



3-DNS® Administrator Guide

version 4.1

MAN-0046-00

Service and Support Information

Product Version

This manual applies to version 4.1 of the 3-DNS® Controller.

Obtaining Technical Support

Web	tech.f5.com
Phone	(206) 272-6888
Fax	(206) 272-6802
Email (support issues)	support@f5.com
Email (suggestions)	feedback@f5.com

Contacting F5 Networks

Web	www.f5.com
Toll-free phone	(888) 88BIG-IP
Corporate phone	(206) 272-5555
Fax	(206) 272-5556
Email	sales@f5.com
Mailing Address	401 Elliott Avenue West Seattle, Washington 98119

Legal Notices

Copyright

Copyright 1998-2001, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described herein. F5 reserves the right to change specifications at any time without notice.

Trademarks

F5 and the F5 logo, F5 Networks, BIG-IP, 3-DNS, GLOBAL-SITE, and SEE-IT are registered trademarks of F5 Networks, Inc. EDGE-FX, FireGuard, iControl, Internet Control Architecture, and IP Application Switch are trademarks of F5 Networks, Inc. In Japan, the F5 logo is trademark number 4386949, BIG-IP is trademark number 4435184, 3-DNS is trademark number 4435185, and SEE-IT is trademark number 4394516. All other product and company names are registered trademarks or trademarks of their respective holders.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

Export Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

FCC Compliance

This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference.

Operation of this equipment in a residential area may cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

Any modifications to this device - unless expressly approved by the manufacturer - can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This class A digital apparatus complies with Canadian I CES-003.

Standards Compliance

The product conforms to ANSI/UL Std 1950 and Certified to CAN/CSA Std. C22.2 No. 950.

Acknowledgments

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, <http://www.and.com>.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by Charles Hannum.

This product includes software developed by Charles Hannum, by the University of Vermont and Stage Agricultural College and Garrett A. Wollman, by William F. Jolitz, and by the University of California, Berkeley, Lawrence Berkeley Laboratory, and its contributors.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

In the following statement, "This software" refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with "386BSD" and similar operating systems. "Similar operating systems" includes mainly non-profit oriented systems for research and education, including but not restricted to "NetBSD," "FreeBSD," "Mach" (by CMU).

In the following statement, "This software" refers to the parallel port driver: This software is a component of "386BSD" developed by William F. Jolitz, TeleMuse.

This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).

This product includes software developed by Darren Reed. (© 1993-1998 by Darren Reed).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at <http://www.perl.com>.

This product includes software developed by Eric Young.

Rsync was written by Andrew Tridgell and Paul Mackerras, and is available under the Gnu Public License.

This product includes Malloc library software developed by Mark Moraes. (© 1988, 1989, 1993, University of Toronto).

This product includes open SSL software developed by Eric Young (eay@cryptsoft.com), (© 1995-1998).

This product includes open SSH software developed by Tatu Ylonen (ylo@cs.hut.fi), Espoo, Finland (© 1995).

This product includes open SSH software developed by Niels Provos (© 1999).

This product includes SSH software developed by Mindbright Technology AB, Stockholm, Sweden, www.mindbright.se, info@mindbright.se (© 1998-1999).

This product includes free SSL software developed by Object Oriented Concepts, Inc., St. John's, NF, Canada (© 2000).

This product includes software developed by Object Oriented Concepts, Inc., Billerica, MA, USA (© 2000).



Table of Contents

I Introduction

Getting started	1-1
Choosing a configuration tool	1-1
Browser support	1-2
Using the Administrator Kit	1-3
Stylistic conventions	1-3
Finding help and technical support resources	1-5
What is the 3-DNS Controller?	1-5
Internet protocol and network management support	1-6
Security features	1-6
Configuration scalability	1-7
System synchronization options	1-7
Configuring data collection for server status and network path data	1-7
Redundant system configurations	1-8
Managing traffic on a global network	1-9
A sample network layout	1-9
Synchronizing configurations and broadcasting performance metrics	1-10
Using a 3-DNS Controller as a standard DNS server	1-11
Load balancing connections across the network	1-13
Working with BIG-IP Controllers and other products	1-13
What's new	1-15
GLOBAL-SITE Controller server type	1-15
Split from BIND	1-15
User administration	1-16

2 Essential Configuration Tasks

Reviewing the configuration tasks	2-1
Planning issues for the network setup	2-1
Defining data centers and servers	2-2
Planning sync groups	2-3
Setting up communications between 3-DNS Controllers, data center servers, and big3d agents	2-4
Planning issues for the load balancing configuration	2-5
Using advanced traffic control features	2-6
Planning DNS zone file management	2-6
Replacing your DNS servers with 3-DNS Controllers	2-7
Running 3-DNS Controllers as authoritative for sub-domains only	2-9
Setting up a basic configuration	2-11
Setting up a data center	2-12
Setting up servers	2-15
Defining 3-DNS Controller servers	2-15
Defining BIG-IP Controller servers	2-17
Defining GLOBAL-SITE Controllers	2-20
Defining EDGE-FX Caches	2-22
Defining host servers	2-24
Configuring host SNMP settings	2-27
Working with sync groups	2-29
Configuring sync groups	2-29

Setting the time tolerance value 2-30
Configuring global variables 2-31

3

Configuring a Globally-Distributed Network

Understanding a globally-distributed network 3-1
Using Topology load balancing 3-1
Setting up a globally-distributed network configuration 3-2
 Adding data centers to the globally-distributed network configuration 3-2
 Adding 3-DNS Controllers to the globally-distributed network configuration 3-3
 Adding BIG-IP Controllers to the globally-distributed network configuration 3-4
 Adding wide IPs to the globally-distributed network configuration 3-5
 Configuring topology records for the globally-distributed
 network configuration 3-6
Additional configuration settings and tools 3-7
 Setting limits thresholds 3-7
 Other resources 3-8

4

Configuring a Content Delivery Network

Introducing the content delivery network 4-1
 Using the 3-DNS Controller in a CDN 4-1
 Reviewing a sample CDN configuration 4-2
Deciding to use a CDN provider 4-4
Setting up a CDN provider configuration 4-4
 Adding data centers 4-5
 Adding 3-DNS Controllers 4-5
 Adding servers 4-6
 Adding wide IPs and pools 4-6
 Adding a topology statement 4-8
Ensuring resource availability 4-9
Monitoring the configuration 4-9

5

Adding 3-DNS Controllers to the Network

Working with more than one 3-DNS Controller 5-1
Preparing to add a second 3-DNS Controller to your network 5-1
 Installing the hardware and running the First-Time Boot utility 5-2
 Making the principal 3-DNS Controller aware of the additional controller 5-2
Running the 3dns_add script 5-3
Verifying the configuration 5-3

6

Administration and Monitoring

Monitoring and administration utilities provided on the 3-DNS Controller 6-1
Working with the 3-DNS Maintenance menu 6-1
 Configuring zone files and wide IPs 6-3
 Viewing statistics 6-3

Working with the big3d agent	6-5
Managing synchronized files	6-6
Working with security issues	6-6
Configuring the 3-DNS Configuration utility	6-7
Working with syncd	6-8
Configuring NTP	6-8
Configuring NameSurfer	6-9
Managing users on the 3-DNS Controller	6-9
Changing the root password	6-9
Adding users for the Configuration utility	6-10
Using the MindTerm SSH Console	6-11
Using the Network Map	6-12
Viewing system statistics	6-13

7

Additional Load Balancing Options

Configuring load balancing using specialized modes	7-1
Setting up Quality of Service mode	7-1
Understanding QOS coefficients	7-2
Customizing the QOS equation	7-3
Using the Dynamic Ratio option	7-5
Working with the Global Availability mode	7-7
Configuring the Global Availability mode	7-8
A Global Availability configuration example	7-9
Setting up load balancing for services that require multiple ports	7-10
Ensuring availability for e-commerce, FTP, and other services that use multiple ports	7-11

Glossary

Index



|

Introduction

- Getting started
- Using the Administrator Kit
- Finding help and technical support resources
- What is the 3-DNS Controller?
- Managing traffic on a global network
- What's new

Getting started

The *3-DNS Administrator Guide* is designed to help you quickly configure your 3-DNS Controller to manage your wide-area network traffic and DNS. The Administrator Guide contains the following chapters:

- ◆ **Essential Configuration Tasks**
This chapter describes the tasks you must complete, regardless of the type of wide-area traffic management you want to configure.
- ◆ **Configuring a Globally Distributed Network**
This chapter describes the tasks you complete to set up a globally distributed network.
- ◆ **Configuring a Content Delivery Network**
This chapter describes the tasks you complete to set up a network that includes a CDN provider.
- ◆ **Adding 3-DNS Controllers to the Network**
This chapter describes the tasks you complete to configure additional 3-DNS Controllers in a network that already contains one or more 3-DNS Controllers.
- ◆ **Administration and Monitoring**
This chapter describes the administrative tasks you complete for the 3-DNS Controller, as well as the monitoring tools that are provided with the controller.
- ◆ **Additional Load Balancing Options**
This chapter describes the specialized load balancing modes, such as Quality of Service, that are available on the 3-DNS Controller.

Choosing a configuration tool

The 3-DNS Controller provides the following web-based and command line administrative tools that make for easy setup and configuration.

First-Time Boot utility

The First-Time Boot utility is a wizard that walks you through the initial system setup. The utility helps you quickly define basic system settings, such as a root password and the IP addresses for the interfaces that connect the 3-DNS Controller to the network. The First-Time Boot utility also helps you configure access to the 3-DNS web server, which hosts the web-based Configuration utility, as well as the NameSurfer™ application that you can use for DNS zone file management.

Configuration utility

The Configuration utility is a web-based application that you use to configure and monitor the 3-DNS Controller. Using the Configuration utility, you can define the load balancing configuration along with the network setup, including data centers, sync groups, and servers used for load balancing and path probing. In addition, you can configure advanced features such as topology settings and SNMP agents. The Configuration utility also monitors network traffic, current connections, load balancing statistics, performance metrics, and the operating system itself.

The 3-DNS web server, which hosts the Configuration utility, provides convenient access to downloads such as the SNMP MIB and documentation for third-party applications such as NameSurfer.

NameSurfer application

The NameSurfer application is a third-party application that automatically configures DNS zone files associated with domains handled by the 3-DNS Controller. You can use NameSurfer to configure and maintain additional DNS zone files on 3-DNS Controllers that run as master DNS servers. The Configuration utility provides direct access to the NameSurfer application, as well as the corresponding documentation for the application. Please note that your license allows you to manage a maximum of 100 IP addresses in the NameSurfer application. For more information, refer to the end-user license agreement included in your product shipment.

3-DNS Maintenance menu

The 3-DNS Maintenance menu is a command line utility that executes scripts which assist you in configuration and administrative tasks, such as installing the latest version of the **big3d** agent on all your systems, or editing the load balancing configuration files. You can use the 3-DNS Maintenance menu directly on the 3-DNS Controller, or you can use the menu when connected to the controller using a remote shell, such as the SSH client (**ssh** is configured on crypto 3-DNS Controllers only), or a standard RSH client (if **rsh** is configured).

Browser support

The Configuration utility, which provides web-based access to the 3-DNS Controller system configuration and features, supports the following browser versions:

- Netscape Navigator 4.5 and 4.7
- Microsoft Internet Explorer, version 4.02 or later

Using the Administrator Kit

The 3-DNS Administrator Kit provides simple steps for quick, basic configuration, and also provides detailed information about more advanced features and tools, such as the **3dnsmaint** command line utility. The information is organized into the guides described as follows.

- ◆ **3-DNS Installation Guide**

The *3-DNS Installation Guide* walks you through the basic steps needed to get the hardware plugged in and the system connected to the network. Most users turn to this guide only the first time that they set up a 3-DNS Controller. The Installation Guide also covers general network administration issues, such as setting up common network administration tools including Sendmail.

- ◆ **3-DNS Administrator Guide**

The *3-DNS Administrator Guide* provides examples of common wide-area load balancing solutions supported by the 3-DNS Controller. For example, in the Administrator Guide, you can find everything from a basic DNS request load balancing solution to a more advanced content acceleration load balancing solution.

- ◆ **3-DNS Reference Guide**

The *3-DNS Reference Guide* provides basic descriptions of individual 3-DNS Controller objects, such as wide IPs, pools, virtual servers, load balancing modes, the **big3d** agent, resource records, and production rules. It also provides syntax information for **3dnsmaint** commands, configuration utilities, the **wideip.conf** file, and system utilities.

- ◆ **Note**

*If you are configuring the 3-DNS module on the BIG-IP Controller, use the **BIG-IP Installation Guide** to set up and configure the hardware.*

Stylistic conventions

To help you easily identify and understand certain types of information, this documentation uses the stylistic conventions described below.

- ◆ **WARNING**

All examples in this documentation use only non-routable IP addresses. When you set up the solutions we describe, you must use IP addresses suitable to your own network in place of our sample IP addresses.

Identifying new terms

When we first define a new term, the term is shown in bold italic text. For example, a ***wide IP*** is a mapping of a fully-qualified domain name to a set of virtual servers that host the domain's content.

Identifying references to objects, names, and commands

We apply bold text to a variety of items to help you easily pick them out of a block of text. These items include web addresses, IP addresses, utility names, and portions of commands, such as variables and keywords. For example, the **nslookup** command requires that you include at least one **<ip_address>** variable.

Identifying references to other documents

We use italic text to denote a reference to another document. In references where we provide the name of a book as well as a specific chapter or section in the book, we show the book name in bold, italic text, and the chapter/section name in italic text to help quickly differentiate the two. For example, you can find information about **3dnsmaint** commands in the ***3-DNS Reference Guide***.

Identifying command syntax

We show actual, complete commands in bold Courier text. Note that we do not include the corresponding screen prompt, unless the command is shown in a figure that depicts an entire command line screen. For example, the following command sets the 3-DNS Controller load balancing mode to Round Robin:

```
lb_mode rr
```

Table 1.1 explains additional special conventions used in command line syntax.

Item in text	Description
\	Continue to the next line without typing a line break.
< >	You enter text for the enclosed item. For example, if the command has <your name> , type in your name.
	Separates parts of a command.
[]	Syntax inside the brackets is optional.
...	Indicates that you can type a series of items.

Table 1.1 *Command line conventions used in this manual*

Finding help and technical support resources

You can find additional technical documentation about the 3-DNS Controller in the following locations:

◆ **Release notes**

Release notes for the 3-DNS Controller are available from the home page of the Configuration utility. The release note contains the latest information for the current version including a list of new features and enhancements, a list of fixes, and a list of known issues.

◆ **Online help for 3-DNS Controller features**

You can find help online in three different locations:

- The Configuration utility home page has PDF versions of the guides included in the Administrator Kit. The 3-DNS Controller software upgrades replace the guides with updated versions as appropriate.
- The Configuration utility has online help for each screen. Simply click the **Help** button in the toolbar.
- Individual commands have online help, including command syntax and examples, in standard UNIX man page format. Type the command followed by the question mark option (-?), and the 3-DNS Controller displays the syntax and usage associated with the command.

◆ **Third-party documentation for software add-ons**

The Configuration utility contains online documentation for the third-party software included with the 3-DNS Controller, including NameSurfer.

◆ **Technical support through the World Wide Web**

The F5 Networks Technical Support web site, <http://tech.F5.com>, contains the Ask F5 knowledge base and provides the latest technical notes and updates for administrator guides (in PDF and HTML formats). To access this site you must first email askf5@f5.com and obtain a customer ID and a password.

What is the 3-DNS Controller?

The 3-DNS Controller is a network appliance that manages and balances traffic over global networks. The 3-DNS Controller manages network traffic patterns using load balancing algorithms, topology-based routing, and production rules that control and distribute traffic according to specific policies. The system is highly configurable, and its web-based and command line configuration utilities allow for easy system setup and monitoring.

The 3-DNS Controller provides a variety of features that meet special needs. For example, with this product you can:

- Configure a content delivery network with a CDN provider
- Guarantee multiple port availability for e-commerce sites
- Provide dynamic persistence by maintaining a mapping between an LDNS IP address and a virtual server in a wide IP pool
- Direct local clients to local servers for globally-distributed sites using Topology load balancing
- Change the load balancing configuration according to current traffic patterns or time of day
- Customize load balancing modes
- Set up load balancing among BIG-IP Controllers, EDGE-FX Caches, and other load-balancing hosts
- Monitor real-time network conditions

Internet protocol and network management support

The 3-DNS Controller supports both standard DNS protocol and the 3-DNS Controller iQuery protocol (a protocol used for collecting dynamic load balancing information). The 3-DNS Controller also supports administrative protocols, such as Simple Network Management Protocol (SNMP), and Simple Mail Transfer Protocol (SMTP) (outbound only), for performance monitoring and notification of system events. For administrative purposes, you can use SSH (distributed only on crypto 3-DNS Controllers), RSH, Telnet, and FTP. The Configuration utility supports HTTPS, for secure web browser connections using SSL (distributed only on crypto 3-DNS Controllers), as well as standard HTTP connections.

The 3-DNS Controller's SNMP agent allows you to monitor status and current traffic flow using popular network management tools, including the Configuration utility. The SNMP agent provides detailed data such as current connections being handled by each virtual server.

Security features

The 3-DNS Controller offers a variety of security features that can help prevent hostile attacks on your site or equipment.

◆ **Secure administrative connections**

Crypto versions of 3-DNS Controllers support Secure Shell (SSH) administrative connections using the Mindterm SSH Console, for browser-based remote administration, and SSH for remote

administration. The 3-DNS web server, which hosts the web-based Configuration utility, supports SSL connections as well as user authentication.

- ◆ **Secure iQuery communications**
Crypto versions of 3-DNS Controllers also support Blowfish encryption for iQuery communications between 3-DNS Controllers and other appliances running the **big3d** agent.
- ◆ **TCP wrappers**
TCP wrappers provide an extra layer of security for network connections.

Configuration scalability

The 3-DNS Controller is a highly scalable and versatile solution. You can configure the 3-DNS Controller to manage up to several hundred domain names, including full support of domain name aliases. The 3-DNS Controller supports a variety of media options, including Fast Ethernet, Gigabit Ethernet, and FDDI; the controller also supports multiple network interface cards that can provide redundant or alternate paths to the network.

◆ Note

If you use NameSurfer to manage your DNS zone files, you can configure only up to 100 IP addresses and domain names.

System synchronization options

The 3-DNS Controller sync group feature allows you to automatically synchronize configurations from one 3-DNS Controller to the other 3-DNS Controllers in the network, simplifying administrative management. The synchronization feature offers a high degree of administrative control. For example, you can set the controller to synchronize a specific configuration file set, and you can also set which 3-DNS Controllers in the network receive the synchronized information and which ones do not.

Configuring data collection for server status and network path data

The 3-DNS Controller platform includes a **big3d** agent, which is an integral part of 3-DNS Controller load balancing. The **big3d** agent continually monitors the availability of the servers that the 3-DNS Controller load balances. It also monitors the integrity of the network paths between the servers that host the domain and the various local DNS servers that attempt to connect to the domain. The **big3d** agent runs on 3-DNS Controllers, BIG-IP Controllers, EDGE-FX Caches, and GLOBAL-SITE Controllers

distributed throughout your network. Each **big3d** agent broadcasts its collected data to all of the 3-DNS Controllers in your network, ensuring that all 3-DNS Controllers work with the latest information.

The **big3d** agent offers a variety of configuration options that allow you to choose the data collection methods you want to use. For example, you can configure the **big3d** agent to track the number of hops (intermediate system transitions) along a given network path, and you can also set the **big3d** agent to collect host server performance information using the SNMP protocol. For further details on the **big3d** agent, refer to Chapter 3, *The big3d Agent*, in the *3-DNS Reference Guide*.

Redundant system configurations

A **redundant system** is essentially a pair of 3-DNS Controller units, one operating as an active unit responding to DNS queries, and one operating as a standby unit. If the active unit fails, the standby unit takes over and begins to respond to DNS queries while the other controller reboots and becomes a standby unit.

The 3-DNS Controller actually supports two methods of checking the status of the peer system in a redundant system:

- ◆ **Hardware-based fail-over**

In a redundant system that has been set up with hardware-based fail-over, the two units in the system are connected to each other directly using a fail-over cable attached to the serial ports. The standby controller checks on the status of the active controller every second using this serial link.

- ◆ **Network-based fail-over**

In a redundant system that has been set up with network-based fail-over, the two units in the system communicate with each other across an Ethernet network instead of going across a dedicated fail-over serial cable. The standby controller checks on the status of the active controller every second using the Ethernet.

- ◆ **Note**

In a network-based fail-over configuration, the standby 3-DNS Controller immediately takes over if the active unit fails. If a client had queried the failed controller, and not received an answer, it automatically re-issues the request (after 5 seconds) and the standby unit, functioning as the active controller, responds.

Managing traffic on a global network

This section provides a brief overview of how 3-DNS Controllers work within a global network and how they interact with BIG-IP Controllers, EDGE-FX Caches, GLOBAL-SITE Controllers, and host machines in the network. The section also illustrates how the 3-DNS Controller works with the **big3d** agents that run in various locations in the network, and with the local DNS servers that make DNS requests on behalf of clients connecting to the Internet.

The following sample configuration shows the 3-DNS Controllers that load balance connections for a sample Internet domain, **domain.com**.

A sample network layout

The 3-DNS Controllers in your network sit in specific data centers, and work in conjunction with BIG-IP Controllers, EDGE-FX Caches, GLOBAL-SITE Controllers, and host servers that also sit in your network data centers. All 3-DNS Controllers in the network can receive and respond to DNS resolution requests from the LDNS servers that clients use to connect to the domain.

Figure 1.1 illustrates the layout of the 3-DNS Controllers, the BIG-IP Controllers, and the host servers in the three data centers. The Los Angeles data center houses one 3-DNS Controller and one BIG-IP Controller, as does the New York data center. The Tokyo data center houses only one 3-DNS Controller and one host server.

In the Los Angeles and New York data centers, the **big3d** agent runs on the BIG-IP Controllers and the 3-DNS Controllers, but in the Tokyo data center, the **big3d** agent runs only on the 3-DNS Controller. Each **big3d** agent collects information about the network path between the data center where it is running and the client's LDNS server in Chicago, as illustrated by the red lines. Each **big3d** agent also broadcasts the network path information it collects to the 3-DNS Controllers running in each data center, as illustrated by the green, blue, and purple lines.

