are available, whereupon they will be 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.

Setting The IP Addresses Via The Control Panel

Use the front panel LCD to set the IP address for either the network 1 or network 2 interface of the DNSMux unit.

If you are replacing an existing DNS Server with a DNSMux, you will assign the same IP address to the DNSMux as was assigned to the DNS Server.

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, and then change the netmask.
3. When complete press CHECK

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

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

Port Configuration for DNSMux

If reconfiguring the ports on a DNSMux unit that is located behind a firewall, the following ports must be kept open:

22 (TCP)	SSH port for propagation
51 (TCP)	Health daemon collaboration protocol
53 (UDP)	Used for accepting and sending DNS queries
80 or 433 (TCP)	Used for DNSMux's GUI configurator

Accessing the DNSMux Setup Screens

To access the setup screens for a DNSMux:

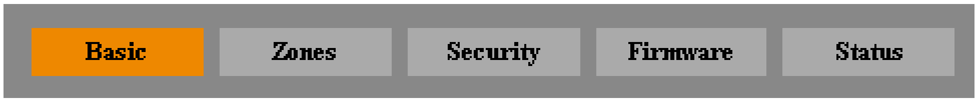
- In your browser, navigate to the IP address assigned to the DNSMux you want to configure, like "http://<dnsmux ip>/" or "https://<dnsmux ip>/"
- Enter the Administrator password
- Browse to the appropriate setup screen(s) to make the desired configuration changes

Note During initial setup, it is also recommended for security reasons that you change the factory-assigned Administrator password, via the Security screen.

Using The DNSMux Setup Screens

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

At the top of each setup 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

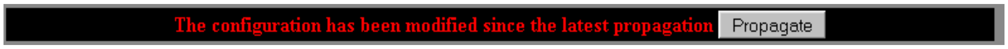
3. Use the Zones screen to configure the DNS zones and hosts for the zone

The settings made in the DNSMux setup screens will be propagated to other DNSMux nameservers in the cluster. For each DNSMux, you will need to allow access to whatever DNSMuxes will propagate to them.

Note The GUI configurator will not function if both port 80 (TCP) and port 433 (TCP) on the DNSMux unit are blocked.

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:



The configuration has been modified since the latest propagation

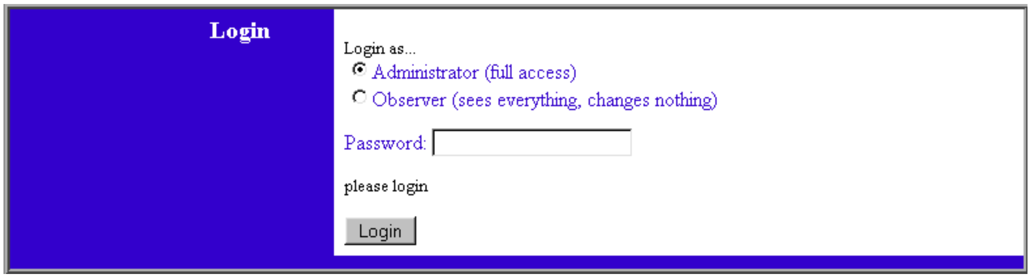
Hitting the "Propagate" button will immediately propagate all queued configuration changes to all allowed available DNSMuxes in the cluster.

Note The propagation bar only appears if configuration changes are queued and have not yet been propagated. Once propagation has completed, the propagation bar is no longer displayed.

Login Screen

The Login screen lets you login to DNSMux as either the Administrator or Observer user. The login screen is displayed each time you enter the DNSMux GUI.

The login screen looks like this:



Login

Login as...

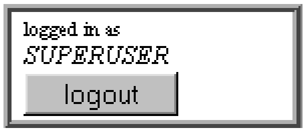
● Administrator (full access)

○ Observer (sees everything, changes nothing)

Password:

please login

Once you have logged in, your user name is displayed in the header. A logout button is also provided:



logged in as

SUPERUSER

Note The login information is held in a session cookie be re-supply the information between screens. If you have cookies disabled in your browser, you will need to login each time you change screens.