◆ **Note**

*Each BIG-IP Controller, EDGE-FX Cache, GLOBAL-SITE Controller, and 3-DNS Controller in a data center typically runs a **big3d** agent.*

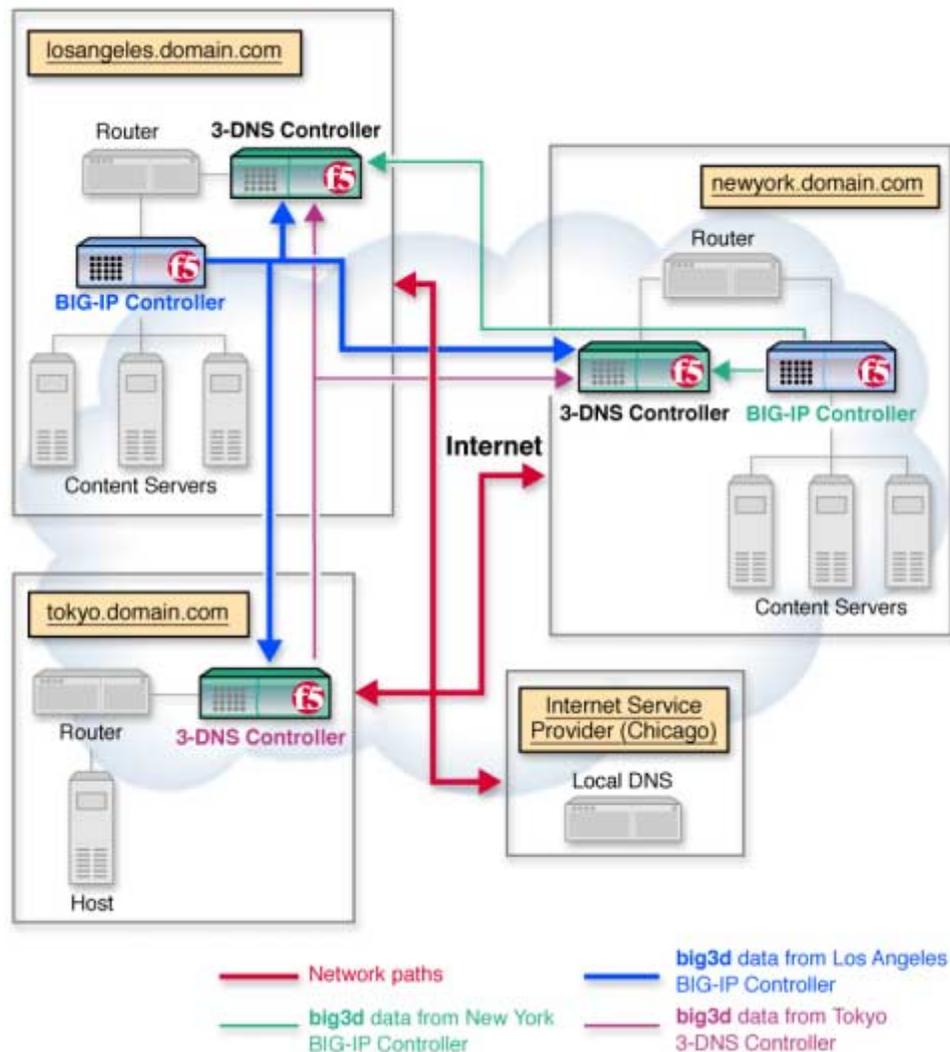


Figure 1.1 A sample network layout

Synchronizing configurations and broadcasting performance metrics

The 3-DNS Controllers typically work in sync groups, where a group of controllers shares load balancing configuration settings. In a sync group, any controller that has new configuration changes can broadcast the changes to any other controller in the sync group, allowing for easy administrative maintenance. To distribute metrics data among the controllers in a sync group, the principal 3-DNS Controller sends requests to the **big3d** agents in the network, asking them to collect specific performance and path data.

Once the **big3d** agents collect the data, they each broadcast the collected data to all controllers in the network, again allowing for simple and reliable metrics distribution.

Using a 3-DNS Controller as a standard DNS server

When a client requests a DNS resolution for a domain name, an LDNS sends the request to the 3-DNS Controller that is authoritative for the zone. The 3-DNS Controller first chooses the best available virtual server out of a pool to respond to the request, and then returns a DNS resource record to the requesting local DNS server. The LDNS server uses the answer for the period of time defined within the resource record. Once the answer expires, however, the LDNS server must request name resolution all over again to get a fresh answer.

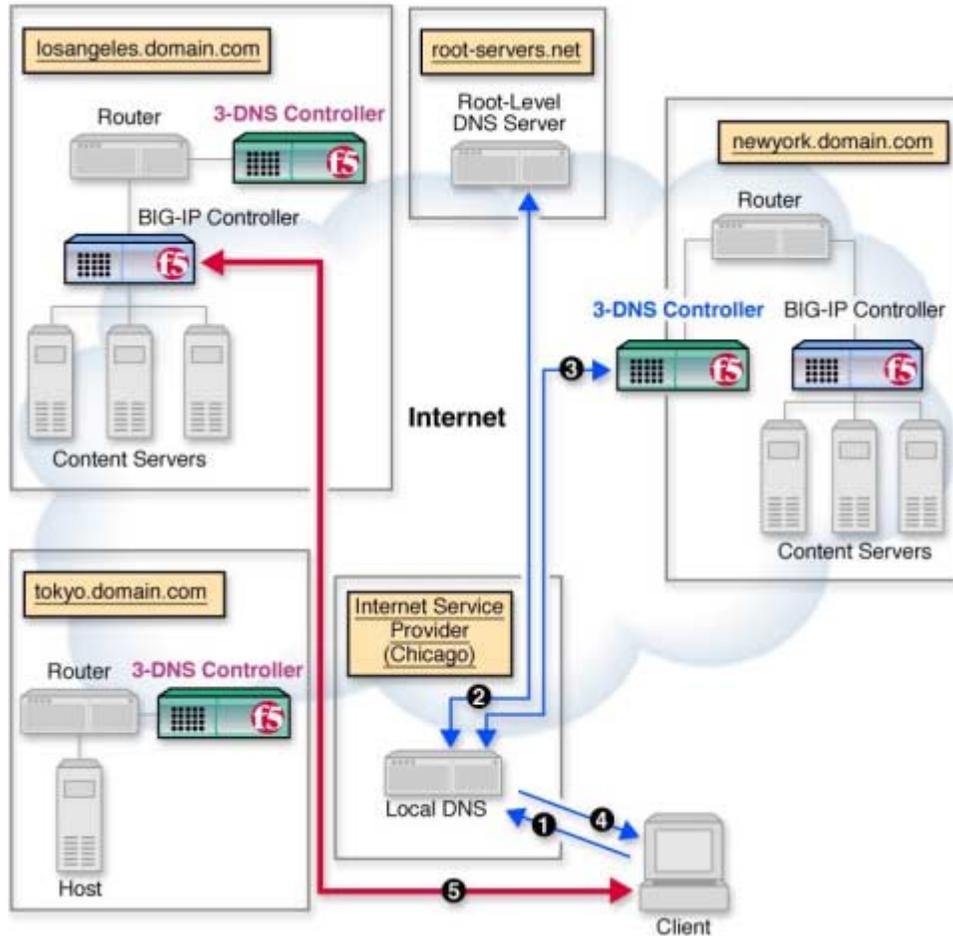


Figure 1.2 DNS name resolution process

Figure 1.2 illustrates the specific steps in the name resolution process.

1. The client connects to an Internet Service Provider (ISP) and queries the local DNS server to resolve the domain name **www.domain.com**.
2. If the information is not already in the LDNS server's cache, the local DNS server queries a root server (such as InterNIC's root servers). The root server returns the IP address of a DNS associated with **www.domain.com**, which in this case runs on the 3-DNS Controller.

3. The LDNS then connects to the 3-DNS Controller looking to resolve the **www.domain.com** name. The 3-DNS Controller uses a load balancing mode to choose an appropriate virtual server to receive the connection, and then returns the virtual server's IP address to the LDNS.
4. The LDNS ends the connection to the 3-DNS Controller and passes the IP address to the client.
5. The client connects to the IP address through an ISP.

Load balancing connections across the network

Each of the 3-DNS Controller load balancing modes can provide efficient load balancing for any network configuration. The 3-DNS Controller bases load balancing on pools of virtual servers. When a client requests a DNS resolution, the 3-DNS Controller uses the specified load balancing mode to choose a virtual server from a pool of virtual servers. The resulting answer to this resolution request is returned as a standard **A** record.

Although some load balancing configurations can get complex, most load balancing configurations are relatively simple, whether you use a static load balancing mode or a dynamic load balancing mode. More advanced configurations can incorporate multiple pools, as well as advanced traffic control features, such as topology or production rules.

For more information on specific load balancing modes, see *Load Balancing* in the *3-DNS Reference Guide*. For more information on load balancing configurations, review the sample configurations in Chapter 3, *Configuring a Globally-Distributed Network*, and Chapter 4, *Configuring a Content Delivery Network*. If you are unfamiliar with the 3-DNS Controller, you may also want to review Chapter 2, *Essential Configuration Tasks*.

Working with BIG-IP Controllers and other products

The 3-DNS Controller balances connections across a group of virtual servers that run in different data centers throughout the network. You can manage virtual servers from the following types of products:

- ◆ **BIG-IP Controllers**
A BIG-IP Controller virtual server maps to a series of content servers.
- ◆ **EDGE-FX Caches**
An EDGE-FX Cache virtual server maps to cached content that gets refreshed at frequent intervals.
- ◆ **Generic hosts**
A host virtual server can be an IP address or an IP alias that hosts the content.

◆ **Other load balancing hosts**

Other load balancing hosts map virtual servers to a series of content hosts.

Figure 1.3 illustrates the hierarchy of how the 3-DNS Controller manages virtual servers.

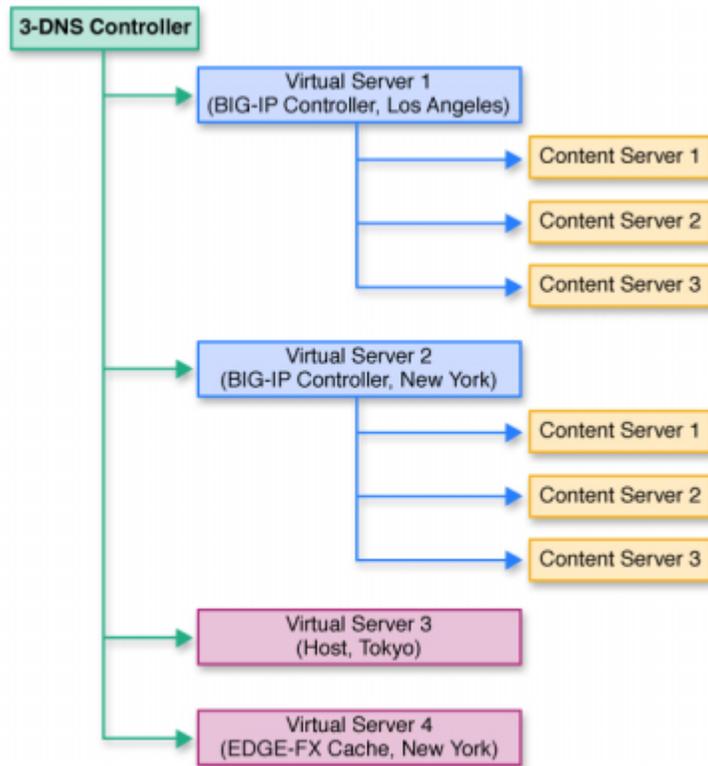


Figure 1.3 The 3-DNS Controller's load balancing management

Comparing 3-DNS Controllers and BIG-IP Controllers

While both controllers provide load balancing, one of the significant differences between the 3-DNS Controller and the BIG-IP Controller is that the 3-DNS Controller responds to DNS requests issued by an LDNS on behalf of a client, while the BIG-IP Controller provides connection management between a client and a back-end server.

Once the 3-DNS Controller returns a DNS answer to an LDNS, the conversation between the LDNS and the 3-DNS Controller ends, and the client connects to the IP address returned by the 3-DNS Controller. Unlike

the 3-DNS Controller, the BIG-IP Controller sits between the client and the content servers. It manages the client's entire conversation with the content server.

What's new

The 3-DNS Controller offers the following major new features in addition to many other enhancements.

GLOBAL-SITE Controller server type

The 3-DNS Controller can now collect network metrics from GLOBAL-SITE Controllers, using iQuery and the **big3d** agent. Note that the GLOBAL-SITE Controller does not manage virtual servers, and is not used for load balancing. For information on configuring GLOBAL-SITE Controllers, refer to *Defining GLOBAL-SITE Controllers*, on page 2-20.

Split from BIND

The DNS engine for the 3-DNS Controller no longer relies on BIND for DNS resolution. Multiple benefits include:

- ◆ You can upgrade the version of BIND independently of 3-DNS Controller upgrades.
- ◆ You can use the 3-DNS Controller to load balance DNS queries to your wide IPs, and redirect other DNS requests to an alternate DNS server.
- ◆ You can now add an unlimited number of wide IP aliases to your configuration.
- ◆ You can use the following wildcard characters in wide IP names and aliases:
 - The asterisk character (*) can replace multiple characters in a wide IP name or alias.
 - The question mark character (?) can replace a single character in a wide IP name or alias.

For more information about using wildcard characters, please see the online help for either the Add a New Wide IP screen or the Modify a Wide IP Alias screen, in the Configuration utility.

User administration

The 3-DNS Controller now has a partial read/write user level. When you assign the partial read/write level to a user, he or she can enable or disable servers, virtual servers, and wide IPs, but cannot add or delete any part of the configuration. For more information on configuring user administration in the Configuration utility, please see the online help for the User Administration screen. For more information on user administration in general, please refer to Chapter 6, *Administration and Monitoring*.



2

Essential Configuration Tasks

- Reviewing the configuration tasks
- Planning issues for the network setup
- Planning issues for the load balancing configuration
- Using advanced traffic control features
- Planning DNS zone file management
- Setting up a basic configuration
- Setting up a data center
- Setting up servers
- Working with sync groups
- Configuring global variables

Reviewing the configuration tasks

Once you have completed the First-Time Boot utility, you set up the network and load balancing aspects of the 3-DNS Controller. The 3-DNS Controller has three essential configuration tasks that all users must complete, regardless of the chosen load balancing solution.

The 3-DNS Controller has three essential configuration tasks that must be completed, regardless of the type of configuration you are setting up:

- ◆ Configure the physical aspects of your load balancing network, which includes the following:
 - Data centers
 - Data center servers and their virtual servers
 - Communications between the controller and other servers
 - 3-DNS Controller synchronization (if you have more than one in your network)
- ◆ Configure the logical aspects of your load balancing network, including wide IPs and pools
- ◆ Configure the global load balancing modes and global variables

Planning issues for the network setup

After you finish running the First-Time Boot utility, and connect each controller to the network, you can set up the network and load balancing configuration on one 3-DNS Controller, and let the sync group feature automatically broadcast the configuration to the other 3-DNS Controllers in the network. You do not have to configure the 3-DNS Controllers individually, unless you are planning an advanced configuration that requires different configurations for different data centers, or you are configuring the 3-DNS Controllers from the command line.

◆ Tip

*If you are configuring additional controllers in a network that already has 3-DNS Controllers in it, please review Chapter 5, **Adding 3-DNS Controllers to the Network**.*

During the network setup phase, you define three basic aspects of the network layout, in the following order:

- **Data centers**
Data centers are the physical locations that house the equipment you use for load balancing.

- **Data center servers**

The data center servers that you define in the network setup include the 3-DNS Controllers, BIG-IP Controllers, EDGE-FX Caches, and host machines that you use for load balancing. Data center servers can also include GLOBAL-SITE Controllers, from which the 3-DNS Controller gathers network metrics.

- **Sync group**

A *sync group* defines the group of 3-DNS Controllers that shares configuration settings and path data.

◆ **Note**

During the network setup phase of configuration, we recommend that you connect to the 3-DNS Controller from a remote workstation where you can complete the remaining configuration tasks using the web-based Configuration utility.

Defining data centers and servers

It is important that you define all of your data centers before you begin defining the data center servers because when you define a server, you specify the data center where the server runs. You do this by choosing a data center from the list of data centers you have already defined. To define a data center, you need only specify the data center name. To define a server, however, you need to specify the following items:

- Server type (3-DNS Controller, BIG-IP Controller, EDGE-FX Cache, GLOBAL-SITE Controller, or host)
- Server IP address (or shared IP alias for redundant systems)
- Name of the data center where the server runs
- **big3d** agent factories (BIG-IP Controllers, 3-DNS Controllers and EDGE-FX Caches, and GLOBAL-SITE Controllers only)
- Virtual servers managed by the server (BIG-IP Controllers, EDGE-FX Caches, and hosts only)
- SNMP host probing settings (hosts only)

◆ **Note**

*One important aspect of planning your network setup is to decide how to set up the **big3d** agent, and which ports you need to open for communications between the controllers in your network. See Chapter 3, **The big3d Agent**, in the **3-DNS Reference Guide**, for help with determining how both of these issues affect your installation.*

Planning sync groups

A *sync group* is a group of 3-DNS Controllers that share information. In a sync group, a *principal* 3-DNS Controller issues requests to the **big3d** agents to gather metrics data. Both the principal controller and the *receiver* 3-DNS Controllers in the group receive broadcasts of metrics data from the **big3d** agents. All controllers in the group also receive broadcasts of updated configuration settings from the 3-DNS Controller that has the latest configuration changes.

When you define the sync group, select 3-DNS Controllers from the list of servers you have already defined. The sync group lists the controllers in the order in which you selected them. The first controller in the list is the principal 3-DNS Controller. The remaining controllers in the list are receiver 3-DNS Controllers. If the principal controller becomes disabled, the next controller in the list becomes the principal 3-DNS Controller until the original principal controller comes back online.

Understanding how sync groups work

The sync group feature synchronizes individual configuration files, such as **wideip.conf** and other files that store system settings. You have the option of adding files to the synchronization list.

The controllers in a sync group operate as peer servers. At set intervals, the **syncd** daemon compares the timestamps of the configuration files earmarked for synchronization on all of the controllers. If the timestamp on a specific file differs between controllers, the controller with the latest file broadcasts the file to all of the other controllers in the group.

Understanding how the time tolerance variable affects sync groups

The time tolerance variable is a global variable that defines the number of seconds that one 3-DNS Controller's time setting can be ahead or behind another 3-DNS Controller's time setting. If the difference between the times on the controllers is greater than the time tolerance, the time setting on the controller running behind is reset to match the controller with the most recent time. For example, if the time tolerance is 5 seconds, and one 3-DNS Controller is running 10 seconds ahead of the other, the controller running behind has its time reset to match the one running 10 seconds ahead. If the second controller was running only 2 seconds ahead of the other, the time settings would remain unchanged. The values are 0, 5, and higher (values of 1-4 are automatically set to 5, and 0 turns off time syncing). The default setting is **10** seconds.

The time setting on 3-DNS Controllers is important because a 3-DNS Controller compares time stamps on files when deciding whether to synchronize files with other 3-DNS Controllers in the sync group.

Setting up communications between 3-DNS Controllers, data center servers, and big3d agents

There are three different communication issues that you need to resolve when you set up communication between the controllers running in your network:

- ◆ **3-DNS Controllers communicating with other 3-DNS Controllers**
To allow 3-DNS Controllers to communicate with each other, you must set up **ssh** and **scp** utilities for crypto controllers (that use SSH and SCP) that communicate with other crypto controllers, and you must set up **rsh** and **rcp** utilities for controllers that communicate with non-crypto controllers (that do not use SSH and SCP).
- ◆ **3-DNS Controllers communicating with BIG-IP Controllers, EDGE-FX Caches, and GLOBAL-SITE Controllers**
To allow 3-DNS Controllers to communicate with BIG-IP Controllers, EDGE-FX Caches, and GLOBAL-SITE Controllers, you address the same **ssh** and **rsh** issues. Crypto controllers communicating with other crypto controllers can use **ssh** and **scp** utilities, but controllers communicating with non-crypto controllers require **rsh** and **rcp** utilities.
- ◆ **3-DNS Controllers communicating with big3d agents**
To allow communications between **big3d** agents and the 3-DNS Controller, you need to configure iQuery ports on any 3-DNS Controllers, BIG-IP Controllers, EDGE-FX Caches, and GLOBAL-SITE Controllers that run the **big3d** agent.

◆ **Note**

Enabling RSH and RCP does not prevent crypto 3-DNS Controllers from using encryption when they communicate with other crypto 3-DNS Controllers, BIG-IP Controllers, EDGE-FX Caches, or GLOBAL-SITE Controllers.

Setting up communication between crypto and non-crypto controllers

The 3-DNS Controllers need to communicate with each other in order to synchronize configuration and performance data. If you use exclusively crypto 3-DNS Controllers (those that use the SSH protocol), or exclusively non-crypto 3-DNS Controllers (those that use the RSH protocol), the communication tools set up by the First-Time Boot utility are all you need.

If your network is a mixed environment, where some 3-DNS Controllers are crypto, and other 3-DNS Controllers are non-crypto, you need to enable the **rsh** and **rcp** utilities on the crypto 3-DNS Controllers. Though the **rsh** and **rcp** utilities come pre-installed on the crypto 3-DNS Controllers, you must explicitly enable these utilities. You can easily do this by running the **rsetup** script or the **config_rshd** script from the command line, or you can

enable the utilities when you run the First-Time Boot utility. Table 2.1 shows the ports and protocols that 3-DNS Controllers use to communicate with each other.

From	To	Protocol	From Port	To Port	Purpose
Crypto 3-DNS Controller	Crypto 3-DNS Controller	TCP	<1023	22	SSH/SCP
Crypto 3-DNS Controller	Non-crypto 3-DNS Controller	TCP	>1024	514	RSH/RCP
Non-crypto 3-DNS Controller	Crypto 3-DNS Controller	TCP	>1024	514	RSH/RCP
Non-crypto 3-DNS Controller	Non-crypto 3-DNS Controller	TCP	>1024	514	RSH/RCP

Table 2.1 Communications between 3-DNS Controllers

Setting up data collection with the big3d agent

The **big3d** agent collects performance information from other 3-DNS Controllers, BIG-IP Controllers, GLOBAL-SITE Controllers, and EDGE-FX Caches, on behalf of the 3-DNS Controller you are configuring. The 3-DNS Controller then uses this performance data for load balancing. The **big3d** agent uses factories to manage the data collection. For detailed information on configuring the **big3d** agent, managing the factories, opening the UDP ports, and working with firewalls, please review Chapter 3, *The big3d Agent*, in the *3-DNS Reference Guide*.

Planning issues for the load balancing configuration

The final phase of installing 3-DNS Controllers is setting up the load balancing configuration. Load balancing configurations are based on pools of virtual servers in a wide IP. When the 3-DNS Controller receives a connection request, it uses a load balancing mode to determine which virtual server in a given pool should receive the connection. The virtual servers in the pool can be the virtual servers managed by BIG-IP Controllers, virtual servers managed by EDGE-FX Caches, virtual servers managed by a generic host servers, or they can be individual host servers themselves. Note that the 3-DNS Controller continuously verifies which virtual servers in the pool are currently available to accept load balanced connections.

Simple configurations typically use a single pool of virtual servers and a load balancing mode, such as Round Robin or Hops, that does not require significant additional configuration steps. More advanced load balancing

configurations can use multiple wide IPs, multiple pools, customized load balancing modes, and other advanced traffic control features, such as topology load balancing and production rules.

We have included two popular 3-DNS Controller configurations in this Administrator Guide, in Chapter 3, *Configuring a Globally-Distributed Network*, and in Chapter 4, *Configuring a Content Delivery Network*. For additional details about advanced load balancing features, refer to Chapter 7, *Additional Load Balancing Options*.

Using advanced traffic control features

The 3-DNS Controller offers two advanced features that you can configure to further control the distribution and flow of network traffic.

◆ **Topology load balancing**

With Topology load balancing, you can direct client requests to virtual servers in the geographically closest data center. You can set up Topology load balancing between pools, or within a pool. For details about working with topology-based features, see Chapter 3, *Configuring a Globally-Distributed Network*, and Chapter 11, *Topology*, in the *3-DNS Reference Guide*.

◆ **Production rules**

Production rules are a policy-based management feature that you can use to dynamically change the load balancing configuration and the system settings based on specific triggers, such as the time of day, or the current network traffic flow. You can set up standard production rules using the Configuration utility, or you can define custom production rules using the production rules scripting language. Refer to Chapter 7, *Production Rules*, in the *3-DNS Reference Guide*, for information about setting up production rules.

Planning DNS zone file management

An important part of installing 3-DNS Controllers in your network is planning which server should be authoritative for a given DNS zone. When you initially set up a 3-DNS Controller in your network, you have two basic options for setting up DNS zone file management:

- You can use the 3-DNS Controller as the authoritative DNS server for your domain.
- You can use an existing authoritative DNS server for your domain, and make the 3-DNS Controller authoritative for your sub-domains (defined as wide IPs).

The 3-DNS Controller must always be authoritative for your wide IP sub-domains, regardless of which server is the authoritative DNS server for the network. However, we strongly recommend that you set up the 3-DNS Controller as authoritative for your domain.

One major benefit of setting up the 3-DNS Controller to be authoritative for your domain is that you can easily manage DNS zone files using NameSurfer, a browser-based, third-party application included on the 3-DNS Controller. With NameSurfer, you can also easily transfer your existing zone files to the 3-DNS Controller after the initial installation.

When you define wide IPs in the Configuration utility, the NameSurfer application automatically makes the appropriate additions to the zone files, and broadcasts the new zone files to the other DNS servers in your network. If you configure wide IPs from the command line, however, you need to make the corresponding zone file changes from the command line.

If you use the advanced synchronization features of the 3-DNS Controller, we strongly recommend that you configure each 3-DNS Controller to run as authoritative for the domain. This type of configuration offers the following advantages:

- You can change zone files on any one of the 3-DNS Controllers in the network and have those changes automatically broadcast to all of the other controllers in the network.
- Each 3-DNS Controller has the most up-to-date zone files, providing you one or more layers of redundancy.
- The NameSurfer application automatically controls the addition, configuration, and deletion of zone files.

Replacing your DNS servers with 3-DNS Controllers

Figure 2.1 shows an implementation where both 3-DNS Controllers in the network are authoritative for the domain, **domain.com**.

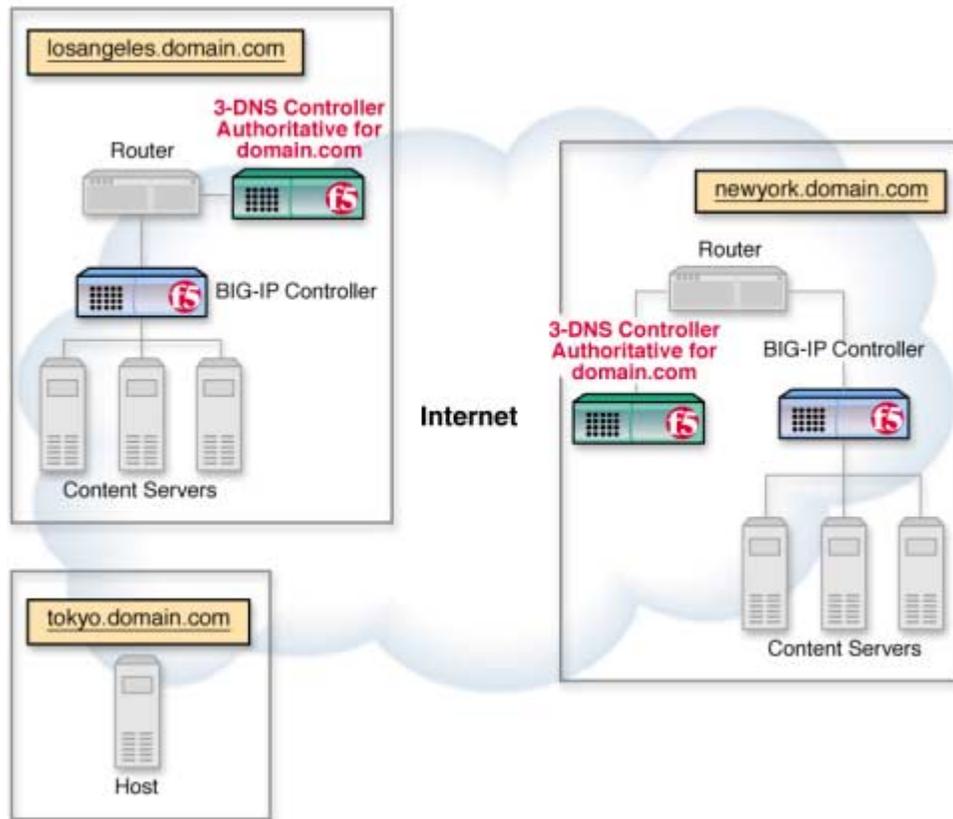


Figure 2.1 Using 3-DNS Controllers as authoritative DNS servers

Converting existing BIND files during an initial installation

After you initially install the 3-DNS Controller, you need to transfer existing BIND files, and then convert them to the NameSurfer format.

The first option for importing your existing BIND files is to transfer your zone files from your current name server to NameSurfer. After configuring NameSurfer during the First-Time Boot utility and connecting to the Configuration utility, use the **Copy from other name server** option in NameSurfer. For more information, refer to the NameSurfer documentation available from the splash screen in the Configuration utility.

The second option for converting your existing BIND files is to skip the NameSurfer configuration when you run the First-Time Boot utility. You transfer the zone files and **named.conf** file after the system has rebooted, and then run the **config_namesurfer** script that configures, converts, and starts the NameSurfer application.

◆ WARNING

*We recommend that you transfer your existing zone files using NameSurfer during the First-Time Boot utility. If you choose to transfer your existing zone files using the **config_namesurfer** script, please consult with your vendor first.*

Running 3-DNS Controllers as authoritative for sub-domains only

At a minimum, all 3-DNS Controllers must be authoritative for the zones associated with wide IP definitions. When you set up a configuration where the 3-DNS Controllers are authoritative for only those sub-domains, you need to make a few changes to the zone files on the DNS server that is authoritative for the domain after you configure the 3-DNS Controller.

Figure 2.2 shows an example where both 3-DNS Controllers are authoritative for the wide IP sub-domain, **wip.domain.com**, and a generic name server in the Tokyo data center is authoritative for the domain, **domain.com**.

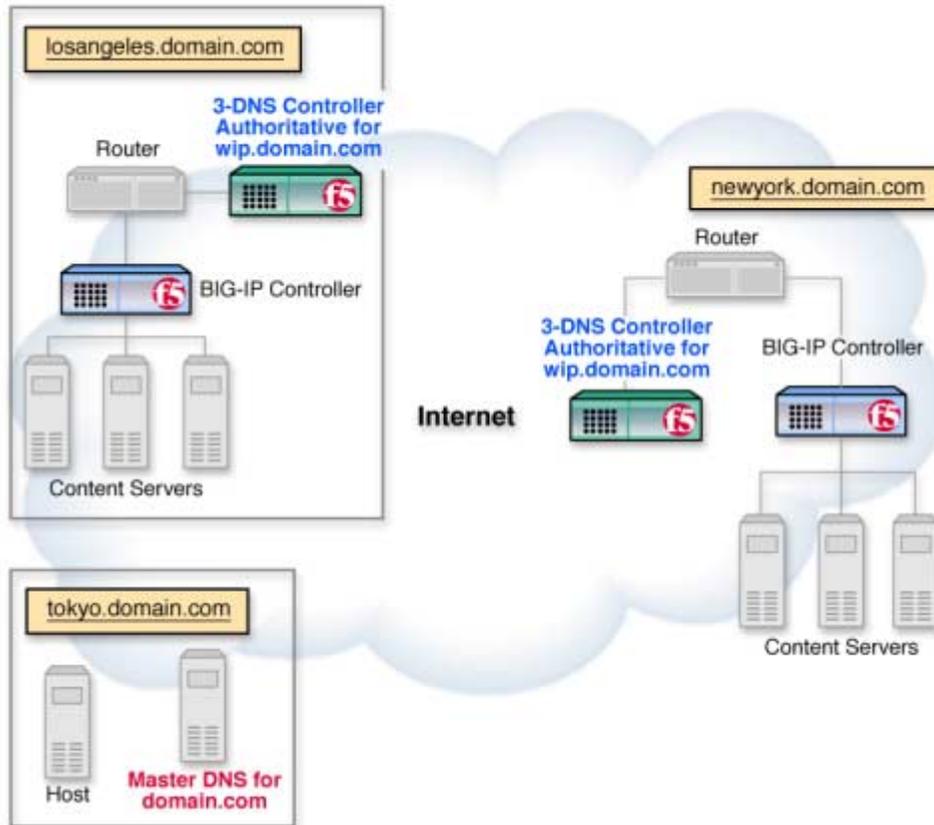


Figure 2.2 Using 3-DNS Controllers as authoritative DNS servers for sub-domains

Note that you should still set NameSurfer to be authoritative during the First-Time Boot utility for initial installations, or during the NameSurfer configuration script for upgrade installations. Remember that NameSurfer is authoritative for the zone files on the 3-DNS Controller, but in this configuration, the zone files contain only those records associated with wide IPs configured on the 3-DNS Controller. When you configure wide IPs in the Configuration utility, the NameSurfer application automatically updates the corresponding sub-domain zones and broadcasts them to the other DNS servers in the network. For configurations where synchronization is enabled, changes to any NameSurfer files are automatically updated to the other 3-DNS Controllers.

Setting up a basic configuration

The second phase of installing 3-DNS Controllers is to define the network setup. Each 3-DNS Controller in the network setup must have information regarding which data center houses specific servers, and with which other 3-DNS Controllers it can share configuration and load balancing information. A basic network setup includes data centers, servers, and one sync group. Once you have the basic network components configured on your 3-DNS Controller, you can set up the wide IPs you need for managing your load balancing. We recommend that you review the load balancing solutions in the remaining chapters of this guide before you configure the wide IPs.

The following sections describe the various elements of a basic network:

◆ **Data centers**

Data centers are the top level of your network setup. We recommend that you configure one data center for each physical location in your global network. The data center element of your configuration defines the servers (3-DNS Controllers, BIG-IP Controllers, EDGE-FX Caches, and hosts) that reside at that location.

A data center can contain any type of server. For example, in Figure 2.3, the Tokyo data center contains a 3-DNS Controller and a host, while the New York and Los Angeles data centers contain 3-DNS Controllers and BIG-IP Controllers.

For information about configuring data centers, see *Setting up a data center*, on page 2-12.

◆ **Servers**

The data center servers that you define in the network setup include 3-DNS Controllers, BIG-IP Controllers, GLOBAL-SITE Controllers, EDGE-FX Caches, and host machines. You define the 3-DNS Controllers that manage load balancing to the BIG-IP Controllers, EDGE-FX Caches, and hosts, and you also define the virtual servers that are managed by the servers. Virtual servers are the ultimate destination for connection requests.

For information about configuring servers, see *Setting up servers*, on page 2-15.

◆ **Sync groups**

Sync groups contain only 3-DNS Controllers. When setting up a sync group, you define which 3-DNS Controllers have the same configuration. In most cases, you should define all 3-DNS Controllers as part of the same sync group.

For information about configuring sync groups, see *Working with sync groups*, on page 2-29.

◆ **Wide IPs**

After you define virtual servers for your BIG-IP Controllers, EDGE-FX Caches, and hosts, you need to define wide IPs to specify how connections are distributed among the virtual servers. A wide IP maps a domain name to a pool of virtual servers, and it specifies the load balancing modes that the 3-DNS Controller uses to choose a virtual server from the pool.

When a local DNS server requests a connection to a specific domain name, the wide IP definition specifies which virtual servers are eligible to answer the request, and which load balancing modes to use in choosing a virtual server to resolve the request.

For information about configuring wide IPs and choosing load balancing modes, please refer to Chapter 5, *Load Balancing*, in the **3-DNS Reference Guide**.

◆ **Global variables**

You can configure global variables that apply to all servers and wide IPs in your network. However, the default values of the global variables work well for most situations, so configuring global variables is optional.

For information about configuring global variables, see *Configuring global variables*, on page 2-31.

Setting up a data center

The first step in configuring your 3-DNS Controller network is to create data centers. A **data center** defines the group of 3-DNS Controllers, BIG-IP Controllers, GLOBAL-SITE Controllers, EDGE-FX Caches, and hosts that reside in a single physical location. Figure 2.3 shows an example of a data center.

The advantage of grouping all machines from a single physical location into one data center in the configuration is to allow path information collected by one server to be shared with all other servers in the data center. The 3-DNS Controller uses the **big3d** agent to collect path and metrics information

about the other servers, and their virtual servers, in the data center. The 3-DNS Controller then applies path metrics results to all the virtual servers in the data center when making load balancing decisions.

◆ **Note**

You must configure at least one data center before you can add servers to the 3-DNS Controller configuration.

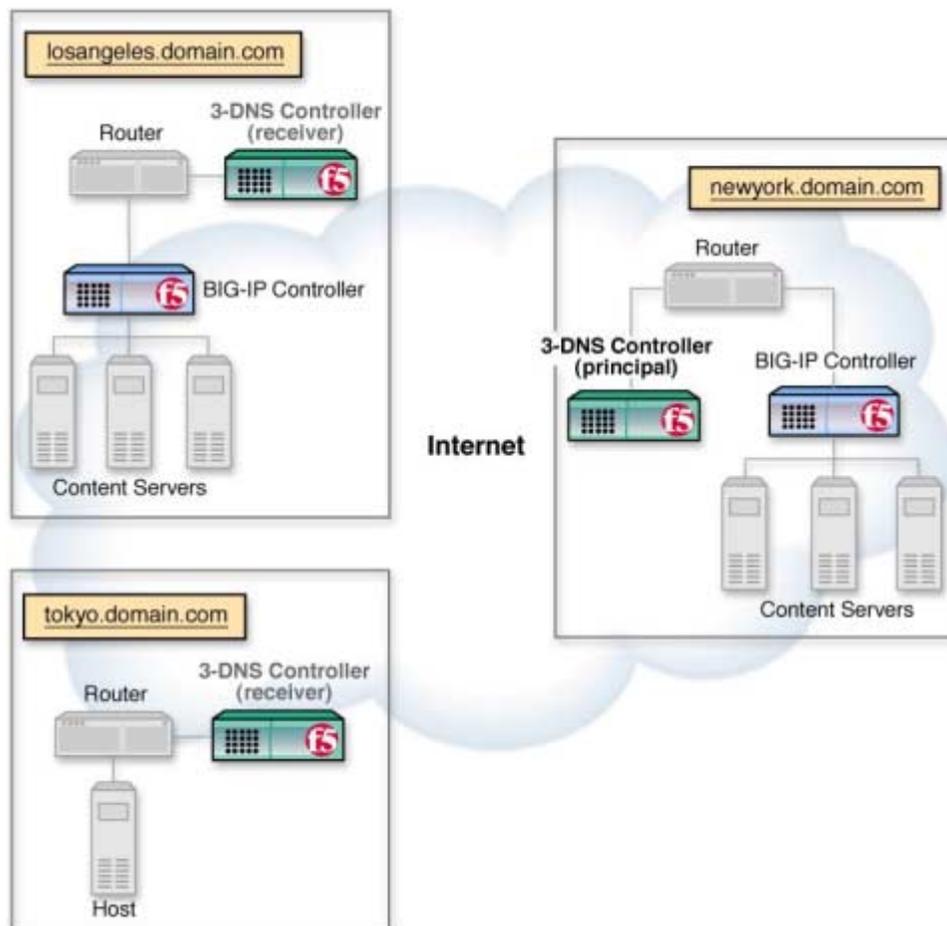


Figure 2.3 Example data center setup

When you add servers to the network setup, you assign the servers to the appropriate data centers.

To configure a data center using the Configuration utility

1. In the navigation pane, click **Data Centers**.
2. On the toolbar, click **Add Data Center**.
The Add New Data Center screen opens.
3. Add the new data center settings. For help on defining data centers, click **Help** on the toolbar.
The data center is added to your configuration.
4. Repeat this process for each data center in your network.

To configure a data center from the command line

1. At the command prompt, type **3dnsmaint** to open the 3-DNS Maintenance menu.
2. Select **Edit 3-DNS Configuration** to open the **wideip.conf** file.
The **EDITOR** environment variable determines whether this command starts **vi** or **pico**.
3. Locate or add the **datacenter** statement.

The **datacenter** statement should be the second statement in the file, after the **globals** statement and before **server** statements.
4. In the first line of the **datacenter** statement, type a name for the data center and enclose the name in quotation marks, as shown in Figure 2.4.
5. Type the server type and IP address for each server that is part of the specified data center.

Figure 2.4 shows the correct syntax for the **datacenter** statement.

```
datacenter {  
    name <"data center name">  
    [ location <"location info"> ]  
    [ contact <"contact info"> ]  
    [ 3dns <IP address> ]  
    [ bigip <IP address> ]  
    [ edge_fx <IP address> ]  
    [ gsite <IP address> ]  
    [ host <IP address> ]  
}
```

Figure 2.4 Syntax for the **datacenter** statement

Repeat the preceding procedure until you have added a separate **datacenter** statement for each data center in your network.

Figure 2.5 shows a sample **datacenter** statement.

```
datacenter {
  name "New York"
  location "NYC"
  contact "3DNS_Admin"
  3dns 192.168.101.2
  bigip 192.168.101.40
  host 192.168.105.40
}
```

Figure 2.5 Sample data center definition

Setting up servers

There are five types of servers: 3-DNS Controllers, BIG-IP Controllers, GLOBAL-SITE Controllers, EDGE-FX Caches, and hosts. At the minimum, your network includes one 3-DNS Controller, and at least one server (BIG-IP Controller, EDGE-FX Cache, GLOBAL-SITE Controller, or host) that it manages.

This section describes how to set up each 3-DNS Controller, BIG-IP Controller, EDGE-FX Cache, GLOBAL-SITE Controller, and host machine that make up your network. The setup procedures here assume that the BIG-IP Controllers, EDGE-FX Caches, GLOBAL-SITE Controllers, and hosts are up and running, and that they already have virtual servers defined. Note that 3-DNS Controllers and GLOBAL-SITE Controllers do not manage virtual servers.

Defining 3-DNS Controller servers

The purpose of defining a 3-DNS Controller server is to establish in which data center the 3-DNS Controller resides and, if necessary, to change **big3d** agent settings. Before you add other 3-DNS Controllers to the configuration, you should add the 3-DNS Controller you are configuring to its own configuration. By adding any additional 3-DNS Controllers to the configuration, you make those 3-DNS Controllers available so that you can add them to a sync group.

◆ Note

*Please review Chapter 5, **Adding 3-DNS Controllers to the Network**, if you are configuring more than one 3-DNS Controller in your network.*

To define a 3-DNS Controller server using the Configuration utility

1. In the navigation pane, expand the **Servers** item, then click **3-DNS Controllers**.
2. On the toolbar, click **Add 3-DNS Controller**.
The Add New 3-DNS Controller screen opens.
3. Add the new 3-DNS Controller settings. For help on defining 3-DNS Controllers, click **Help** on the toolbar.

The 3-DNS Controller is added to your configuration. Repeat this procedure for each 3-DNS Controller you need to add.

To define a 3-DNS Controller server from the command line

1. At the command prompt, type **3dnsmaint** to open the 3-DNS Maintenance menu.
2. On the 3-DNS Maintenance menu, select **Edit 3-DNS Configuration** to open the **wideip.conf** file.
3. Use the syntax shown in Figure 2.6 to define a 3-DNS Controller.

All **server** statements should appear after the **sync_group** statement and before **wideip** statements.

```
server {
  type 3dns
  address <IP address>
  name <"3dns_name">
  iquery_protocol [ udp | tcp ]
  [ remote {
    secure <yes | no>
    user <"user name">
  } ]
  [ interface {
    address <NIC IP address>
    address <NIC IP address>
  } ]
  [ factories {
    prober <number>
    discovery <number>
    snmp <number>
    hops <number>
  } ]
}
```

Figure 2.6 Syntax for defining a 3-DNS Controller server

Figure 2.7 shows a sample **server** statement that defines a 3-DNS Controller.

```
// New York
server {
    type 3dns
    address 192.168.101.2
    name "3dns-newyork"
    iquery_protocol udp
    remote {
        secure yes
        user "root"
    }
}
```

Figure 2.7 Sample 3-DNS Controller server definition

Defining BIG-IP Controller servers

Before you define BIG-IP Controller servers, you should have the following information:

- The IP address and service name or port number of each virtual server to be managed by the BIG-IP Controller
- The IP address of the server itself

To define a **BIG-IP Controller server** using the **Configuration utility**

1. In the navigation pane, expand the **Servers** item, and then click **BIG-IP Controllers**.
2. On the toolbar, click **Add BIG-IP Controller**.
The Add New BIG-IP Controller screen opens.
3. Add the new BIG-IP Controller settings. (For help on defining BIG-IP Controllers, click **Help** on the toolbar.)
The BIG-IP Controller and specified virtual server are added to your configuration.