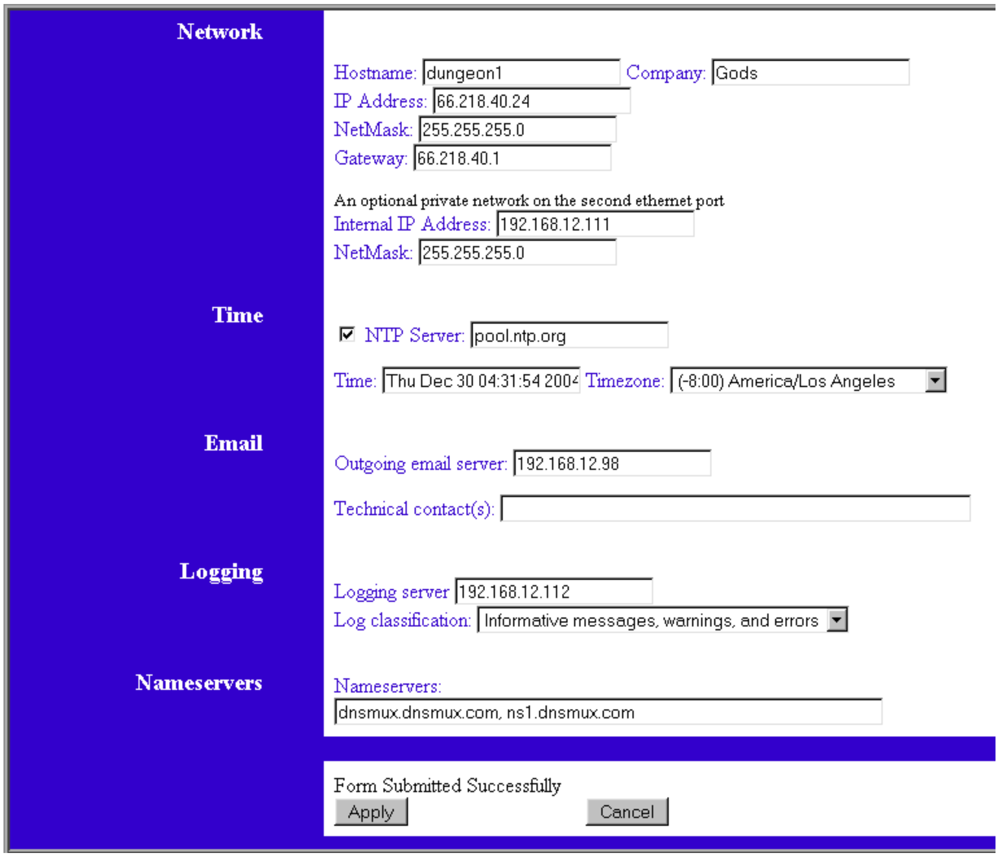
Basic Screen

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

From the Basic setup screen, you can configure the following:

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

The Basic setup screen looks like this:



Network

Hostname: dungeon1 Company: Gods
IP Address: 66.218.40.24
NetMask: 255.255.255.0
Gateway: 66.218.40.1

An optional private network on the second ethernet port
Internal IP Address: 192.168.12.111
NetMask: 255.255.255.0

Time

☑ NTP Server: pool.ntp.org

Time: Thu Dec 30 04:31:54 2004 Timezone: (-8:00) America/Los Angeles

Email

Outgoing email server: 192.168.12.98

Technical contact(s):

Logging

Logging server 192.168.12.112
Log classification: Informative messages, warnings, and errors

Nameservers

Nameservers:
dnsmux.dnsmux.com, ns1.dnsmux.com

Form Submitted Successfully

Network

These are the networking-related settings for the DNSMux nameserver you are configuring. Each DNSMux must have unique values for these settings, except for the NetMask and Gateway fields.