To add more virtual servers using the **Configuration utility**

1. In the navigation pane, expand the **Servers** item, and then click **BIG-IP Controllers**.
2. In the table, find the BIG-IP Controller that you just added.
3. Click the entry in its **BIG-IP Virtual Servers** column.

4. On the toolbar, click **Add Virtual Server**.
The Add Virtual Server to BIG-IP screen opens.
5. Add the new virtual server settings. For help on adding virtual servers, click **Help** on the toolbar.

Repeat this process for each virtual server you want to add to this BIG-IP Controller.

To define a BIG-IP Controller server from the command line

1. At the command prompt, type **3dnsmaint** to open the 3-DNS Maintenance menu.
2. On the 3-DNS Maintenance menu, select **Edit 3-DNS Configuration** to open the **wideip.conf** file.
3. Use the syntax shown in Figure 2.8 to define a BIG-IP Controller.

All **server** statements should appear after the **sync_group** statement and before **wideip** statements.

If you need to allow iQuery packets to pass through firewalls, include the **translate** keyword in the **server** statement that defines the BIG-IP Controller. When you include the **translate** keyword, the iQuery utility includes translated IP addresses in the packets sent to the specific BIG-IP Controller. For more information on configuring the **big3d** agent and iQuery, see Chapter 3, *The big3d Agent*, of the *3-DNS Reference Guide*.

```
server {
  type bigip
  address <IP address>
  name <"bigip_name">
  iquery_protocol [ udp | tcp ]
  [ limit {
    [ kbytes_per_second <number>
      packets_per_second <number>
      disk_avail <number>
      cpu_usage <number>
      memory_avail <number>
      current_connections <number> ]
    } ]
  [ remote {
    secure <yes | no>
    user <"user name">
    } ]
  [ interface {
    address <NIC IP address>
    address <NIC IP address>
    } ]
  [ factories {
    prober <number>
    discovery <number>
    snmp <number>
    hops <number>
    } ]

  vs {
    address <virtual server IP address>
    port <port number> | service <"service name">
    [ depends_on {
      address <IP address>
      address <IP address>
    } ]
    [ translate {
      address <IP address>
      port <port number> | service <"service name">
    } ]
  }
}
```

Figure 2.8 Syntax for defining a BIG-IP Controller server

Figure 2.9 shows a sample **server** statement that defines a BIG-IP Controller.

```
server {
    type          bigip
    address       192.168.101.40
    name          "bigip-newyork"
    iquery_protocol udp
    remote {
        secure    yes
        user      "administrator"
    }
    # Tell 3-DNS about the 2 interfaces on a BIG-IP HA
    interface {
        address   192.168.101.41
        address   192.168.101.42
    }
    # Change the number of factories doing the work at big3d
    factories {
        prober    6
        discovery 1
        snmp      1
        hops      2
    }
    vs {
        address   192.168.101.50
        service   "http"
        translate {
            address 10.0.0.50
            port    80
        }
    }
    vs {
        address   192.168.101.50:25 // smtp
        translate {
            address 10.0.0.50:25
        }
    }
}
```

Figure 2.9 Sample BIG-IP Controller server definition

Defining GLOBAL-SITE Controllers

Before you define GLOBAL-SITE Controller servers, you should have the following information:

- The name of the controller
- The IP address of the controller

To define an GLOBAL-SITE Controller server using the Configuration utility

1. In the navigation pane, expand the **Servers** item, then click **GLOBAL-SITE Controllers**.
2. On the toolbar, click **Add GLOBAL-SITE Controller**.
The Add New GLOBAL-SITE Controller screen opens.
3. Add the new GLOBAL-SITE Controller settings. For help on defining a GLOBAL-SITE Controller, click **Help** on the toolbar.
The GLOBAL-SITE Controller is added to your configuration.

To define a GLOBAL-SITE Controller server from the command line

1. At the command prompt, type **3dnsmaint** to open the 3-DNS Maintenance menu.
2. On the 3-DNS Maintenance menu, select **Edit 3-DNS Configuration** to open the **wideip.conf** file.
3. Use the syntax shown in Figure 2.10 to define a GLOBAL-SITE Controller.

```
server {
  type gsite
  address <IP address>
  name <"gsite_name">
  iquery_protocol [ udp | tcp ]
  [ remote {
    secure <yes | no>
    user <"user name">
  }]
  [ factories {
    prober <number>
    discovery <number>
    snmp <number>
    hops <number>
  }]
}
```

Figure 2.10 Syntax for defining a GLOBAL-SITE Controller server

In the **wideip.conf** file, all **server** statements should appear after the **sync_group** statement and before **wideip** statements.

Figure 2.11 shows a sample **server** statement that defines a GLOBAL-SITE Controller.

```
server { // datacenter=East Coast
  type gsite
  address 192.168.10.150
  name "gsite_east1"
  iquery_protocol udp
  remote { secure yes
    user "root" }
  factories {
    hops 1 }
}
```

Figure 2.11 Sample GLOBAL-SITE Controller server definition

Defining EDGE-FX Caches

Before you define EDGE-FX Cache servers, you should have the following information:

- The IP address and service name or port number of each virtual server to be managed by the EDGE-FX Cache
- The IP address of the cache itself

To define an EDGE-FX Cache server using the Configuration utility

1. In the navigation pane, expand the **Servers** item, then click **EDGE-FX Caches**.
2. On the toolbar, click **Add EDGE-FX Cache**.
The Add New EDGE-FX Cache screen opens.
3. Add the new EDGE-FX Cache settings. For help on defining an EDGE-FX Cache, click **Help** on the toolbar.
The EDGE-FX Cache and specified virtual server are added to your configuration.

To add more virtual servers using the Configuration utility

1. In the navigation pane, click **Servers**, then click **EDGE-FX Caches**.
2. In the table, find the EDGE-FX Cache that you just added.
3. Click the entry in its **EDGE-FX Virtual Servers** column.
4. On the toolbar, click **Add Virtual Server**.
The Add Virtual Server to EDGE-FX screen opens.

5. Add the new virtual server settings. For help on adding virtual servers, click **Help** on the toolbar.

Repeat this process for each virtual server you want to add to this EDGE-FX Cache.

To define an EDGE-FX Cache server from the command line

1. At the command prompt, type **3dnsmaint** to open the 3-DNS Maintenance menu.
2. On the 3-DNS Maintenance menu, select **Edit 3-DNS Configuration** to open the **wideip.conf** file.
3. Use the syntax shown in Figure 2.12 to define an EDGE-FX Cache.

```
server {
    type edge_fx
    address <IP address>
    name <"edge_name">
    iquery_protocol [ udp | tcp ]
    [ limit {
        [ kbytes_per_sec <number>
          pkts_per_sec   <number>
          current_conns  <number>
          cpu_usage      <number>
          mem_avail      <number>
          disk_avail     <number> ]
        } ]
    [ remote {
        secure <yes | no>
        user <"user name">
    } ]
    [ factories {
        prober <number>
        discovery <number>
        snmp <number> //minimum of 1 to collect metrics
        hops <number>
    } ]
    vs {
        address <virtual server IP address>
        port <port number> | service <"service name">
    [ depends_on {
        address <IP address>
        address <IP address>
    } ]
    }
}
```

Figure 2.12 Syntax for defining an EDGE-FX Cache server

In the **wideip.conf** file, all **server** statements should appear after the **sync_group** statement and before **wideip** statements.

If you need to allow iQuery packets to pass through firewalls, include the **translate** keyword in the **server** statement that defines the EDGE-FX Cache. When you include the **translate** keyword, the iQuery utility includes translated IP addresses in the packets sent to the specific EDGE-FX Cache. For more information on configuring the **big3d** agent and iQuery, see Chapter 3, *The big3d Agent*, of the *3-DNS Reference Guide*.

Figure 2.13 shows a sample **server** statement that defines an EDGE-FX Cache.

```
server { // datacenter=East Coast, #VS=1
  type edge_fx
  address 192.168.10.150
  name "edge_east1"
  limit { /* none */ }
  iquery_protocol udp
  remote { secure yes
           user "root"
         }
  factories {
    snmp 1
  }
  vs {
    address 10.10.10.10:80 // http
    limit { /* none */ }
    probe_protocol tcp
  }
}
```

Figure 2.13 Sample EDGE-FX Cache server definition

Defining host servers

A **host** is an individual network server or server array controller other than the BIG-IP Controller, EDGE-FX Cache, or GLOBAL-SITE Controller. Before configuring a host, you should have the following information:

- ◆ **Address information**

The IP address and service name or port number of each virtual server to be managed by the host.

- ◆ **SNMP information for host probing**

To implement host probing and to collect performance metrics, you must specify SNMP agent settings after you define the host server. The settings you specify include the type and version of SNMP agent that runs on the host, the community string, and the number of

communication attempts that you want the **big3d** agent to make while gathering host metrics. SNMP agent settings for hosts are described in *Configuring host SNMP settings*, on page 2-27.

◆ **Note**

*To fully configure host probing, you must configure the SNMP agent settings in the host definition as previously described, and you must also set up the **big3d** agents to run SNMP factories, and configure the SNMP agents on the hosts themselves. For details, please refer to Chapter 3, **The big3d Agent**, and Chapter 10, **SNMP**, in the **3-DNS Reference Guide**.*

To define a host server using the Configuration utility

1. In the navigation pane, expand the **Servers** item, and then click **Host Servers**.
2. On the toolbar, click **Add Host Server**.
The Add New Host Server screen opens
3. Add the new host server settings. For help on adding host servers, click **Help** on the toolbar.
The host and the specified virtual server are added to your configuration.

To add more virtual servers using the Configuration utility

1. In the navigation pane, click **Host Servers**.
2. In the table, find the host that you just added, and click the entry in its **Host Virtual Servers** column.
3. On the toolbar, click **Add Host Virtual Server**.
The Add Virtual Server to Host screen opens.
4. Add the new virtual server settings. For help on adding virtual servers, click **Help** on the toolbar.

Repeat this process for each virtual server you want to add to this host.

To define a host server from the command line

1. At the command prompt, type **3dnsmaint** to open the 3-DNS Maintenance menu.
2. On the 3-DNS Maintenance menu, select **Edit 3-DNS Configuration** to open the **wideip.conf** file.
3. Use the syntax shown in Figure 2.14 to define a host.

All **server** statements should appear after the **sync_group** statement and before **wideip** statements.

```
server {
    type host
    address <IP address>
    name <"host_name">
    [ prober <ip_address> ]
    probe_protocol <tcp | icmp | udp | dns_rev | dns_dot>
    port <port number> | service <"service name">
    [ snmp {
        agent <generic | ucd | solstice | ntserv | ciscoldv2 | ciscoldv3 | arrowpoint |
foundry | alteon | cacheflow | win2kserv>
        port <port number>
        community <"community string">
        timeout <seconds>
        retries <number>
        version <SNMP version>
    } ]
    vs {
        address <virtual server IP address>
        port <port number> | service <"service name">
    [ depends_on {
        address <IP address>
        address <IP address>
    } ]
    [ probe_protocol <tcp | icmp | dns_rev | dns_dot> ]
    }
}
```

Figure 2.14 Syntax for defining a host server

Figure 2.15 shows a sample **server** statement that defines a host.

```
server {
    type          host
    address       192.168.104.40
    name          "host-tokyo"
    prober        192.168.101.40
    probe_protocol icmp
    port          53
    snmp {
        agent      ucd
        community  "public"
        version    1
    }
    vs {
        address    192.168.104.50:25
    }
    vs {
        address    192.168.104.50:80
    }
}
```

Figure 2.15 Sample host server definition

Configuring host SNMP settings

After defining a host server, you need to configure its SNMP settings if you want to use SNMP host probing. Remember that you must first set up at least one SNMP probing factory on any 3-DNS Controller or BIG-IP Controller that runs the **big3d** agent.

The SNMP prober collects some or all of the following information from hosts.

- Memory utilization
- CPU utilization
- Disk space utilization
- Packet rate (packets per second)
- Throughput rate (kilobytes per second)
- Current connections

The 3-DNS Controller uses this performance information for advanced load balancing modes such as Packet Rate, Quality of Service, and Kilobytes/Second.

The 3-DNS Controller supports the following host SNMP agents:

SNMP Agent	Description
Generic	A generic SNMP agent is an SNMP agent that collects metrics provided by object identifiers (OIDs) as specified in the RFC 1213 document.
UCD	This free SNMP agent is provided by the University of California at Davis. It is available on the web at http://net-snmp.sourceforge.net
Solstice	This SNMP agent is a product of Sun Microsystems.
NTServ	This SNMP matrix agent is a product of Microsoft Corporation and is distributed with Microsoft Windows NT Server 4.0.
Win2KServ	This SNMP matrix agent is a product of Microsoft Corporation and is distributed with Microsoft Windows 2000 Server.
Cisco LDV2	This SNMP agent is a product of Cisco Systems and is distributed with the Cisco LocalDirector, version 2.X.
Cisco LDV3	This SNMP agent is a product of Cisco Systems and is distributed with the Cisco LocalDirector, version 3.X.
ArrowPoint	This SNMP agent is a product of Cisco Systems and is distributed with the Cisco/ArrowPoint CSS series.

Table 2.2 Supported SNMP agents

SNMP Agent	Description
Alteon	This SNMP agent is a product of Alteon WebSystems and is distributed with the ACEdirector.
Foundry	This SNMP agent is a product of Foundry Networks and is distributed with the Foundry ServerIron.
CacheFlow	This SNMP agent is a product of CacheFlow and is distributed with the CacheFlow appliances.

Table 2.2 Supported SNMP agents

Viewing host performance metrics

The Configuration utility displays the host metrics in the Host Statistics screen. The 3-DNS Controller bases the advanced load balancing decisions on packet rate, kilobytes per second, and current connections metrics, but the Host screen displays the other metrics as well, for information purposes.

Reviewing SNMP configuration issues

The SNMP probing feature requires that each host run an SNMP agent, and that the hosts and the **big3d** agents in the data centers have open network communication. Certain firewall configurations block SNMP communications, and you may need to verify that the firewalls in your network allow SNMP traffic to pass through. For information on configuring the **big3d** agent and working with firewalls, see Chapter 3, *The big3d Agent*, in the *3-DNS Reference Guide*.

In addition to properly configuring the SNMP agents on the hosts themselves, you need to specify SNMP host probing settings in two places in the 3-DNS Controller configuration. First, when you define a BIG-IP Controller or 3-DNS Controller server, you set the **big3d** agent to run at least one SNMP factory. Second, when you define the host servers, you configure specific SNMP agent settings for each host. For example, you need to specify the type of agent running on the host as well as the community string that allows access to the SNMP agent. For more information on configuring SNMP agents, please review Chapter 10, *SNMP*, in the *3-DNS Reference Guide*.

The SNMP chapter also includes some useful tips on configuring the different SNMP agents on the hosts themselves. We recommend that you use the information in conjunction with the documentation originally provided with the SNMP agent.

Working with sync groups

A *sync group* defines a group of 3-DNS Controllers that synchronize their configuration settings and metrics data. A sync group contains a principal controller and one or more receiver controllers. The *principal* controller is the 3-DNS Controller from which the *receiver* controllers obtain their metrics and server statistics information. You configure a sync group from the principal 3-DNS Controller. First list the IP address of the principal itself. Then list the receiver 3-DNS Controllers in the order that they should become principals if previously listed 3-DNS Controllers fail.

Each 3-DNS Controller in your network must be included in a sync group. There may be cases where you do not want a 3-DNS Controller to share its configuration with other controllers. In this case, you can create a separate sync group for each 3-DNS Controller. Each sync group contains only its own name or IP address.

```
sync_group {
  name "sync-ny"
  3dns 192.168.101.2    // New York
}

sync_group {
  name "sync-la"
  3dns 192.168.102.2    // Los Angeles
}
```

Figure 2.16 Sample non-syncing *sync groups* statements

◆ Note

To implement such a configuration, you must modify each 3-DNS Controller's *wideip.conf* file; the Configuration utility does not support this function.

Configuring sync groups

The following procedures describe how to configure sync groups.

To define a sync group using the Configuration utility

1. In the navigation pane, click **3-DNS Sync**.
The System - Add a New Sync Group screen opens.
2. In the **New Sync Group Name** box, type the name of the new sync group and click **Add**.
The Add a 3-DNS to a Sync Group screen opens.

3. From the list of 3-DNS Controllers, first select the 3-DNS Controller that you want to be the principal controller. Then check the box next to each 3-DNS Controller that you want to add to the sync group.
4. Click **Add**.

To define a sync group from the command line

1. At the command prompt, type **3dnsmaint** to open the 3-DNS Maintenance menu.
2. On the 3-DNS Maintenance menu, select **Edit 3-DNS Configuration** to open the **wideip.conf** file.
3. Use the syntax shown in Figure 2.17 to define sync groups.

The **sync_group** statement should appear after the **datacenter** statement and before **server** statements.

```
sync_group {
    name "<name>"
    3dns <ip_address | "domain_name">
    [ 3dns <ip_address | "domain_name"> ] ...
}
```

Figure 2.17 Syntax for setting up a sync group

Figure 2.18 shows a sample **sync_group** statement.

```
sync_group {
    name "default"
    3dns 192.168.101.2    // New York
    3dns 192.168.102.2    // Los Angeles
}
```

Figure 2.18 Sample sync group definition

Setting the time tolerance value

The time tolerance value is a global variable that defines the number of seconds that one 3-DNS Controller's time setting is allowed to be out of sync with another 3-DNS Controller's time setting. We recommend that you leave the time tolerance variable at the default setting of **10**.

To check the value for the time tolerance setting using the Configuration utility

1. In the navigation pane, click **System**.
The System - General screen opens.
2. On the toolbar, click **Timers and Task Intervals**.
3. Note the value in the **3-DNS Sync Time Tolerance** box, and change it if necessary.
4. If you change this setting, click **Update** to save it. For more information about the settings on this screen, click **Help** on the toolbar.

To check the value for the time tolerance setting in the configuration file

1. At the command prompt, type **3dnsmaint** to open the 3-DNS Maintenance menu.
2. On the 3-DNS Maintenance menu, select **Edit 3-DNS Configuration** to open the **wideip.conf** file.
3. Search for **time_tolerance**. If the **time_tolerance** sub-statement is not in the configuration file, the default (**10**) is used.

Configuring global variables

The default values for global parameters are sufficient for most load balancing situations. However, we recommend that you specifically enable encryption for crypto 3-DNS Controllers.

To configure global parameters using the Configuration utility

1. In the navigation pane, click **System**.
The System - General screen opens. Note that global parameters are grouped into several categories on this screen. Each category has its own toolbar item, and online help is available for each parameter.
2. Make general global changes at the System - General screen or, to make changes to global parameters in other categories, click the appropriate toolbar item.
3. Add the new global settings. For help on configuring the global settings, click **Help** on the toolbar.

The new global parameters are added to your configuration.

To configure global parameters from the command line

1. At the command prompt, type **3dnsmaint** to open the 3-DNS Maintenance menu.
2. On the 3-DNS Maintenance menu, select **Edit 3-DNS Configuration** to open the **wideip.conf** file.
3. Locate or add the **globals** statement. The **globals** statement should be at the top of the file.
4. Under the **globals** statement, type the appropriate sub-statement and value.

For example, to enable encryption for iQuery transactions (which is recommended), change the encryption parameter to **yes** (the default setting is **no**). If you want to use a non-default name for the encryption key file, type it on the next line.

Figure 2.19 shows the correct syntax for enabling encryption.

```
globals {  
    encryption yes  
    encryption_key_file "/etc/F5key.dat"  
}
```

Figure 2.19 Syntax for enabling encryption



3

Configuring a Globally-Distributed Network

- Understanding a globally-distributed network
- Using Topology load balancing
- Setting up a globally-distributed network configuration
- Additional configuration settings and tools

Understanding a globally-distributed network

When you are familiar with your traffic patterns and are expanding into a global marketplace, you can use the 3-DNS Controller to distribute requests in an efficient and seamless manner using Topology load balancing. When you use Topology load balancing, the 3-DNS Controller compares the location information derived from the DNS query message to the topology records in the topology statement. The controller then distributes the request according to the topology record that best matches the location information.

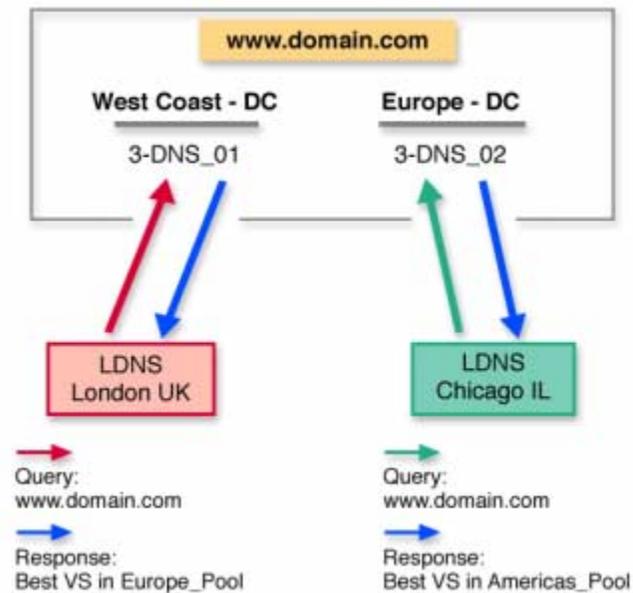


Figure 3.1 Topology load balancing in a globally-distributed network

Using Topology load balancing

The Topology load balancing mode is optimal for organizations that have data centers in more than one country or on more than one continent. The crypto 3-DNS Controller enables topology-based load balancing by resolving DNS requests to the geographically closest server. The traditional topology load balancing mode, that provides basic topology mapping

functionality, uses IP subnets of virtual servers and known LDNS servers. This can result in a very large list of IP subnets to manage when you want to map a specific geographic region.

To simplify topology load balancing, the 3-DNS Controller contains a classifier that maps IP addresses to geographic locations. With this classifier, the 3-DNS Controller resolves DNS requests to the geographically closest LDNS server at either the country or the continent level. The controller then load balances the request to virtual servers in IP subnets, wide IP pools, or data centers.

You can set up Topology load balancing either between wide IP pools or within a wide IP pool. For the example in Figure 3.1, we configure Topology load balancing between wide IP pools.

Setting up a globally-distributed network configuration

By going through the following setup tasks, you can configure the 3-DNS Controller to process requests, using Topology, in a globally-distributed network. This configuration is based on the following assumptions:

- You have more than one data center.
- You have a 3-DNS Controller in each data center.
- You have BIG-IP Controllers, or other load balancing hosts, in the data centers.
- You want to load balance requests to the geographically closest virtual server.

If you use a CDN for some or all of your content delivery, please refer to Chapter 4, *Configuring a Content Delivery Network*, to set up this configuration.

The following sections describe, in order, the specific configuration tasks you perform to set up a globally-distributed network. Please review the tasks before you actually perform them, so that you are familiar with the process.

Adding data centers to the globally-distributed network configuration

The first task you perform is to add your data centers to the 3-DNS Controller configuration.

To add data centers using the Configuration utility

1. In the navigation pane, click **Data Centers**.
The Data Centers screen opens.

2. Click **Add Data Center** on the toolbar.
The Add Data Centers screen opens.
3. Add your data center information. For information and help on the specific settings on this screen, click **Help** on the toolbar.
4. Repeat the previous steps to add all of your data centers to the configuration.

Configuration notes

*For the globally-distributed network configuration shown in Figure 3.1, on page 3-1, we have added two data centers labeled **West Coast - DC** and **Europe - DC**.*

Adding 3-DNS Controllers to the globally-distributed network configuration

Once you have added all of your data centers to the 3-DNS Controller configuration, you are ready to let the controller that you are configuring know about the 3-DNS Controllers in your network, including the controller you are configuring.

◆ Note

*Please note that when you are working with more than one 3-DNS Controller, you create your entire configuration on one controller and then add the second controller using the **3dns_add** script. The **3dns_add** script copies the entire configuration from the first (or existing) controller onto the second (new) controller, and synchronizes all of the settings. For details on configuring additional 3-DNS Controllers in existing networks, using the **3dns_add** script, see Chapter 5, **Adding 3-DNS Controllers to the Network**.*

To add 3-DNS Controllers using the Configuration utility

1. In the navigation pane, expand the **Servers** item, then click **3-DNS Controllers**.
The 3-DNS Controllers screen opens.
2. Click **Add 3-DNS Controller** on the toolbar.
The Add New 3-DNS Controller screen opens.

For information and help on the specific settings on any screen in the Configuration utility, click **Help** on the toolbar.
3. Add the 3-DNS Controller information.
4. Repeat the previous steps to add any additional 3-DNS Controllers to the configuration.

Configuration notes

*For the globally-distributed network configuration shown in Figure 3.1, on page 3-1, we have a 3-DNS Controller in each data center, **West Coast - DC** and **Europe - DC**. The controller we are configuring is labeled **3-DNS_01**, and is in the **West Coast - DC** data center. The additional controller is in the **Europe - DC** data center, and is labeled **3-DNS_02**.*

Adding BIG-IP Controllers to the globally-distributed network configuration

Now you are ready to let the controller know about any BIG-IP Controllers, or other servers, that you have in your network. Remember that the 3-DNS Controller load balances requests to the virtual servers managed by the BIG IP Controllers, EDGE-FX Caches, or host servers in your network. In this example configuration, we set up BIG-IP Controllers. For information on adding EDGE-FX Caches or host servers to your network, please refer to *Setting up servers*, on page 2-15.

The following steps outline how to add BIG-IP Controllers to your configuration.

To add BIG-IP Controllers using the Configuration utility

1. In the navigation pane, expand the **Servers** item, then click **BIG-IP Controllers**.
The BIG-IP Controllers screen opens.
2. Click **Add BIG-IP Controller** on the toolbar.
The Add New BIG-IP Controller screen opens.
3. Add the BIG-IP Controller information and click **Next**. For information and help on the specific settings on this screen, click **Help** on the toolbar.
4. In the Data Centers screen, select the Data Center where the BIG-IP Controller is located and click **Next**.
5. In the Configure Virtual Server screen, add the information for the first virtual server managed by the BIG-IP Controller and click **Finish**.
6. To add more virtual servers to your configuration, click **Add Virtual Server** on the toolbar.

7. Once you have configured your first BIG-IP Controller, you can repeat the previous steps to add all of the additional BIG-IP Controllers to the 3-DNS Controller configuration.

◆ **Tip**

*For information and help on the specific settings on any screen in the Configuration utility, click **Help** on the toolbar.*

Adding wide IPs to the globally-distributed network configuration

Once you have added all the physical elements to your 3-DNS Controller configuration, you can begin configuring wide IPs and pools for load balancing. Before you start adding wide IPs, verify that you have configured all the virtual servers you need for load balancing. In order to optimize the Topology load balancing mode, you need to properly configure the wide IPs and pools, as follows.

To add a wide IP and pool using the Configuration utility

1. In the navigation pane, click **Wide IPs**.
The Wide IP List screen opens.
2. Click **Add Wide IP** on the toolbar.
The Add a New Wide IP screen opens.
3. Add the wide IP address, name, and port information.
4. For the **Pool LB Mode**, select **Topology** and click **Next**.
The Configure Load Balancing for New Pool screen opens.
5. Add the pool name and click **Next**.
The Select Virtual Servers screen opens.
6. In the Select Virtual Servers screen, check the virtual servers among which you want the 3-DNS Controller to load balance DNS requests, and click **Finish**.
The 3-DNS Controller adds the wide IP and settings to the configuration.
7. If you want to create additional pools for load balancing, click the name of the wide IP you just created in the Wide IPs List screen. When the Modify Wide IP screen opens, click **Add Pool** on the toolbar.

8. Repeat the previous procedures to add as many wide IPs and pools as are required for your network.

◆ **Tip**

*For information and help on the specific settings on any screen in the Configuration utility, click **Help** on the toolbar.*

Configuration notes

*For the globally-distributed network configuration shown in Figure 3.1, on page 3-1, we have set up one wide IP, labeled **www.domain.com**, and we added two pools to the wide IP, **americas_pool** and **europa_pool**. When you configure the topology records, as explained in the next section, we designate these two pools to process the load balancing requests based on the geographic location of the local DNS server or client making the request.*

Configuring topology records for the globally-distributed network configuration

You must configure the topology records before the 3-DNS Controller can use the Topology load balancing mode. The Topology load balancing mode distributes connections after evaluating and scoring the topology records in the topology statement. If you have no topology records in the topology statement, or if the scores returned for two or more records are equal, the 3-DNS Controller load balances the virtual servers using the Random load balancing mode.

The following procedure explains how to configure topology records in the Configuration utility. For more information on how the 3-DNS Controller uses the topology records, and how to configure topology in the **wideip.conf** file, please review Chapter 11, *Topology*, in the **3-DNS Reference Guide**.

To configure topology records using the Configuration utility

1. In the navigation pane, click **Topology**.
The Manage Topology Records screen opens.
2. Add the settings for the topology records.
3. Click **Add**.

◆ **Tip**

*For information and help on the specific settings on any screen in the Configuration utility, click **Help** on the toolbar.*

For the globally-distributed network configuration shown in Figure 3.1, on page 3-1, we added topology records, as shown in Figure 3.2:

//server	ldns	score
pool.americas_pool	cont.North America	100
pool.europe_pool	!cont.North America	100

Figure 3.2 Example of a topology statement

Configuration notes

*With this topology statement, in our example configuration, queries to resolve **www.domain.com** from local DNS servers somewhere in North America get responses from virtual servers in the pool **americas_pool**. All other queries to resolve **www.domain.com** get responses from virtual servers in the pool **europe_pool**.*

Additional configuration settings and tools

The following optional settings and tools can help you refine your load balancing configuration.

Setting limits thresholds

When you set limits thresholds for availability, the 3-DNS Controller can detect when a managed server or virtual server is low on system resources and redirect the traffic to another virtual server. Setting limits helps eliminate any negative impact on a virtual server's performance of service tasks that may be time critical, require high bandwidth, or put high demand on system resources. The system resources for which you can set limits are:

- CPU
- Disk
- Memory
- Packet rate
- Kilobytes per second (throughput rate)
- Current connections

To set limits thresholds for BIG-IP Controllers

1. In the navigation pane, expand the **Servers** item and click **BIG-IP Controllers**.

2. In the Limits Settings column of the BIG-IP Controller for which you want to set limit thresholds, click the Configure Limits button



The Modify Server Limits Settings screen opens.

3. Check the metrics for which you want to set limits, and type values based on your network resources. For more information and help on this screen, click **Help** on the toolbar.

You can also set limits thresholds on virtual server resources. Please note that if a server meets or exceeds its limits settings, both the server and the virtual servers it manages are marked as unavailable for load balancing. You can quickly review the availability of any of your servers or virtual servers in the Statistics screens in the Configuration utility.

Other resources

Monitoring system performance

The Statistics screens in the Configuration utility provide a great deal of information about the 3-DNS Controller. For example, you can monitor server performance and view limits settings in the Server and Virtual Server Metrics statistics screen. For more information, see Chapter 6, *Administration and Monitoring*.

Viewing your configuration

The Network Map provides an interactive map of your configuration. You can see how the data centers, servers, and virtual servers you configured are related to the wide IPs and pools you created for load balancing. You can also make real-time changes to your configuration from the Network Map. For more information, see Chapter 6, *Network Map*, in the **3-DNS Reference Guide**.

To view the Network Map

1. In the navigation pane, click **Network Map**.
The Network Map screen opens.
2. To open the Network Map in a separate popup screen, click **Undock**. (This is useful if you are making a series of changes and want to see how it affects your configuration.)



4

Configuring a Content Delivery Network

- Introducing the content delivery network
- Deciding to use a CDN provider
- Setting up a CDN provider configuration
- Ensuring resource availability
- Monitoring the configuration

Introducing the content delivery network

A *content delivery network* (CDN) is a network of clusters that includes devices designed and configured to maximize the speed at which a content provider's content is delivered. The purpose and goal of a content delivery network is to cache content closer, in Internet terms, to the user than the origin site is. Using a CDN to deliver content greatly reduces wide area network (WAN) latency so the content gets to the user more quickly, and the origin site servers are not overloaded and slowed by requests for content. The fundamental WAN traffic distribution mechanism in all CDNs that we know about is DNS.

Using the 3-DNS Controller in a CDN

The following features make the 3-DNS Controller a logical choice for the wide-area traffic management in a CDN.

- ◆ **CDN switching**

CDN switching is the functionality of the 3-DNS Controller that allows a user to delegate global traffic to a third-party network. The two features of the 3-DNS Controller that make CDN switching possible are:

- **Geographic redirection**

The 3-DNS Controller uses the Topology load balancing mode Topology to redirect DNS requests based on location information derived from the DNS query message. You can set up wide IPs so that the controller delegates DNS queries either to a data center, by responding with **A** records, or to a CDN provider, by responding with a **CNAME** record and two or more **NS** records.

- **CDN providers**

We have partnered with several CDN providers to facilitate usage of CDNs. To take advantage of these content delivery partnerships, you can designate a pool type CDN on the 3-DNS Controller so that the controller redirects requests to a CDN provider's name servers rather than to a grouping of virtual servers.

- ◆ **Resource monitoring, limits, and thresholds**

The 3-DNS Controller has sophisticated monitoring screens so you can quickly analyze the performance and availability of your network resources. You can also set limits on physical and throughput resources to ensure that your content is always available and none of your resources are overtaxed.

Reviewing a sample CDN configuration

The two following diagrams illustrate how DNS query resolutions for content delivery networks are processed by the 3-DNS Controller. In the example, the content provider for **www.download.domain.com** has two data centers, one in San Jose, California (see Figure 4.1), and one in Washington, DC (see Figure 4.2). The 3-DNS Controllers (in the two data centers) use the Topology load balancing mode to direct the DNS queries to the geographically closest virtual servers.

In Figure 4.1, a local DNS server in Seattle, Washington, sends a query for the domain **www.download.domain.com** (1A). Based on the location information in the query packet header, the 3-DNS Controller in the content provider's North American data center resolves the query to the best virtual server in that data center, and sends an **A** record response to the Seattle LDNS (1B).

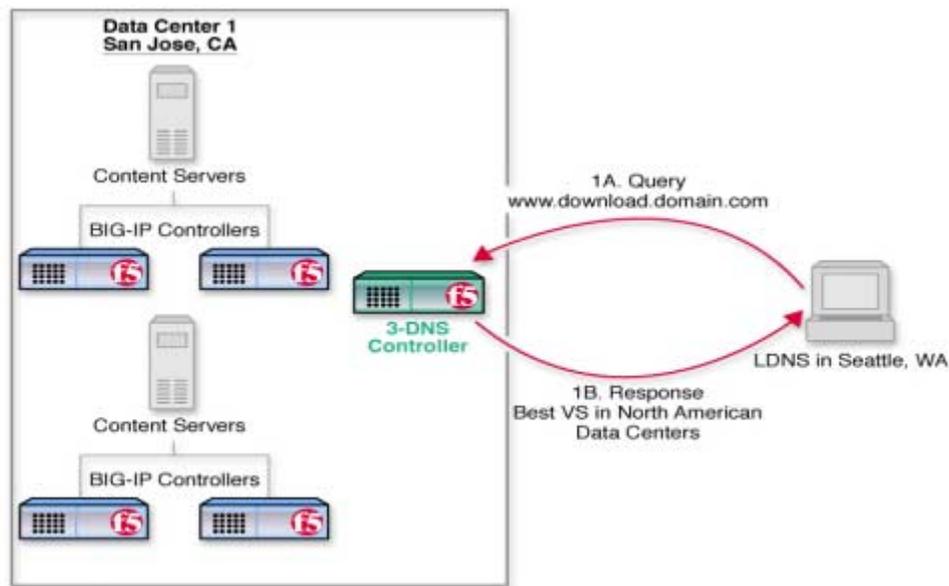


Figure 4.1 DNS query resolution based on Topology load balancing mode

In Figure 4.2, a local DNS server in London sends a query for the same domain, **www.download.domain.com** (2A). Based on the location information in the query packet header, the 3-DNS Controller in the content provider's North American data center responds to the London LDNS with delegation information (a **CNAME** record and two or more **NS** records) about the DNS for the content delivery peer (2B). The London LDNS then sends the redirected query (based on the **CNAME** record) for

www.download.domain.com to the CDN provider (2C). The CDN provider's DNS server responds with the IP address of the best virtual server for resolution among those in the CDN (2D). The CDN provider's cache servers resolve to the origin site virtual servers for cache refreshes using a different domain name (**origin.download.domain.com**).

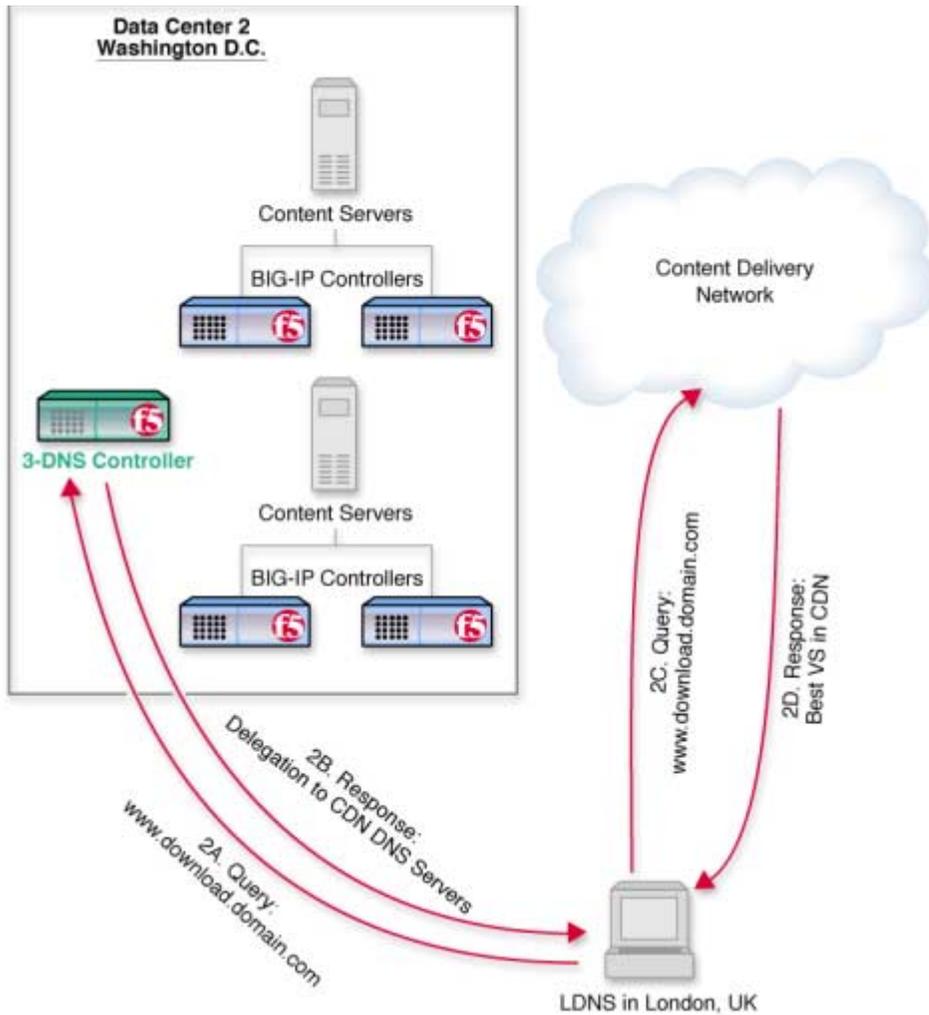


Figure 4.2 DNS query resolution to content delivery network provider

Deciding to use a CDN provider

The 3-DNS Controller is well-suited to serve as the wide-area traffic manager (WATM), for CDNs that have many of the following attributes:

- ◆ The CDN provider has a global presence around the edge of the Internet.
- ◆ The CDN provider outsources a content delivery infrastructure to content providers.
- ◆ The CDN provider is the authoritative DNS for the content provider's domain, and uses DNS to find a data center with CDN resources at the edge of the network nearest to the client.
- ◆ The CDN provider serves all of the content provider's traffic because the CDN is authoritative for the content provider's domain. Content providers manage this by creating logical groupings of their content under different domains. For example, an investment firm might have a CDN host their news content with the subdomain, **news.domain.com**, while they serve their stock quotes content with the subdomain, **quote.domain.com**, from their corporate data center.
- ◆ The CDN provider charges X dollars per megabit per second. The CDN provider determines billing by collecting and processing edge cache and server logs.
- ◆ The CDN provider has an infrastructure in place to manage the multitude of geographically distributed devices.
- ◆ The CDN provider usually establishes some type of service level agreement (SLA) to ensure that content is being served faster from the CDN than from the content provider's origin servers.

Setting up a CDN provider configuration

The following sections describe the specific tasks you perform to set up a CDN provider configuration, as shown in the example configuration on page 4-2. The tasks are as follows:

- Adding data centers
- Adding 3-DNS Controllers
- Adding servers
- Adding wide IPs and pools
- Adding a topology statement

Please review the tasks before you actually perform them so that you are familiar with the process.

Adding data centers

The first task you perform is to add the data centers to the configuration on the 3-DNS Controller.

To add data centers using the Configuration utility

1. In the navigation pane, click **Data Centers**.
The Data Centers screen opens.
2. Click **Add Data Center** on the toolbar.
The Add Data Centers screen opens.
3. Add the data center information. For our example, we add the two data centers labeled **Data Center 1** and **Data Center 2**.
4. Repeat the previous steps to add all of your data centers to the configuration.

Adding 3-DNS Controllers

Once you have added all of your data centers to the 3-DNS Controller configuration, you are ready to let the controller you are configuring know about other 3-DNS Controllers in your network.

◆ Note

*Please note that when you are working with more than one 3-DNS Controller, you create your entire configuration on one controller and then add the second controller using the **3dns_add** script. The **3dns_add** script copies the entire configuration from the first controller onto the second controller, and synchronizes all of the settings. For details on configuring additional 3-DNS Controllers in existing networks, using the **3dns_add** script, see Chapter 5, **Adding 3-DNS Controllers to the Network**.*

To add 3-DNS Controllers using the Configuration utility

1. In the navigation pane, expand the **Servers** item, then click **3-DNS Controllers**.
The 3-DNS Controllers screen opens.
2. Click **Add 3-DNS Controller** on the toolbar.
The Add New 3-DNS Controller screen opens.
3. Add the 3-DNS Controller information.
4. Repeat the previous steps to add any additional 3-DNS Controllers to the configuration.

Adding servers

Now you are ready to let the controller know about any BIG-IP Controllers, EDGE-FX Caches, or hosts that you have in your data centers. The servers and virtual servers that you add to this configuration are the servers that host your origin site content. For specific information on configuring any of these server types, please review *Setting up servers*, on page 2-15.

Adding wide IPs and pools

Once you have added all the physical elements to the 3-DNS Controller configuration, you can begin configuring wide IPs and pools for the CDN configuration. In addition to setting up the wide IPs and pools for your origin site, you also set up a pool for the CDN provider.

Before you start adding wide IPs, verify that you have configured all the virtual servers you need for load balancing for your origin site. The following instructions describe how to set up the CDN configuration shown in Figures 4.1 and 4.2.

To add a wide IP and pool using the Configuration utility

1. In the navigation pane, click **Wide IPs**.
The Wide IP List screen opens.
2. Click **Add Wide IP** on the toolbar.
The Add a New Wide IP screen opens.
3. Add the wide IP address, name, and port information. For our example, the wide IP name is **www.download.domain.com**.
4. For the **Pool LB Mode**, select **Topology** and click **Next**.
The Configure Load Balancing for New Pool screen opens.
5. In the Configure Load Balancing for New Pool screen, update these settings:
 - a) Add the pool name.
For our example, the first pool name is **origin**.
 - b) Check the **Use Dynamic Ratio** option.
 - c) In the **Load Balancing Modes, Preferred** list, select **Round Trip Time**.
 - d) In the **Load Balancing Modes, Alternate** list, select **Packet Rate**.
 - e) In the **Load Balancing Modes, Fallback** list, select **Round Robin**.
 - f) Accept the defaults for the rest of the settings and click **Next**.
The Select Virtual Servers screen opens.

6. In the Select Virtual Servers screen, check the virtual servers among which you want the 3-DNS Controller to load balance DNS requests, and click **Finish**.
The 3-DNS Controller adds the wide IP and settings to the configuration. For our example, you would check the virtual servers that map to the download site content in the North American data center.