Hostname

This is the hostname for this DNSMux. The hostname is optional but it is recommended that you specify it. In other DNSMux configuration screens, nameservers that have a hostname assigned are shown by name, whereas nameservers with no hostname are shown by IP address.

IP Address

This is the IP address assigned to this DNSMux unit.

NetMask

This is the netmask assigned for devices on this network.

Gateway

This is the IP address of the network's gateway system.

Internal IP address

This is the IP address assigned for the second network card in the DNSMux, generally used for private access.

NetMask

This is the netmask for the second network.

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.

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.

Timezone

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

Email

DNSMux will send a notification to

Outgoing email server

Host name or IP address of the outgoing email server

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 (“,”).

Logging

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

DNSMux 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.

Logging server

Host name or IP address and optionally the port number of the system to which log files should be sent. 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.

Once you have configured the first DNSMux in your network, the specified nameservers specified are immediately echoed to all those DNSMuxes based on the nameservers addresses and when configuring those DNSMuxes the nameservers field will be automatically filled with those values.

Should you adjust the nameservers list for any DNSMux, that new information immediately updates all other DNSMuxes in the cluster..

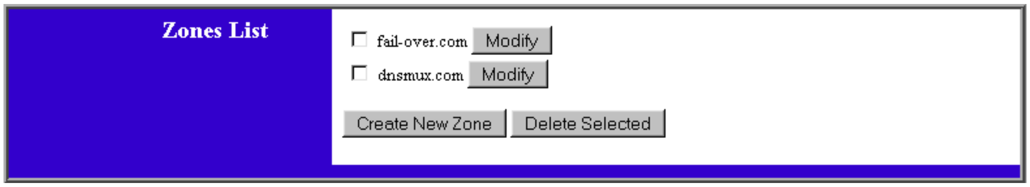
Zones Screen

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

From the Zone setup 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 setup screen looks like this:

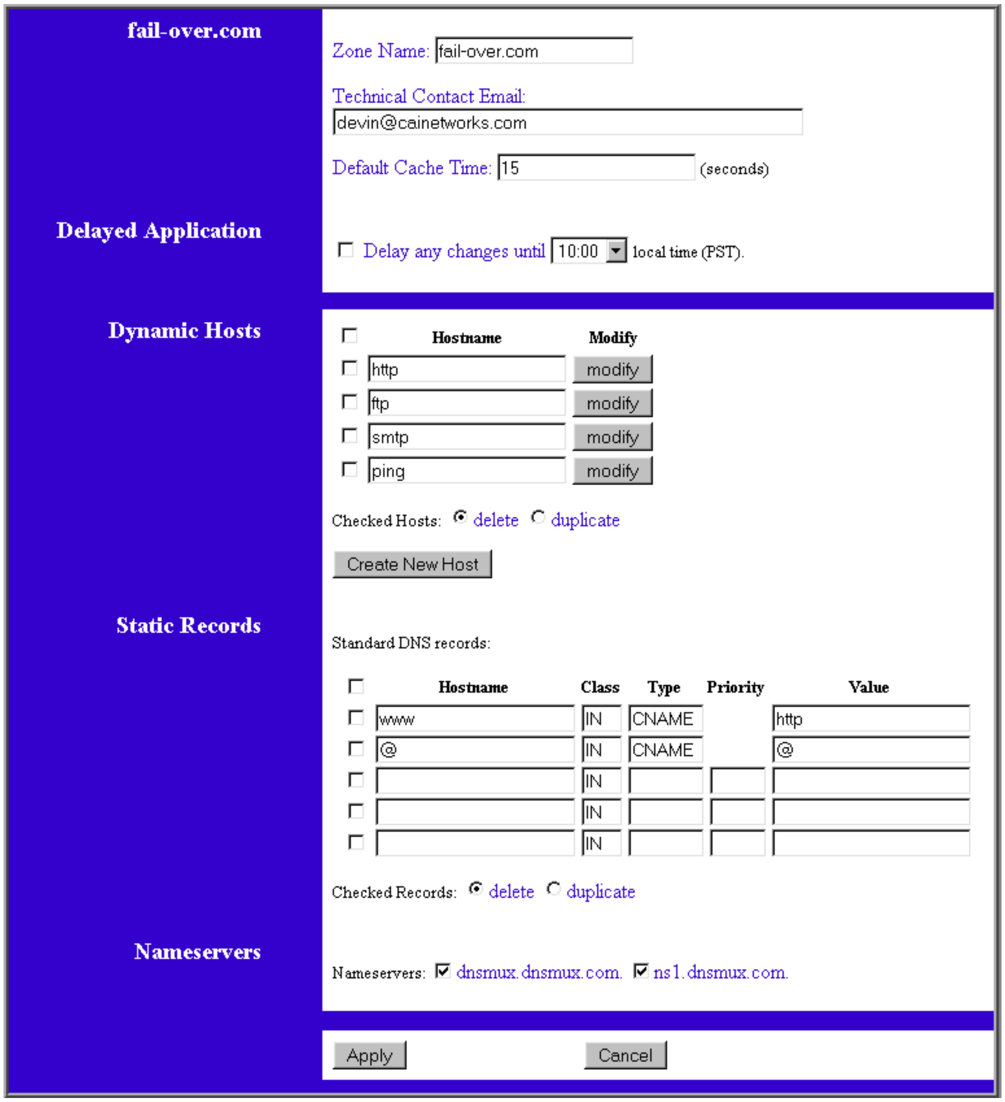


Zones List

□ fail-over.com

□ dnsmux.com

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



fail-over.com

Zone Name: fail-over.com

Technical Contact Email: devin@cainetworks.com

Default Cache Time: 15 (seconds)

Delayed Application

□ Delay any changes until 10:00 local time (PST).

Dynamic Hosts

□	Hostname	Modify
□	http	modify
□	ftp	modify
□	smtp	modify
□	ping	modify

Checked Hosts: ● delete ○ duplicate

Static Records

Standard DNS records:

□	Hostname	Class	Type	Priority	Value
□	www	IN	CNAME		http
□	@	IN	CNAME		@
□		IN			
□		IN			
□		IN			

Checked Records: ● delete ○ duplicate

Nameservers

Nameservers: ☑ dnsmux.dnsmux.com. ☑ ns1.dnsmux.com.

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

Specify the name of the zone.

Technical Contact Email

Specify the email address of the technical contact person for the zone.

Default Cache Time

Specify the Time To Live (TTL), in seconds, that should be broadcast to other DNS servers accessing this DNSMux nameserver. The TTL determines how long each of those DNS servers will retain the gotten DNS information in its cache before requesting it again.

The Default Cache Time default is 15 seconds. A TTL value for this field must be specified.

Refer to the discussion of 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 typically assign a TTL of 1 day to 3 days.

Delayed Application

Configuration changes can be activated immediately, or delayed until a specified time.

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 host DNS entries.

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 host DNS entries.

Hostname

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

Class

This is the class for the host entry

Type

This is the type of host entry (blank for A records)

Priority

This is the priority of the host entry

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 two exceptions:

- SOA records may not be configured, and there is no need to do so. DNSMux automatically sets the proper SOA configuration based on the technical contact email(s) specified for the zone
- NS records should not be configured. DNSMux automatically sets the proper NS config for other DNSMux nameservers in the cluster. Non-DNSMux nameservers should not be configured for the same domains as DNSMuxen are servicing

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.