To add a CDN provider pool to the wide IP

1. In the navigation pane, click **Wide IPs**.
The Wide IP List screen opens.
2. In the Wide IP List screen, click **1 Pools** in the Pools column for the wide IP **www.download.domain.com**.
The Modify Wide IP Pools screen opens.
3. On the toolbar, click **Add Pool**.
The Configure Load Balancing for New Pool opens.
4. In the Configure Load Balancing for New Pool screen, update these settings:
 - a) Add the pool name.
For our example, the CDN provider pool name is **cdn_pool**.
 - b) In the Pool TTL box, type **60**. With a longer time-to-live, an LDNS has time to follow the **CNAME** record and redirect queries to the CDN.
 - c) In the **Load Balancing Modes, Preferred** list, select **Round Robin**.
 - d) In the **Load Balancing Modes, Alternate** list, select **None**.
 - e) In the **Dynamic Delegation, Type** list, select **CDN**.
 - f) In the **Dynamic Delegation, Canonical Name** box, type the canonical name that you want the 3-DNS Controller to deliver in the **CNAME** record when it redirects traffic to the CDN provider. For our example, the canonical name is **www.cdn.download.domain.com**. Note that the canonical name for the CDN pool type automatically becomes an alias for the wide IP.
 - g) In the **Dynamic Delegation, Zone Name** box, type the name of the zone for which the CDN provider's DNS servers are authoritative. For our example, the zone name is **cdn.download.domain.com**.
 - h) Accept the defaults for the rest of the settings, and click **Next**.
The Select CDN for <pool name> screen opens.

5. In the Select CDN for <pool name> screen, select the CDN provider that hosts your content and click **Update**.

You have now set up the load balancing and delegation pools for your domain. The last required configuration step is to create a topology statement.

Adding a topology statement

The topology statement contains the topology records that the 3-DNS Controller uses to load balance DNS queries from geographically dispersed local DNS servers. The following procedure describes how to set up a topology statement, with two topology records, for our example.

◆ Note

*For more detailed information on working with topology on the 3-DNS Controller, see Chapter 11, **Topology**, in the **3-DNS Reference Guide**. For information on setting up globally-distributed network with Topology load balancing, see Chapter 3, **Configuring a Globally-Distributed Network**, in this guide.*

To set up topology records using the Configuration utility

1. In the navigation pane, click **Topology**.
The Manage Topology Records screen opens.
2. For the first topology record, select **Continent** in the upper **LDNS** box.
3. In the lower **LDNS** box, select **North America**.
4. In the upper **Server** box, select **Wide IP Pool**.
5. In the lower **Server** box, select **origin**.
6. In the **Weight** box, type a value. For our example, we type **100**.
7. Click **Add**.
The first topology record is added to the configuration.
8. For the second topology record, in the upper **LDNS** box select **Continent**.
9. In the lower **LDNS** box, select **North America**.
10. Check the **LDNS Not Equal** box.
11. In the upper **Server** box, select **Wide IP Pool**.
12. In the lower **Server** box, select **cdn_pool**.
13. In the **Weight** box, type a value. For our example, we type **100**.

14. Click **Add**.

The second topology record is added to the configuration.

Now you have created a topology statement for your CDN and the 3-DNS Controller can successfully load balance DNS queries based on the location information derived from the DNS query message.

Ensuring resource availability

The following resource availability settings are designed to ensure that your content is always available and that your system resources are not overtaxed to the point of failure. The resource availability settings you may want to use with your CDN configuration are:

◆ **Last resort pool**

You can designate a pool as the last resort pool so that in the event that all other pools become unavailable for load balancing, the 3-DNS Controller directs DNS queries to the virtual servers in this pool. For information on configuring a last resort pool, see *Using the last resort pool designation* in Chapter 5, *Load Balancing*, in the **3-DNS Reference Guide**.

◆ **Limit settings**

You can set limits on system resources and throughput to enhance availability. You can set limits for any server type, virtual servers, and pools. For more information on setting limits, view the online help for the Modify Limit Settings screens in the Configuration utility.

Monitoring the configuration

The following resources can help you monitor your configuration and troubleshoot problems.

- ◆ You can view performance metrics, limit settings, and other details about your data centers, servers, virtual servers, wide IPs, and pools in the Statistics screens in the Configuration utility. For more information on specific Statistics screens, click **Help** on the toolbar.
- ◆ You can view your configuration using the Network Map in the Configuration utility. You can also make modifications to the configuration from the Network Map. Click **Help** on the toolbar if you have questions on how to use the Network Map.
- ◆ You can review detailed information on the specific features of the 3-DNS Controller in the **3-DNS Reference Guide**.



5

Adding 3-DNS Controllers to the Network

- Working with more than one 3-DNS Controller
- Preparing to add a second 3-DNS Controller to your network
- Running the 3dns_add script
- Verifying the configuration

Working with more than one 3-DNS Controller

When you are working with more than one 3-DNS Controller in your network, and you want the controllers to load balance to the same virtual servers, you can create your entire configuration on one controller and then add the second controller using the **3dns_add** script. The **3dns_add** script copies the entire configuration from the first controller onto the second controller, and synchronizes all of the settings between the controllers. When you are finished, the first controller acts as the principal controller in the sync group, and the second controller becomes a receiver controller. (For more information about sync groups, see *Working with sync groups*, on page 2-29.)

The following sections of this chapter describe the procedures you follow to add a 3-DNS Controller into a network that already has at least one 3-DNS Controller configured and working properly. If you are adding the first 3-DNS Controller to your network, refer to Chapter 2, *Essential Configuration Tasks*.

◆ Note

*If you are adding a second 3-DNS Controller to your network but do not want it to be in the same sync group as your first controller, or you want the second 3-DNS Controller to load balance to a different set of virtual servers, then do not use the **3dns_add** script.*

Preparing to add a second 3-DNS Controller to your network

Before you run the **3dns_add** script on any additional 3-DNS Controllers you are adding to your network, you should complete the following tasks:

- ◆ Physically install the second 3-DNS Controller in its data center. (For more information on hardware installation, see the **3-DNS Installation Guide**, or, if you are running the 3-DNS module on the BIG-IP Controller, refer to the **BIG-IP Installation Guide**.)
- ◆ Run the First-Time Boot utility on the second controller. (For more information on the First-Time Boot utility, see the **3-DNS Installation Guide**, or if you are running the 3-DNS module on the BIG-IP Controller, refer to the **BIG-IP Installation Guide**.)
- ◆ Make the principal 3-DNS Controller aware of the IP address, fully-qualified domain name, and data center location of the second 3-DNS Controller. (See the following section, *Making the principal 3-DNS Controller aware of the additional controller*.)

Completing these tasks ensures that when you run the **3dns_add** script, the second 3-DNS Controller successfully copies the configuration information from the first 3-DNS Controller.

Installing the hardware and running the First-Time Boot utility

You can find detailed instructions on installing the 3-DNS Controller hardware in the Installation Guide. The Installation Guide also includes detailed instructions on running the First-Time Boot utility. When you have finished this part of the setup for the second controller, do not make any other changes to the configuration.

◆ Note

*If you are working with the 3-DNS module on the BIG-IP Controller, please refer to the **BIG-IP Installation Guide**, which is included in the Administrator Kit. If you are working with the standalone 3-DNS Controller, please refer to the **3-DNS Installation Guide**, which is included in the Administrator Kit.*

Making the principal 3-DNS Controller aware of the additional controller

Once you have installed the hardware and run the First-Time Boot utility on the new controller, you add its configuration information to the existing 3-DNS Controller. The existing controller becomes the principal controller in the sync group once you run the **3dns_add** script on the new controller.

To add the new controller to the existing controller's configuration using the Configuration utility

1. Add the second data center to the configuration.
 - a) In the navigation pane, click **Data Centers**.
The Data Centers screen opens.
 - b) Click **Add Data Center** on the toolbar.
The Add Data Centers screen opens.
 - c) Add the information for the data center where you installed the new controller, and click **Update**.
2. Add the second 3-DNS Controller to the configuration.
 - a) In the navigation pane, expand the **Servers** item, and click **3-DNS Controllers**.
The 3-DNS Controllers screen opens.
 - b) Click **Add 3-DNS Controller** on the toolbar.
The Add New 3-DNS Controller screen opens.

- c) Add the information for the new controller and click **Update**.
3. Add the new controller to the existing controller's sync group.
 - a) In the navigation pane, click **3-DNS Sync**.
The System-Synchronization screen opens.
 - b) Click **Add to Group** on the toolbar.
The Add a 3-DNS to a Sync Group screen opens.
 - c) Check the controller you just defined and click **Add**.
The new controller becomes a receiver in the sync group of the existing controller.

You have now successfully added the new controller to the existing controller's configuration. The following sections describe how to run the **3dns_add** script and verify the configuration.

Running the 3dns_add script

You can run the **3dns_add** script on the new 3-DNS Controller either using a remote secure shell session, or using a monitor and keyboard connected locally to the controller.

To run the 3dns_add script

1. At the **login** prompt, type **root**.
2. At the **password** prompt, type the password you configured when you ran the First-Time Boot utility.
3. To run the script, type **3dns_add** at the command line.
The script copies the entire configuration of the existing 3-DNS Controller to the new controller.

Verifying the configuration

Once the script finishes, we recommend that you verify the following aspects of your configuration:

- Verify that each 3-DNS Controller has the necessary agents and daemons running.
- Verify that any servers you configured are **up** and available to receive load balancing requests.

- Verify that any virtual servers you configured are **up** and available to respond to requests.
- Verify that any wide IPs you configured are load balancing requests as you configured them.

You can perform these verification tasks on any of the controllers in the sync group. The following sections describe the verification process in detail.

◆ **Tip**

You may want to wait a few minutes before you verify the configuration so that the 3-DNS Controllers have time to synchronize with each other.

To verify that each 3-DNS Controller has the necessary agents and daemons running

1. In the navigation pane, expand the **Statistics** item and click **3-DNS**. The 3-DNS Statistics screen opens.
2. Click the **Refresh** button.
3. In the Server and Big3d columns, make sure the status is **up**, which is indicated by a small green ball.
4. In the E/D column, make sure the controllers are enabled.
5. If the status of any of your controllers is **down**, **unknown**, or **unavailable**, wait a few minutes and click **Refresh** again. If status of the controllers remains **down**, **unknown**, or **unavailable**, contact Technical Support for assistance.

To verify that the servers you configured are up

1. In the navigation pane, expand the **Statistics** item and click **Data Centers**. The Data Centers Statistics screen opens.
2. Click the **Refresh** button.
3. In the Server column, make sure that the status of each BIG-IP Controller, EDGE-FX Cache, or host you configured is **up**, which is indicated by a small green ball.
4. If the status of any of your servers is **down**, **unknown**, or **unavailable**, wait a few minutes and click **Refresh** again. If status of the servers remains **down**, **unknown**, or **unavailable**, contact Technical Support for assistance.

To verify that the virtual servers you configured are up

1. In the navigation pane, expand the **Statistics** item and click **Virtual Servers**.
The Data Centers Statistics screen opens.
2. Click the **Refresh** button.
3. In the OK column, make sure that the status of each virtual server you configured is **up**, which is indicated by a small green ball.
4. If the status of any of your virtual servers is **down**, **unknown**, or **unavailable**, wait a few minutes and click **Refresh** again. If status of the virtual servers remains **down**, **unknown**, or **unavailable**, contact Technical Support for assistance.

To verify that the wide IPs are load balancing properly

1. At the command prompt, type **nslookup** and press Enter.
2. Type the following command where **<IP_address>** is the IP address of one of your 3-DNS Controllers, and press Enter.

```
server <IP_address>
```
3. Type the name of the wide IP (for example, news.domain.com) for which you want to verify load balancing and press Enter.

If the virtual servers belonging to the wide IP appear in a pattern that reflects the load balancing mode you selected, you have successfully configured your 3-DNS Controllers. Note that you can repeat the previous procedure for each wide IP you configured.

◆ Note

*This is the only verification task that you perform from the command line. The **nslookup** utility is part of DNS distributions. For more information on how to use the **nslookup** utility, please refer to the book, **DNS and BIND**, by Albitz and Liu.*



6

Administration and Monitoring

- Monitoring and administration utilities provided on the 3-DNS Controller
- Working with the 3-DNS Maintenance menu
- Managing users on the 3-DNS Controller
- Using the MindTerm SSH Console
- Using the Network Map
- Viewing system statistics

Monitoring and administration utilities provided on the 3-DNS Controller

The 3-DNS Controller provides utilities for monitoring and administration. You can perform configuration tasks, and monitor system statistics for all components of the 3-DNS Controller.

The 3-DNS Controller provides the following configuration, monitoring, and administration utilities:

◆ **Configuration utility**

The Configuration utility is a browser-based application you can use to configure and monitor the 3-DNS Controller. The Configuration utility supports Netscape Navigator, version 4.5 or later, and Internet Explorer, version 4.02 or later.

◆ **3-DNS Maintenance menu**

The 3-DNS Maintenance menu is a command line utility you can use to configure the 3-DNS Controller. Use the 3-DNS Maintenance menu to simplify certain tasks such as updating the **big3d** agent and editing the **wideip.conf** file.

◆ **MindTerm SSH Console**

The MindTerm SSH Console is a secure shell tool that you can use, from the Configuration utility, to view the command line utility from a web browser.

◆ **Network Map**

The Network Map is an interactive screen, in the Configuration utility, where you can view your physical and logical configurations simultaneously.

◆ **Statistics screens**

Using the Statistics screens in the Configuration utility, you can view a myriad of performance and metrics details about the 3-DNS Controller, the servers and the virtual servers it manages, and the load balancing it performs.

Working with the 3-DNS Maintenance menu

You can use the 3-DNS Maintenance menu to configure and monitor the 3-DNS Controller from the command line.

You can use the 3-DNS Maintenance menu to perform the following types of manual configuration tasks:

- Edit the **wideip.conf** configuration file
- Edit BIND configuration files

- View statistics
- Work with the **big3d** agent
- Manage synchronized files
- Work with security issues
- Configure the 3-DNS web server
- Work with **syncd**
- Configure NTP
- Configure NameSurfer

◆ **WARNING**

*If you use the browser-based NameSurfer application, you cannot use the **Edit BIND Configuration** command on the 3-DNS Maintenance menu to configure your DNS zone files. For more information on managing your zone files, please refer to **Planning DNS zone file management**, on page 2-6.*

Figure 6.1 shows the main screen of the 3-DNS Maintenance menu.

```
3 D N S(®) Maintenance Menu

Configure SSH communication with remote devices
Generate and Copy iQuery Encryption Key
Check remote versions of big3d
Edit big3d matrix
Install and Start big3d
Edit BIND Configuration
Edit 3-DNS Configuration
Backup the 3-DNS Controller
Restore a 3-DNS Controller from a backup
Synchronize Metrics Data
Restart big3d
Reconfigure 3-DNS Configuration Utility
Restart 3-DNS Configuration Utility
Change/Add Users for 3-DNS Configuration Utility
Dump 3dnsd Statistics
Stop syncd
Restart syncd
Configure connection to NTP time server
Configure NameSurfer(TM)
Enter 'q' to Quit
```

Figure 6.1 The 3-DNS Maintenance menu main screen

To use the 3-DNS Maintenance menu from the command line

1. On the command line, type the following command to open the menu:
`3dnsmaint`
2. From the menu, choose the command to you wish to run, and press the Enter key.

Each command is described in the following sections.

Configuring zone files and wide IPs

We recommend that you use NameSurfer to configure BIND zone files, and that you use the Configuration utility to configure wide IPs. However, if you choose to edit the BIND zone files and the 3-DNS Controller configuration files from the command line, use the following commands.

Edit BIND Configuration

The **Edit BIND Configuration** command opens the **named.conf** file for editing.

◆ WARNING

Use this command only if you are performing all configuration tasks from the command line. It is important that you do not use this command if you are using NameSurfer.

Edit 3-DNS Configuration

The **Edit 3-DNS Configuration** command runs the **edit_wideip** script, which performs the following tasks:

- Opens the **wideip.conf** file for editing
- Copies the **wideip.conf** file to all other 3-DNS Controllers in the local 3-DNS Controller's sync group
- Restarts **3dnscd**

Viewing statistics

From the Maintenance menu, use the **Dump 3dnscd Statistics** command to view various 3-DNS Controller statistics. The **Dump 3dnscd Statistics** command corresponds to the **3dprint** script, which lets you view the following statistics screens at the command line:

- ◆ **3-DNS**

This object displays statistics about each 3-DNS Controller in your network. The statistics include such things as whether the controller is enabled or disabled, the number of packets per second traveling in and out of the 3-DNS Controller during the last sample period, the name of the sync group to which each 3-DNS Controller belongs, and so on.
- ◆ **BIG-IP**

This object displays statistics about all BIG-IP Controllers known to the 3-DNS Controller. The statistics include such things as the number of virtual servers each BIG-IP Controller manages, the number of times the 3-DNS Controller resolves requests to those virtual servers, and more.
- ◆ **EDGE-FX**

This object displays statistics about all EDGE-FX Caches known to the 3-DNS Controller. The statistics include such things as the number of virtual servers each EDGE-FX Cache manages, the number of times the 3-DNS Controller resolves requests to those virtual servers, and more.
- ◆ **Hosts**

This object displays statistics about all hosts known to the 3-DNS Controller, such as the number of times the 3-DNS Controller resolves requests to the host, and the number of virtual servers that the hosts manage.
- ◆ **Virtual Servers**

This object displays statistics about BIG-IP Controller, EDGE-FX Cache, and host virtual servers; the statistics include such things as the server state, and the number of times it has received resolution requests.
- ◆ **Paths**

This object displays path statistics such as round trip time, packet completion rate, the remaining time to live (TTL) before a path's metric data needs to be refreshed, and so on.
- ◆ **Local DNS**

This object displays statistics collected for LDNS servers: the number of resolution requests received from a given server, the current protocol used to probe the server, and more.
- ◆ **Wide IPs**

This object displays statistics about each wide IP defined on the 3-DNS Controller. The statistics include such things as load balancing information, the remaining time to live (TTL) before the wide IP's metrics data needs to be refreshed, and so on.
- ◆ **Globals**

This object displays statistics about the globals sub-statements. The statistics include such things as the current and default values for each of the globals sub-statements, and whether you have to restart **3dnsd** when you make changes to the parameters.

- ◆ **Summary**

This object displays summary statistics such as the 3-DNS Controller version, the total number of resolved requests, and the load balancing methods used to resolve requests.

- ◆ **Data Centers**

This object displays statistics about the data centers and their servers in your network. The statistics include such things as the names of the data centers, the name or IP address of the servers in the data center, and whether the data center is enabled or disabled.

- ◆ **Sync Groups**

This object displays statistics about each sync group in your network. The statistics include such things as the name of the sync group, whether **3dnsd** is running on each 3-DNS Controller, whether the **big3d** agent is running on each 3-DNS Controller, the name and IP address of the 3-DNS Controller, and whether the 3-DNS Controller is a principal or receiver.

To view more statistics information, expand the **Statistics** item on the navigation pane in the Configuration utility.

Working with the big3d agent

You can use the following commands to work with the **big3d** agent, which collects information about paths between a data center and a specific local DNS server.

Check big3d versions

The **Check remote versions of big3d** command runs the **big3d_version** script. This script checks that the correct version of **big3d** is running on all BIG-IP Controllers, EDGE-FX Caches, and GLOBAL-SITE Controllers known to the 3-DNS Controller.

Edit big3d matrix

The **Edit big3d matrix** command opens an editable file that lists version numbers, and the appropriate **big3d** agent, for all BIG-IP Controllers, EDGE-FX Caches, and GLOBAL-SITE Controllers known to the 3-DNS Controller.

You do not need to edit this file unless a new version of BIG-IP Controller, EDGE-FX Cache, or GLOBAL-SITE Controller creates a conflict. If this happens, you need to place a new version of the **big3d** agent on all affected servers.

The **Install and Start big3d** command uses the matrix file to determine which version of the **big3d** agent to transfer to the BIG-IP Controllers, EDGE-FX Caches, and GLOBAL-SITE Controllers.

Install and Start big3d

The **Install and Start big3d** command runs the **big3d_install** script, which installs and starts the appropriate version of the **big3d** agent on each BIG-IP Controller, EDGE-FX Cache, and GLOBAL-SITE Controller in the network.

Restart big3d

The **Restart big3d** command runs the **big3d_restart** script, which stops and restarts the **big3d** agent on each BIG-IP Controller, EDGE-FX Cache, and GLOBAL-SITE Controller.

Managing synchronized files

You can use the following commands to copy metrics data to a new 3-DNS Controller, to archive synchronized files, or to retrieve an archive.

Synchronize Metrics Data

The **Synchronize Metrics Data** command runs the **3dns_sync_metrics** script, which prompts you to copy metrics data from a remote 3-DNS Controller to the local 3-DNS Controller.

You should use this command only when you are configuring a new 3-DNS Controller in a network that already contains 3-DNS Controllers.

Working with security issues

You can use the following commands to address security issues for your network setup.

Configure SSH communication with remote devices

The **Configure SSH communication with remote devices** command runs the **config_ssh** script, which configures secure shell access to any new 3-DNS Controller, BIG-IP Controller, EDGE-FX Cache, or GLOBAL-SITE Controller that is added to a network.

For more information, see Chapter 9, *Scripts*, and Chapter 12, *Utilities*, in the *3-DNS Reference Guide*.

Generate and Copy iQuery Encryption key

The **Generate and Copy iQuery Encryption key** command runs the **install_key** script, which then runs the **F5makekey** program. The **F5makekey** program generates a seed key for encrypting communications between the 3-DNS Controller and BIG-IP Controllers, EDGE-FX Caches, and GLOBAL-SITE Controllers.

For more information, see Chapter 9, *Scripts*, and Chapter 12, *Utilities*, in the *3-DNS Reference Guide*.

◆ Note

This command is not available in the non-crypto version of the 3-DNS Controller.

Configuring the 3-DNS Configuration utility

You can use the following commands to configure the 3-DNS Configuration utility, which is hosted by the 3-DNS web server.

Reconfigure 3-DNS Configuration Utility

The **Reconfigure 3-DNS Configuration Utility** command runs the **config_httpd** script, which lets you make configuration changes to the 3-DNS web server.

Restart 3-DNS Configuration Utility

The **Restart 3-DNS Configuration Utility** command runs the **3dns_admin_start** script, which restarts the 3-DNS web server.