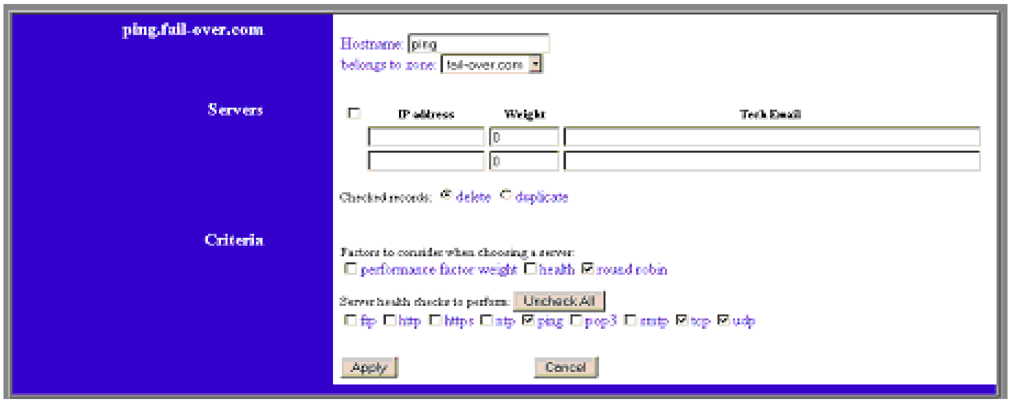
Host Screen (Subscreen of Zones screen)

The Host screen lets you configure the hosts managed by DNSMux and the servers that comprise them. The Host screen is accessible from the Zones screen: select the …

From the Host setup 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 setup screen looks like this:


ping.fail-over.com

Hostname: ping
belongs to zone: fail-over.com

Servers

□	IP address	Weight	Tech Email
		0	
		0	

Checked records: ● delete ○ duplicate

Criteria

Factors to consider when choosing a server:
□ performance factor weight □ health ☑ round robin

Server health checks to perform: Uncheck All
□ ftp □ http □ https □ ntp ☑ ping □ pop3 □ smtp ☑ tcp ☑ udp

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

This lets you specify all the IP servers 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. More powerful servers should be …. 0 is neutral

Tech Email — Select from the drop-down lists for each IP server the DNSMux nameserver to assign it to

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)

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 – tests connectivity of IP hosts
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 – faciliates Internet data transfer
udp	User Datagram Protocol – network transport protocol

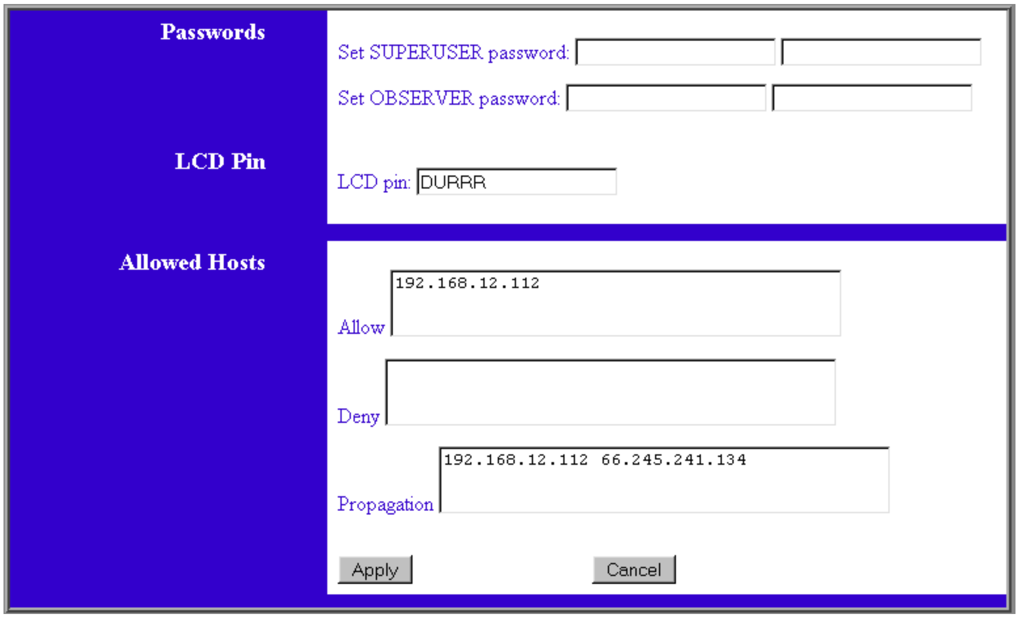
Security Screen

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

From the Security setup 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

The Security setup screen looks like this:



Passwords

Set SUPERUSER password:

Set OBSERVER password:

LCD Pin

LCD pin: DURRR

Allowed Hosts

Allow: 192.168.12.112

Deny:

Propagation: 192.168.12.112 66.245.241.134

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.