Change/Add Users for 3-DNS Configuration Utility

The **Change/Add Users for 3-DNS Configuration Utility** command runs the **3dns_web_passwd** script, which lets you provide one of three levels of access to the 3-DNS Configuration utility for selected users only, and assign passwords for those users. The three levels of user access are:

- ◆ **Read-only**
Users with this level of access can only view the configuration and statistics information in the Configuration utility.
- ◆ **Partial read/write**
Users with this level of access can view configuration and statistics information in the Configuration utility. They can also enable and disable objects in the configuration.

◆ **Full read/write**

Users with this level of access have full administrative access to all components of the Configuration utility.

You can also add, remove, and modify users and their administrative access levels using the Configuration utility. For more information, please see *Adding users for the Configuration utility*, on page 6-10.

Working with syncd

You can use the following commands to work with **syncd**, the synchronization daemon that runs on all 3-DNS Controllers. The function of **syncd** is to update and synchronize all 3-DNS Controller configuration files.

Stop syncd

The **Stop syncd** command runs the **syncd_stop** script, which stops the **syncd** daemon, if it is running.

Restart syncd

The **Restart syncd** command runs the **syncd_start** script, which restarts the **syncd** daemon if it is already running, or starts it if it is not.

Configuring NTP

The 3-DNS Controllers in a network must have their time synchronized to within a few seconds of each other. If you do not synchronize the controllers, it is done by default through iQuery messages exchanged between 3-DNS Controllers. However, the following command allows much more precise time synchronization between the 3-DNS Controllers.

Configure Connection to NTP Time Server

The **Configure Connection to NTP Time Server** command allows the 3-DNS Controller to synchronize its time to a public NTP (Network Time Protocol) server on the Internet. To simplify the task of choosing the best time server, this command has a list of regional time servers built into it. A 3-DNS Controller is not required to have NTP configured; depending on the network configuration, it may not be possible to configure NTP (for example, if the 3-DNS Controller is behind a firewall and the firewall does not pass NTP packets).

Configuring NameSurfer

You can use the following command to have NameSurfer handle DNS zone file management on the 3-DNS Controller.

Configure NameSurfer

The **Configure NameSurfer** command makes NameSurfer the master on the 3-DNS Controller, and NameSurfer then handles the zone file management, dealing with all changes and updates to the zone files. Note that configuring NameSurfer as the master is an optional setting. You can access the NameSurfer application in the Configuration utility by clicking **NameSurfer** in the navigation pane.

WARNING

If you do not set NameSurfer to be the master for your wide IP zones, you must maintain all of your zone file information manually.

Managing users on the 3-DNS Controller

The First-Time Boot utility prompts you to define a password that allows remote access to the 3-DNS Controller, and also prompts you to define a user name and password for the 3-DNS web server, which hosts the Configuration utility. You can change these passwords at any time.

Changing the root password

The root password is the password that allows access to the 3-DNS Controller itself, at the command line.

To change the root password for command line access

1. At the 3-DNS Controller command line, log in as **root** and use the **passwd** command.
2. At the **password** prompt, type the password you want to use for the 3-DNS Controller and press Enter.
3. To confirm the password, retype it and press Enter.

Adding users for the Configuration utility

You can create new users for the Configuration utility, change a password for an existing user, or recreate the password file altogether, without actually going through the 3-DNS web server configuration process. (The 3-DNS web server hosts the Configuration utility.) You can also modify a user's administrative access level for the Configuration utility. The three level of user access are:

◆ **Read-only**

Users with this level of access can only view the configuration and statistics information in the Configuration utility.

◆ **Partial read/write**

Users with this level of access can view configuration and statistics information in the Configuration utility. They can also enable and disable objects in the configuration.

◆ **Full read/write**

Users with this level of access have full administrative access to all components of the Configuration utility.

To change or add user information using the Configuration utility

1. In the navigation pane, click **User Admin**.
The User Administration screen opens.
2. Add the user administration settings. For help on configuring the settings, click **Help** on the toolbar.

To change or add user information from the command line

1. At the command prompt, type **3dnsmaint** to open the 3-DNS Maintenance menu.
2. On the 3-DNS Maintenance menu, select the **Change/Add Users for 3-DNS Configuration Utility** command.

To create new users and change passwords for existing users from the command line

The following command creates a new user ID, or changes the password for an existing user ID. In place of the **<username>** parameter, type the user ID for which you want to create a password:

```
/usr/local/bin/htpasswd /config/httpd/users \ <username>
```

Once you enter the command, you are prompted to type the new password for the new user.

To create a new password file from the command line

The following command recreates the Configuration utility password file, and defines one new user ID and password. In place of the `<username>` parameter, type the user ID that you want to create:

```
/usr/local/htpasswd -c /config/httpd/users \ <username>
```

Once you enter the command, you are prompted to type the new password for the new user.

Using the MindTerm SSH Console

With the MindTerm SSH Console, you can open an SSH session for the 3-DNS Controller from the Configuration utility. The crypto 3-DNS Controller uses the MindTerm SSH client to enable secure command line administration. You can perform any of the command line tasks in a popup console screen.

◆ WARNING

The MindTerm SSH client requires a Java virtual machine to operate. If you are unable to run the MindTerm SSH client, make sure that you have a Java virtual machine installed and that your browser has Java enabled in the Preferences, or Options, section. For more information on Java virtual machines and download options, visit your web browser manufacturer's web site.

To open the MindTerm SSH Console using the Configuration utility

1. In the navigation pane, click **MindTerm SSH Console**.
A popup console opens.
2. When you see the command prompt, press Enter.
3. Log in to the controller as you normally would.

◆ Note

When you use the MindTerm SSH Console, you can only administer the local 3-DNS Controller. If you wish to administer remote controllers, you do so using an SSH or Telnet session from the command line on the local controller.

Using the Network Map

The Network Map is a dynamic, illustrative map of the physical and logical components of your network. The Network Map lets you see how the data centers, servers, and virtual servers you configured are mapped to the wide IPs and pools you configured. You can also make changes to your configuration from the Network Map, using the following options:

- You can double-click any object name on the Network Map to expand the object.
- You can right-click any object name to view a popup menu of configuration options for that object.

To view the Network Map using the Configuration utility

1. In the navigation pane, click **Network Map**.
The Network Map screen opens.
2. To see the relationships between the components, double-click the component. The tree expands and the component is highlighted (in blue).
3. To modify a component, right-click the component to view a popup menu, then select the item you want to change.
4. You can also click the name of the component in the status bar in the lower portion of the screen to edit the component's configuration.

For more information on the features of the Network Map, click **Help** on the toolbar.

◆ **WARNING**

The Network Map requires a Java virtual machine to operate. If you are unable to view the Network Map, make sure that you have a Java virtual machine installed and that your browser has Java enabled in the Preferences, or Options, section. For more information on Java virtual machines and download options, visit your web browser manufacturer's web site.

Viewing system statistics

Using the Configuration utility, you can view current statistics about the following objects in the configuration:

Statistics Item	Description
Summary	This statistics screen provides information about the 3-DNS Controller itself.
Globals	This statistics screen provides information on the global settings for the 3-DNS Controller.
Disabled objects	This statistics screen provides information on the servers and virtual servers that you have disabled.
Metrics	This statistics screen provides performance information for the servers and virtual servers you have configured.
Dynamic persistence requests	This statistics screen provides information on the virtual connections between local DNS servers and virtual servers for given wide IPs in the network.
Data centers	This statistics screen provides information on the data centers in your network.
Sync groups	This statistics screen provides information on the 3-DNS Controllers that are in the same sync group as the controller you are looking at.
Wide IPs	This statistics screen provides information on the wide IPs and pools you configured.
ECV	This statistics screen provides performance information for any ECV health monitors you have configured.
3-DNS Controllers	This statistics screen provides information on the 3-DNS Controllers you have configured.
BIG-IP Controllers	This statistics screen provides information on the BIG-IP Controllers you have configured.
EDGE-FX Caches	This statistics screen provides information on the EDGE-FX Caches you have configured.
Probers	This statistics screen provides information on the probers you have configured.
Hosts	This statistics screen provides information on the hosts you have configured.
Virtual servers	This statistics screen provides information on the virtual servers you have configured.

Table 6.1 Configuration utility Statistics screens

Statistics Item	Description
Paths	This statistics screen provides information on the paths created by the 3-DNS Controller when paths are required to fulfill name resolution requests.
Local DNS servers	This statistics screen provides information on the local DNS servers in the 3-DNS Controller's database.

Table 6.1 Configuration utility Statistics screens

To view system statistics

1. In the navigation pane, expand the **Statistics** item.
2. From the list, select the item representing the statistics you wish to view.
3. For details about the information displayed on a specific statistics screen, click **Help** on the toolbar.



7

Additional Load Balancing Options

- Configuring load balancing using specialized modes
- Setting up Quality of Service mode
- Working with the Global Availability mode
- Setting up load balancing for services that require multiple ports

Configuring load balancing using specialized modes

The 3-DNS Controller offers many options for load balancing DNS queries to virtual servers. The specialized modes described in this chapter help you refine the 3-DNS Controller's load balancing capabilities. This chapter describes the following specialized load balancing modes:

- Quality of Service
- Global Availability
- E-commerce

You can use these performance-based load balancing modes within in a pool, or you can use them among pools. For example, you can use the Topology mode to load balance among your pools, but you can use the Quality of Service mode within the pools. These specialized modes help you refine the 3-DNS Controller's load balancing capabilities.

In addition to the information in this chapter, Chapter 5, *Load Balancing*, in the *3-DNS Reference Guide*, contains extensive details on all of the load balancing options for the 3-DNS Controller.

Setting up Quality of Service mode

The Quality of Service mode is a user-definable mode that includes a configurable combination of the Round Trip Time (RTT), Completion Rate, Packet Rate, Topology, Hops, VS Capacity, and Kilobytes/Second (KBPS) modes. The Quality of Service mode is based on an equation that takes each of these performance factors into account. When the 3-DNS Controller selects a virtual server, it chooses the server with the best overall score.

The Quality of Service mode has default settings that make it easy to use: simply specify Quality of Service as your preferred load balancing mode. There is no need to configure it, but if you want to change the settings, you can customize the equation to put more or less weight on each individual factor. The following topics explain how to use and adjust the various settings.

Understanding QOS coefficients

Table 7.1 lists each Quality of Service (QOS) coefficient, its scale, a likely upper limit for each, and whether a higher or lower value is more efficient.

Coefficient	How measured	Example upper limit	Higher or lower?
Packet rate	Packets per second	700	Lower
Round trip time	Microseconds	2,000,000	Lower
Completion rate	Percentage of successfully transferred packets (0-100%)	100%	Higher
Topology	Score that defines network proximity by comparing server and LDNS IP addresses (0-2 ³²)	100	Higher
Hops	Number of intermediate systems transitions (hops)	64	Lower
VS capacity	Number of nodes <i>up</i>	20	Higher
Kilobytes/second	Kilobytes per second throughput	15000	Lower

Table 7.1 QOS coefficients: Ranges and limits

If you change the default QOS coefficients, keep the following issues in mind.

◆ **Scale**

The raw metrics for each coefficient are not on the same scale. For example, completion rate is measured in percentages, while the packet rate is measured in packets per second.

◆ **Normalization**

The 3-DNS Controller normalizes the raw metrics to values in the range of 0 to 10. As the QOS value is calculated, a high measurement for completion rate is good, because a high percentage of completed connections are being made, but a high value for packet rate is not desirable because the packet rate load balancing mode attempts to find a virtual server that is not overly taxed at the moment.

- **Emphasis**

You can adjust coefficients to emphasize one normalized metric over another. For example, by changing the coefficients to the values shown in Figure 7.1, you are putting the most emphasis on completion rate.

```
globals {
    qos_coeff_rtt 20
    qos_coeff_completion_rate 100
    qos_coeff_packet_rate 50
    qos_coeff_topology 0
    qos_coeff_hops 0
    qos_coeff_vs_capacity 0
    qos_coeff_kbps 0
}
```

Figure 7.1 QOS coefficients emphasizing completion rate

In the preceding example, if the completion rates for two virtual servers are close, the virtual server with the best packet rate is chosen. If both completion rates and packet rates are close, the round trip time (RTT) breaks the tie. In this example, the metrics for Topology, Hops, VS Capacity, and Kilobytes/Second modes are not used in determining how to distribute connections.

Customizing the QOS equation

You can customize the QOS equation globally, meaning that the equation applies to all wide IPs that use the Quality of Service mode. You can also customize individual wide IPs, in which case the global QOS equation settings are overwritten.

To modify global QOS coefficients using the Configuration utility

1. In the navigation pane, click **System**.
The System - General screen opens.
2. On the toolbar, click **Load Balancing**.
The System - Load Balancing screen opens.
3. Define the global QOS coefficients in the **Round Trip Time**, **Completion Rate**, **Hops**, **BIG-IP Packet Rate**, **Topology**, **VS Capacity**, and **Kilobytes/Second** boxes.
4. Click **Update**.

To modify QOS coefficients for a specific wide IP using the Configuration utility

1. In the navigation pane, click **Wide IPs**.
2. In the Wide IP column, click a wide IP name.
The Modify Wide IP screen opens.
3. On the toolbar, click **Modify Pool**.
The Modify Wide IP Pools screen opens.
4. In the Pool Name column, click the name of a pool.
The Modify Load Balancing screen opens.
5. Define the wide IP's QOS coefficients in the **Round Trip Time**, **Completion Rate**, **Hops**, **BIG-IP Packet Rate**, **Topology**, **VS Capacity**, and **Kilobytes/Second** boxes.
6. Click **Update**.

To assign global QOS coefficients from the command line

1. At the command prompt, type **3dnsmaint** to open the 3-DNS Maintenance menu.
2. On the 3-DNS Maintenance menu, select **Edit 3-DNS Configuration** to open the **wideip.conf** file.
3. Locate or add the **globals** statement. The **globals** statement should be at the top of the file.
4. Refer to the example syntax shown in Figure 7.2 to define a global QOS equation.

```
globals {  
    qos_coeff_rtt 20  
    qos_coeff_completion_rate 5  
    qos_coeff_packet_rate 3  
    qos_coeff_topology 0  
    qos_coeff_hops 0  
    qos_coeff_vs_capacity 0  
    qos_coeff_kbps 0  
}
```

Figure 7.2 Sample global QOS equation

To assign QOS coefficients for a specific wide IP from the command line

1. At the command prompt, type **3dnsmaint** to open the 3-DNS Maintenance menu.

2. On the 3-DNS Maintenance menu, select **Edit 3-DNS Configuration** to open the **wideip.conf** file.
3. Locate the **wideip** statement you want to edit.
4. Refer to the example syntax shown in Figure 7.3 to define a wide IP's QOS equation.

Figure 7.3 displays a wide IP definition that overrides the global QOS equation settings shown in Figure 7.2.

```

wideip {
  address      192.168.101.50
  service      "http"
  name         "www.wip.domain.com"
  ttl          60 // increase the domain default ttl
  qos_coeff {
    rtt         21
    hops        0
    completion_rate 7
    packet_rate 5
    topology    1
    vs_capacity 0
    kbps        0
  }
  pool {
    name        "Pool_1"
    ratio       2 // applies to pool_lbmode == ratio
    preferred   qos
    alternate   ratio
    address     192.168.101.50 ratio 2
    address     192.168.102.50 ratio 1
    address     192.168.103.50 ratio 1
  }
  pool {
    name        "Pool_2"
    ratio       1
    preferred   rr
    address     192.168.102.60 ratio 2
    address     192.168.103.60 ratio 1
  }
}

```

Figure 7.3 QOS coefficient settings that override the global QOS settings

Using the Dynamic Ratio option

When the Dynamic Ratio option is turned on, the 3-DNS Controller treats QOS scores as ratios, and it uses each server in proportion to the ratio determined by the QOS calculation. When the Dynamic Ratio option is

turned off (the default), the 3-DNS Controller uses only the server with the highest QOS score for load balancing, (in which case it is a winner takes all situation) until the metrics information is refreshed.

To turn on the Dynamic Ratio option using the Configuration utility

1. In the navigation pane, click **Wide IPs**.
2. In the Wide IP column, click a wide IP name.
The Modify Wide IP screen opens.
3. On the toolbar, click **Modify Pool**.
The Modify Wide IP Pools screen opens.
4. In the Pool Name column, click the name of a pool.
The Modify Load Balancing screen opens.
5. Check **Use Dynamic Ratio**.
6. Click **Update**.

To turn on the Dynamic Ratio option from the command line

1. At the command prompt, type **3dnsmaint** to open the 3-DNS Maintenance menu.
2. On the 3-DNS Maintenance menu, select **Edit 3-DNS Configuration** to open the **wideip.conf** file.
3. Locate the **wideip** statement and the pool definition you want to edit.

4. Add the syntax (shown in bold in Figure 7.4) to the pool definition.

```
pool {
  name <"pool_name">
  [ ratio <pool_ratio> ]
  dynamic_ratio yes
  [ rr_ldns < yes | no > ]
  [ rr_ldns_limit <number> ]
  [ preferred < completion_rate | ga | hops | kbps | leastconn | packet_rate | qos |
random | ratio | return_to_dns | rr |
  rtt | static_persist | topology | vs_capacity | null > ]
  [ alternate < ga | kbps | null | random | ratio | return_to_dns | rr |
static_persist | topology | vs_capacity > ]
  [ fallback < completion_rate | ga | hops | kbps | leastconn |
  packet_rate | qos | random | ratio | return_to_dns | rr | rtt | static_persist |
topology | vs_capacity | null > ]
  address <vs_addr>[:<port>] [ratio <weight>]
}
}
```

Figure 7.4 Enabling dynamic ratio in a pool configuration

Working with the Global Availability mode

The Global Availability mode repeatedly selects the first available virtual server in a wide IP definition to respond to DNS queries. If that virtual server becomes unavailable, subsequent connections go to the next listed virtual server in the wide IP definition.

The 3-DNS Controller always starts with the first virtual server in the list. Over time, the first server in the list receives the most connections, and the last server in the list receives the fewest connections. Figure 7.5 shows the 3-DNS Controller using the Global Availability load balancing mode.

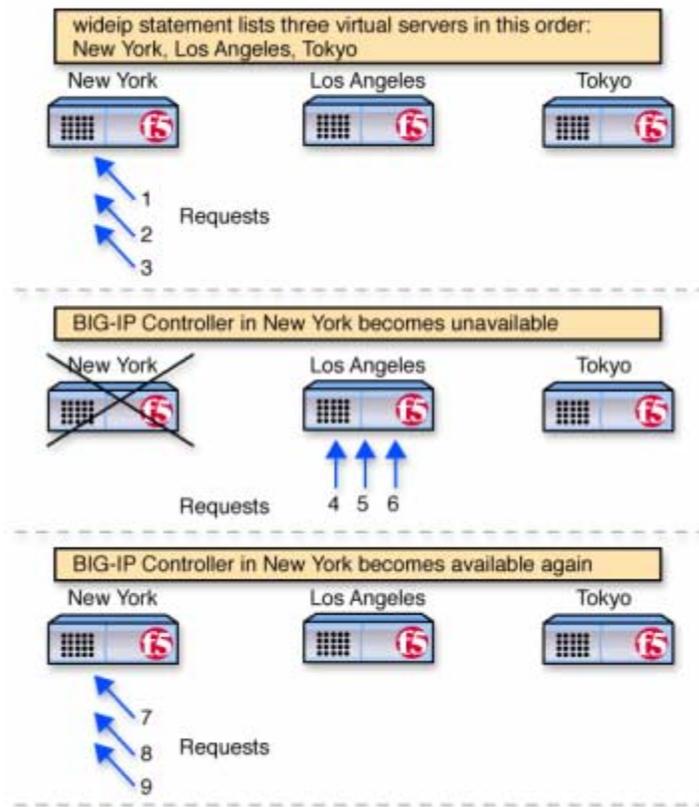


Figure 7.5 Global Availability mode

Configuring the Global Availability mode

The following sections describe how to configure the Global Availability load balancing mode.

To configure the Global Availability load balancing mode using the Configuration utility

1. In the navigation pane, click **Wide IPs**.
2. In the Wide IP column, click a wide IP name.
The Modify Wide IP screen opens.
3. On the toolbar, click **Modify Pool**.
The Modify Wide IP Pools screen opens.

4. In the Pool Name column, click the name of a pool.
The Modify Load Balancing screen opens.
5. Select Global Availability as the Preferred, Alternate, or Fallback load balancing mode.
6. Click **Update**.
7. A popup screen appears, indicating that with the Global Availability load balancing mode you must order the virtual servers. Click **OK**.
The Modify Virtual Servers screen opens.
8. In the Order column, specify the order in which you want to list the virtual servers for Global Availability.
9. Click **Update**.

To configure the Global Availability load balancing mode from the command line

1. At the command prompt, type **3dnsmaint** to open the 3-DNS Maintenance menu.
2. On the 3-DNS Maintenance menu, select **Edit 3-DNS Configuration** to open the **wideip.conf** file.
3. Locate the **wideip** statement you want to edit.
4. Define Global Availability as the preferred, alternate, or fallback load balancing mode.
5. List the virtual servers in descending order of preference. See Figure 7.6 for details.

A Global Availability configuration example

With the Global Availability load balancing mode, you can configure one data center as your primary service provider and have several alternate service providers on standby. In the **wideip** statement, list the virtual servers in descending order of preference. The first available virtual server is chosen for each resolution request.

Figure 7.6 shows a sample **wideip** definition where Global Availability is the preferred load balancing mode.

```
// Global availability
wideip {
  address      192.168.101.60
  port         80 // http
  name         "cgi.wip.domain.com"
  pool {
    name       "mypool"
    preferred  ga
    address    192.168.101.60
    address    192.168.102.60
    address    192.168.103.60
  }
}
```

Figure 7.6 Configuring a standby data center using Global Availability

The first listed virtual server (**192.168.101.60** in this example) receives all resolution requests unless it becomes unavailable. If the first listed virtual server does become unavailable, then the 3-DNS Controller sends resolution requests to the second listed virtual server, and so on.

Setting up load balancing for services that require multiple ports

Some sites require that you use multiple ports or services to access them, for example an e-commerce site. For these cases, you can configure a wide IP so that connections are not sent to a given address unless all specified ports or services are available.

To configure multiple ports for a wide IP using the Configuration utility

1. In the navigation pane, click **Wide IPs**.
2. In the Wide IP column, click a wide IP name.
The Modify Wide IP screen opens.
3. On the toolbar, click **Port List**.
The Wide IP Port List screen opens.
4. Type a port number in the box or select a service from the list, then click the right arrow button.
5. Repeat step 4 for each port or service you need to add.
6. Click **Update**.