LCD 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. (The CANCEL and CHECK buttons have special functionality in control panel unlock mode and therefore cannot be used in the keypad sequence.)

Allowed hosts

DNSMux can be configured to block access to and from specified hosts. In configuring this, you either specify which hosts are allowed or which are denied (but not both). If allowed hosts are specified, only those hosts are granted access; if denied servers are specified, all servers but those specified are allowed.

Allow

Specify the IP address(es) of one or more hosts to allow access to, as hostname followed by subnet mask, separated by a slash ("/"). To specify multiple hosts, delimit them with commas.

If any allowed hosts are specified, the 'Deny' field must be empty.

Deny

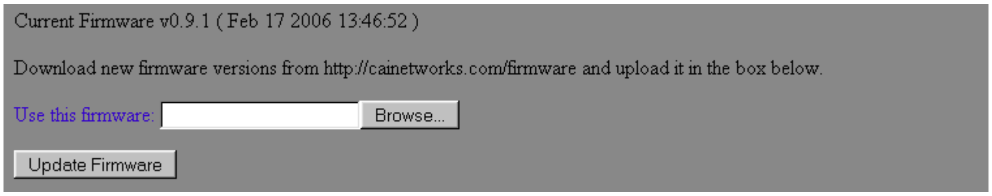
Specify the IP address(es) of one or more hosts to deny access to, as hostname followed by subnet mask, separated by a slash ("/"). To specify multiple hosts, delimit them with commas.

If any denied hosts are specified, the 'Allow' field must be empty.

Firmware Screen

The Firmware setup 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 setup screen looks like this:



Current Firmware v0.9.1 (Feb 17 2006 13:46:52)

Download new firmware versions from http://cainetworks.com/firmware and upload it in the box below.

Use this firmware:

Specify the file and hit the Accept button to update the firmware or the Cancel button to not proceed with the update.

Warning Updating DNSMux firmware will sever all active connections. This will not affect users if at least one DNSMux is functioning at all times.

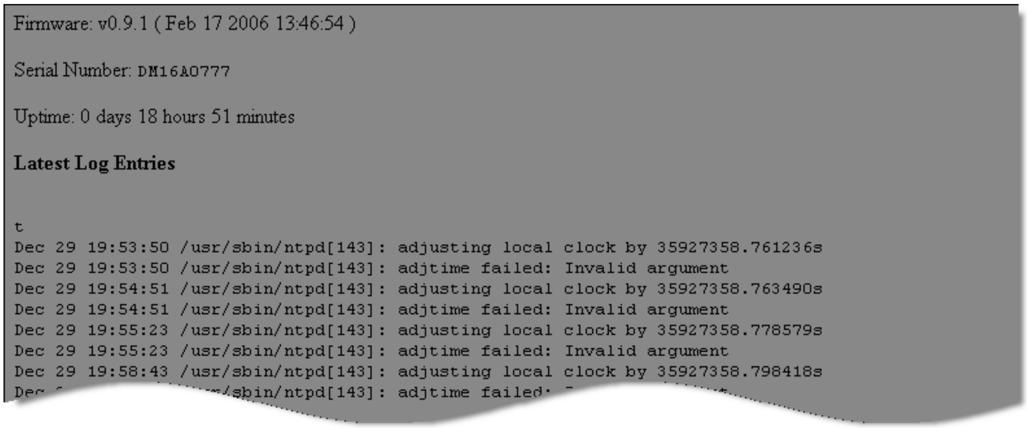
Status Screen

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

- The revision level of the installed firmware
- The serial number of the DNSMux unit
- How long ago the configuration was last updated

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

The status screen looks like this:



Firmware: v0.9.1 (Feb 17 2006 13:46:54)

Serial Number: DM16A0777

Uptime: 0 days 18 hours 51 minutes

Latest Log Entries

```
t
Dec 29 19:53:50 /usr/sbin/ntpd[143]: adjusting local clock by 35927358.761236s
Dec 29 19:53:50 /usr/sbin/ntpd[143]: adjtime failed: Invalid argument
Dec 29 19:54:51 /usr/sbin/ntpd[143]: adjusting local clock by 35927358.763490s
Dec 29 19:54:51 /usr/sbin/ntpd[143]: adjtime failed: Invalid argument
Dec 29 19:55:23 /usr/sbin/ntpd[143]: adjusting local clock by 35927358.778579s
Dec 29 19:55:23 /usr/sbin/ntpd[143]: adjtime failed: Invalid argument
Dec 29 19:58:43 /usr/sbin/ntpd[143]: adjusting local clock by 35927358.798418s
Dec              /sbin/ntpd[143]: adjtime failed:
```

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

Appendix A

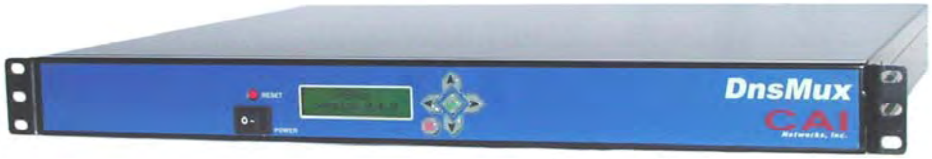
DNSMux Appliance Layout

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:

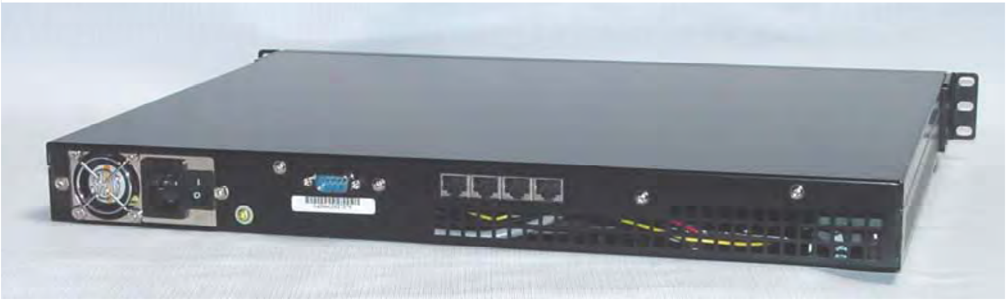


On the front of the DNSMux unit, you will find:

- An indicator light which lights red when the DNSMux unit is powered on
- A reset button for rebooting the unit
- 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 serial interface to which a serial or virtual terminal can be connected to configure the DNSMux unit via Telnet (as an alternative to using the GUI configurator)
- Two 100BaseT Ethernet interface ports

Appendix B

Front Panel LCD Values

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

Front Panel LCD Screen Values and Meanings

LCD value	Meaning.
CAI Networks DNSMux *n.n.nn*	Boot-up screen. Shows the vendor name and the firmware version.
0.0 0.0 MB/s 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 LCD 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 → *nnn.nnn.nnn.nnn*	The IP address for the first network card is shown and can be set.
←Net 1 Netmask→ *nnn.nnn.nnn.nnn*	The Netmask for the first network card is shown and can be set.
←Net 1 Gateway→ *nnn.nnn.nnn.nnn*	The gateway IP address for the first and second network cards is shown and can be set
←Net 2 IP → *nnn.nnn.nnn.nnn*	The IP address for the second network card is shown and can be set.
←Net 2 Netmask→ *nnn.nnn.nnn.nnn*	The Netmask for the second network card is shown and can be set.

LCD value	Meaning
← 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.
← 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 LCD daemon has restarted.
← SUCCESS → restore defaults	This message is displayed after DNSMux's factory defaults have been successfully restored.