To configure multiple ports for a wide IP from the command line

1. At the command prompt, type **3dnsmaint** to open the 3-DNS Maintenance menu.
2. On the 3-DNS Maintenance menu, select **Edit 3-DNS Configuration** to open the **wideip.conf** file.
3. Locate the **wideip** statement you want to edit.
4. Add the **port_list** line as indicated in bold in Figure 7.7.

```
wideip {
  address <ip_addr>
  port <port_number> | <"service name">
  name <"domain_name">
  [ alias <"alias_name"> ]
  [ ttl <number> ]
  [ port_list <port_number> <port_number> ... ]
  [ qos_coeff {
    rtt <n>
    completion_rate <n>
    packet_rate <n>
    topology <n>
    hops <n>
    vs_capacity <n>
    kbps <n>
  } ]
  [ pool_lbmode <rr | ratio | ga | random | topology> ]
  [ pool definitions ...]
```

*Figure 7.7 Enabling multiple ports with the **port_list** option*

Ensuring availability for e-commerce, FTP, and other services that use multiple ports

Before the 3-DNS Controller selects a virtual server to receive a connection, it verifies that the virtual server is up and available. Certain types of network traffic, such as FTP traffic or e-commerce traffic, require that more than one port be available in order for the client's requests to be properly handled. For example, FTP servers use both ports 20 and 21, while e-commerce sites typically require that both ports 80 and 443 are available to handle HTTP and SSL traffic.

When you set up a load balancing configuration, you can define a port list for a wide IP. When the 3-DNS Controller receives a query, all of the ports in the port list must be available for each virtual server in the wide IP. If a

virtual server does not have all ports in the port list available, the 3-DNS Controller marks it as unavailable for load balancing. In this example, you are setting up a site for selling a product on the Internet. This site contains a non-secure area that contains the product catalog, and a secure area for placing orders. You can configure a wide IP so that clients are sent to a virtual server only when both the secure and non-secure ports are available.

The key entry for this configuration is **port_list**. The **port_list** entry specifies that requests can be sent to virtual servers in this pool only if ports 80 (non-secure area) and 443 (secure area) are available.

```
wideip {
  address      192.168.101.70
  port         80 // http
  port_list    80 443 // e-commerce
  name         "ssl.wip.domain.com"
  pool_lbmode  rr
  pool {
    name       "bigip_pool"
    ratio      2
    preferred  qos
    alternate  ratio
    address    192.168.101.70  ratio 7
    address    192.168.102.60  ratio 2
  }
  pool {
    name       "host_pool"
    ratio      1
    preferred  ratio
    address    192.168.104.50  ratio 2
    address    192.168.105.60  ratio 1
  }
}
```

Figure 7.8 Syntax for e-commerce services

For every virtual server address in the pool, a virtual server definition must exist for each port in the port list.

For the syntax example shown in Figure 7.8, the BIG-IP Controllers and host machines must have the following virtual servers defined:

```
192.168.101.70:80
192.168.101.70:443
192.168.102.60:80
192.168.102.60:443
192.168.104.50:80
192.168.104.50:443
192.168.105.60:80
192.168.105.60:443
```



Glossary

3-DNS Distributed Traffic Controller

The 3-DNS Distributed Traffic Controller is a wide area load distribution solution that intelligently allocates Internet and intranet service requests across geographically distributed network servers. The 3-DNS Distributed Traffic Controller is also called the 3-DNS Controller.

3-DNS Maintenance menu

The 3-DNS Maintenance menu is a command line utility that you use to configure the 3-DNS Controller.

3-DNS web server

The 3-DNS web server is a standard web server that hosts the Configuration utility on the 3-DNS Controller.

A record

The **A** record is the ADDRESS resource record that a 3-DNS Controller returns to a local DNS server in response to a name resolution request. The **A** record contains a variety of information, including one or more IP addresses that resolve to the requested domain name.

access control list (ACL)

An access control list is a list of local DNS server IP addresses that are excluded from path probing, hops, or port discovery queries.

active unit

In a redundant system, an active unit is a controller that currently load balances name resolution requests. If the active unit in the redundant system fails, the standby unit assumes control and begins to load balance requests.

alternate method

The alternate method specifies the load balancing mode that the 3-DNS Controller uses to pick a virtual server if the preferred method fails. See also *fallback method*, *preferred method*.

big3d agent

The **big3d** agent is a monitoring agent that collects metrics information about server performance and network paths between a data center and a specific local DNS server. The 3-DNS Controller uses the information collected by the **big3d** agent for dynamic load balancing.

BIND (Berkeley Internet Name Domain)

BIND is the most common implementation of the Domain Name System (DNS). BIND provides a system for matching domain names to IP addresses. For more information, refer to <http://www.isc.org/products/BIND>.

CNAME record

A canonical name (CNAME) record acts as an alias to another domain name. A canonical name and its alias can belong to different zones so the **CNAME** record must always be entered as a fully qualified domain name. **CNAME** records are useful for setting up logical names for network services so that they can be easily relocated to different physical hosts.

completion rate

The completion rate is the percentage of packets that a server successfully returns during a given session.

Completion Rate mode

The Completion Rate mode is a dynamic load balancing mode that distributes connections based on which network path drops the fewest packets, or allows the fewest number of packets to time out.

Configuration utility

The Configuration utility is the browser-based application that you use to configure the 3-DNS Controller.

content delivery network (CDN)

A content delivery network (CDN) is an architecture of Web-based network components that helps dramatically reduce the wide-area network latency between a client and the content they wish to access. A CDN includes some or all of the following network components: wide-area traffic managers, Internet service providers, content server clusters, caches, and origin content providers.

CDN switching

CDN switching is the functionality of the 3-DNS Controller that allows a user to redirect traffic to a third-party network, or transparently switch traffic to a CDN. The two features of the 3-DNS Controller that make CDN switching possible are geographic redirection and the pool type CDN.

data center

A data center is a physical location that houses one or more 3-DNS Controllers, BIG-IP Controllers, EDGE-FX Caches, GLOBAL-SITE Controllers, or host machines.

data center server

A data center server is any server recognized in the 3-DNS Controller configuration. A data center server can be any of the following: a 3-DNS Controller, a BIG-IP Controller, an EDGE-FX Cache, a GLOBAL-SITE Controller, or a host.

discovery factory

A discovery factory is a tool managed by the **big3d** agent that checks for alternate ports to ping when trying to collect path data for a local DNS server.

domain name

A domain name is a unique name that is associated with one or more IP addresses. Domain names are used in URLs to identify particular Web pages. For example, in the URL **http://www.f5.com/index.html**, the domain name is **f5.com**.

dynamic load balancing modes

Dynamic load balancing modes base the distribution of name resolution requests to virtual servers on live data, such as current server performance and current connection load.

dynamic site content

Dynamic site content is a type of site content that is automatically generated each time a user accesses the site. Examples are current stock quotes or weather satellite images.

Extended Content Verification (ECV)

On the 3-DNS Controller, ECV is a service monitor that checks the availability of actual content, (such as a file or an image) on a server, rather than just checking the availability of a port or service, such as HTTP on port 80.

external interface

An external interface is the network interface that can be accessed across a wide-area network (WAN). See also *internal interface*.

fail-over

Fail-over is the process whereby a standby unit in a redundant system takes over when a software failure or hardware failure is detected on the active unit.

fail-over cable

The fail-over cable is the cable that directly connects the two controller units in a hardware-based redundant system.

fallback method

The fallback method is the third method in a load balancing hierarchy that the 3-DNS Controller uses to load balance a resolution request. The 3-DNS Controller uses the fallback method only when the load balancing modes specified for the preferred and alternate methods fail. Unlike the preferred method and the alternate method, the fallback method uses neither server nor virtual server availability for load balancing calculations. See also *preferred method*, *alternate method*.

FDDI (Fiber Distributed Data Interface)

FDDI is a multi-mode protocol for transmitting data on optical-fiber cables at speeds up to 100 Mbps.

First-Time Boot utility

The First-Time Boot utility is a utility that takes you through the initial system configuration process. The First-Time Boot utility runs automatically when you turn on a controller for the first time.

Global Availability mode

Global Availability is a static load balancing mode that bases connection distribution on a particular server order, always sending a connection to the first available server in the list. This mode differs from Round Robin mode in that it searches for an available server always starting with the first server in the list, while Round Robin mode searches for an available server starting with the next server in the list (with respect to the server selected for the previous connection request).

hops factory

A hops factory is a type of factory run by the **big3d** agent that collects hops data about network paths.

host

A host is a network server that manages one or more virtual servers that the 3-DNS Controller uses for load balancing.

ICMP (Internet Control Message Protocol)

ICMP is an Internet communications protocol used to determine information about routes to destination addresses, such as virtual servers managed by BIG-IP Controllers and 3-DNS Controllers.

internal interface

An internal interface is a network interface that can be accessed from a local-area network (LAN). See also *external interface*.

iQuery

The iQuery protocol is used to exchange information between 3-DNS Controllers, BIG-IP Controllers, EDGE-FX Caches, and GLOBAL-SITE Controllers. The iQuery protocol is officially registered with IANA for port 4353, and works on UDP and TCP connections.

Kilobytes/Second mode

The Kilobytes/Second mode is a dynamic load balancing mode that distributes connections based on which available server currently processes the fewest kilobytes per second.

Least Connections mode

The Least Connections mode is a dynamic load balancing mode that bases connection distribution on which server currently manages the fewest open connections.

load balancing methods

Load balancing methods are the settings that specify the hierarchical order in which the 3-DNS Controller uses three load balancing modes. The preferred method specifies the first load balancing mode that the 3-DNS Controller tries, the alternate method specifies the next load balancing mode to try if the preferred method fails, and the fallback method specifies the last load balancing mode to use if both the preferred and the alternate methods fail.

load balancing mode

A load balancing mode is the way in which the 3-DNS Controller determines how to distribute connections across an array.

local DNS

A local DNS is a server that makes name resolution requests on behalf of a client. With respect to the 3-DNS Controller, local DNS servers are the source of name resolution requests. Also referred to as LDNS.

metrics information

Metrics information is the data that is typically collected about the paths between BIG-IP Controllers, EDGE-FX Caches or GLOBAL-SITE Controllers, and local DNS servers. Metrics information is also collected about the performance and availability of virtual servers. Metrics information is used for load balancing, and it can include statistics such as round trip time, packet rate, and packet loss.

MindTerm SSH

MindTerm SSH is the third-party application on 3-DNS Controllers that uses SSH for secure remote communications. SSH encrypts all network traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks. SSH also provides secure tunneling capabilities and a variety of authentication methods.

name resolution

Name resolution is the process by which a name server matches a domain name request to an IP address, and sends the information to the client requesting the resolution.

name server

A name server is a server that maintains a DNS database, and resolves domain name requests to IP addresses using that database.

named

The **named** daemon manages domain name server software.

NameSurfer

NameSurfer is the third-party application on 3-DNS Controllers that automatically manages DNS zone files, synchronizing them with the configuration on the controller. NameSurfer automatically updates any configuration changes that you make using the Configuration utility. NameSurfer also provides a graphical user interface for DNS zone file management.

Network Time Protocol (NTP)

Network Time Protocol functions over the Internet to synchronize system clocks to Universal Coordinated Time. NTP provides a mechanism to set and maintain clock synchronization within milliseconds.

NS record

A name server (NS) record is used to define a set of authoritative name servers for a DNS zone. A name server is considered authoritative for some given zone when it has a complete set of data for the zone, allowing it to answer queries about the zone on its own, without needing to consult another name server.

packet rate

The packet rate is the number of data packets per second processed by a server.

Packet Rate mode

The Packet Rate mode is a dynamic load balancing mode that distributes connections based on which available server currently processes the fewest packets per second.

path

A path is a logical network route between a data center server and a local DNS server.

path probing

Path probing is the collection of metrics data, such as round trip time and packet rate, for a given path between a requesting LDNS server and a data center server.

persistence

On a 3-DNS Controller, persistence is a series of related requests received from the same local DNS server for the same wide IP name. When persistence is turned on, a 3-DNS Controller sends all requests from a particular local DNS server for a specific wide IP to the same virtual server, instead of load balancing the requests.

picks

Picks represent the number of times a particular virtual server is selected to receive a load balanced connection.

pool

A pool is a group of virtual servers managed by a BIG-IP Controller, an EDGE-FX Cache, or a host. The 3-DNS Controller load balances among pools (using the Pool LB Mode), as well as among individual virtual servers.

pool ratio

A pool ratio is a ratio weight applied to pools in a wide IP. If the Pool LB mode is set to Ratio, the 3-DNS Controller uses each pool for load balancing in proportion to the weight defined for the pool.

preferred method

The preferred method specifies the first load balancing mode that the 3-DNS Controller uses to load balance a resolution request. See also *alternate method*, *fallback method*.

principal 3-DNS Controller

A 3-DNS Controller that initiates metrics collection by the **big3d** agents and distributes the metrics to other members of a sync group. See also *receiver 3-DNS Controller*.

production rule

A production rule, on the 3-DNS Controller, can change system behavior under specific operating conditions. For example, a production rule can switch load balancing modes or can reroute network traffic to a specific set of servers. Production rules are based on triggers such as time of day or current network traffic load.

probe protocol

The probe protocol is the specific protocol used to probe a given path and collect metrics information for the path. The probe protocols available on the 3-DNS Controller are: ICMP, DNS_REV, DNS_DOT, UDP, and TCP. The probe protocols that are available change based on the data center server type.

prober

A prober is a specific thread of the **big3d** agent that is used for path probing of a given set of paths.

prober factory

A prober factory is a utility that collects metrics data, such as round trip time and packet rate, for a given path between a requesting LDNS and a data center server. Prober factories are managed by the **big3d** agent, which reports the path probing metrics to the 3-DNS Controller. Prober factories can run on BIG-IP Controllers, EDGE-FX Caches, and GLOBAL-SITE Controllers.

Quality of Service load balancing mode

The Quality of Service load balancing mode is a dynamic load balancing mode that bases connection distribution on a configurable combination of the packet rate, completion rate, round trip time, hops, virtual server capacity, kilobytes per second, and topology information.

QOS equation

The QOS equation is the equation on which the Quality of Service load balancing mode is based. The equation calculates a score for a given path between a data center server and a local DNS server. The Quality of Service mode distributes connections based on the best path score for an available data center server. You can apply weights to the factors in the equation, such as round trip time and completion rate.

ratio

A ratio is the parameter in a virtual server statement that assigns a weight to the virtual server for load balancing purposes.

Ratio mode

The Ratio load balancing mode is a static load balancing mode that distributes connections across an pool of virtual servers in proportion to the ratio weight assigned to each individual virtual server.

receiver 3-DNS Controller

A receiver 3-DNS Controller is a controller, in a sync group, that receives metrics data that are broadcast from **big3d** agents, but does not initiate metrics collection. See also *principal 3-DNS Controller*.

redundant system

A redundant system is a pair of controllers that are configured for fail-over. In a redundant system, one controller runs as the active unit and the other controller runs as the standby unit. If the active unit fails, the standby unit takes over and manages resolution requests.

remote administrative IP address

A remote administrative IP address is an IP address from which a controller allows shell connections, such as SSH, RSH, or Telnet.

resolver

The resolver is the client part of the Domain Name System. The resolver translates a program's request for host name information into a query to a name server, and translates the response into an answer to the program's request. See also *name server*.

resource record

resource record is a record in a DNS database that stores data associated with domain names. A resource record typically includes a domain name, a TTL, a record type, and data specific to that record type. See also *A record*, *CNAME record*, *NS record*.

reverse domains

A type of DNS resolution request that matches a given IP address to a domain name. The more common type of DNS resolution request starts with a given domain name and matches that to an IP address.

root name server

A root name server is a master DNS server that maintains a complete DNS database. There are approximately 13 root name servers in the world that manage the DNS database for the World Wide Web.

Round Robin mode

Round Robin mode is a static load balancing mode that bases connection distribution on a set server order. Round Robin mode sends a connection request to the next available server in the order.

round trip time (RTT)

Round trip time is the calculation of the time (in microseconds) that a local DNS server takes to respond to a ping issued by the **big3d** agent running on a data center server. The 3-DNS Controller takes RTT values into account when it uses dynamic load balancing modes.

Round Trip Time mode

Round Trip Time is a dynamic load balancing mode that bases connection distribution on which virtual server has the fastest measured round trip time between the data center server and the local DNS server.

secondary DNS

The secondary DNS is a name server that retrieves DNS data from the name server that is authoritative for the DNS zone.

site content

Site content is data (including text, images, audio, and video feeds) that is accessible to clients who connect to a given site. See also *dynamic site content*, *static site content*.

SNMP (Simple Network Management Protocol)

SNMP is the Internet standard protocol, defined in STD 15, RFC 1157, that was developed to manage nodes on an IP network.

sod (switch over daemon)

The **sod** daemon controls the fail-over process in a redundant system.

SSH

SSH is a protocol for secure remote login and other secure network services over a non-secure network.

standby unit

A standby unit is a controller in a redundant system that is always prepared to become the active unit if the active unit fails.

static load balancing modes

Static load balancing modes base the distribution of name resolution requests to virtual servers on a pre-defined list of criteria and server and virtual server availability; they do not take current server performance or current connection load into account.

static site content

Static site content is a type of site content that is stored in HTML pages, and changes only when an administrator edits the HTML document itself.

subdomain

A subdomain is a sub-section of a higher level domain. For example, **.com** is a high level domain, and **F5.com** is a subdomain within the **.com** domain.

sub-statement

A sub-statement is a logical section within a statement that defines a particular element in the statement. A sub-statement begins with the sub-statement name followed by an open brace ({) and ends with a closed brace (}). Everything between those braces is part of the sub-statement. Sub-statements typically define a group of related variables, such as the calculation coefficients used in Quality of Service load balancing.

sync group

A sync group is a group of 3-DNS Controllers that share system configurations and path metrics for data center servers and virtual servers. Sync groups have one principal 3-DNS Controller, and may contain one or

more receiver controllers. The receiver controllers obtain their configuration information from the principal controller. See also *principal 3-DNS Controller*, *receiver 3-DNS Controller*.

time tolerance value

The time tolerance value is the number of seconds that one 3-DNS Controller's clock is allowed to differ in comparison to another 3-DNS Controller's clock, without the two clocks being considered out of sync.

Topology mode

The Topology mode is a static load balancing mode that bases the distribution of name resolution requests on the weighted scores for topology records. Topology records are used by the Topology load balancing mode to redirect DNS queries to the closest virtual server, geographically, based on location information derived from the DNS query message.

topology record

A topology record specifies a score for a local DNS server location endpoint and a virtual server location endpoint.

topology score

The topology score is the weight assigned to a topology record when the 3-DNS Controller is filtering the topology records to find the best virtual server match for a DNS query.

topology statement

A topology statement is a collection of topology records.

traceroute

Traceroute is the utility that the hops factory uses to calculate the total number of network hops between a local DNS server and a specific data center.

TTL (Time to Live)

The TTL is the number of seconds for which a specific DNS record or metric is considered to be valid. When a TTL expires, the server usually must refresh the information before using it again.

unavailable

The **unavailable** is a status used for data center servers and virtual servers. When a data center server or virtual server is **unavailable**, the 3-DNS Controller does not use it for load balancing.

unknown

The **unknown** status is used for data center servers and virtual servers. When a data center server or virtual server is new to the 3-DNS Controller and does not yet have metrics information, the 3-DNS Controller marks its status as **unknown**. The 3-DNS Controller can use unknown servers for load balancing, but if the load balancing mode is dynamic, the 3-DNS Controller uses default metrics information for the unknown server until it receives live metrics data.

up

The **up** status is used for data center servers and virtual servers. When a data center server or virtual server is **up**, the data center server or virtual server is available to respond to name resolution requests.

virtual server

A virtual server is a specific combination of a virtual IP address and virtual port, and is associated with a content site that is managed by a BIG-IP Controller, EDGE-FX Cache, or host server.

watchdog timer card

The watchdog timer card is a hardware device that monitors the 3-DNS Controller for hardware failure.

wide IP

A wide IP is a collection of one or more domain names that maps to one or more groups of virtual servers managed either by BIG-IP Controllers, EDGE-FX Caches, or by host servers. The 3-DNS Controller load balances name resolution requests across the virtual servers that are defined in the wide IP that is associated with the requested domain name.

WKS (well-known services)

Well-known services are protocols on ports 0 through 1023 that are widely used for certain types of data. Some examples of some well-known services (and their corresponding ports) are: HTTP (port 80), HTTPS (port 443), and FTP (port 20).

WKS record

A WKS record is a DNS resource record that describes the services usually provided by a particular protocol on a specific port.

zone

In DNS terms, a zone is a subset of DNS records for one or more domains.

zone file

In DNS terms, a zone file is a database set of domains with one or many domain names, designated mail servers, a list of other name servers that can answer resolution requests, and a set of zone attributes, which are contained in an SOA record.



Index

3-DNS Maintenance menu
 about 1-2, 6-1
 changing passwords 6-10
 using 6-3
 working with commands 6-2
 3-DNS web server. See Configuration Utility
 3dns_add script
 about 5-1
 and sync groups 5-1
 running the script 5-3
 verifying the configuration 5-3
 3dns_sync_metrics script 6-6
 3dnsmaint command. See 3-DNS Maintenance menu
 3dprint script 6-3

A

A records 1-11
 additional controllers
 configuring 5-1
 Administrator Kit, PDF versions 1-5
 Ask F5 knowledge base 1-5
 authoritative DNS
 configuring 3-DNS Controller 2-7, 2-9
 configuring NameSurfer 2-10

B

basic configuration
 adding 3-DNS Controllers 2-15
 adding data centers 2-12
 adding EDGE-FX Caches 2-22
 adding GLOBAL-SITE Controllers 2-20
 adding hosts 2-24
 configuring global variables 2-31
 creating a sync group 2-29
 setting up 2-11
 big3d agent
 about 1-7
 broadcasting 1-9
 configuring 2-5
 restarting 6-6
 sample configuration 1-9
 updating 6-5
 working with 6-5
 big3d_install script 6-6
 big3d_restart script, 6-6

BIG-IP Controller
 connection management 1-14
 defining 2-17
 updating big3d agent 6-5
 verifying big3d versions 6-5
 BIND files
 transferring to NameSurfer 2-8
 browsers, supported versions 1-2

C

CDN
 configuration example 4-2
 configuring 4-4
 delegating DNS queries 4-2
 described 4-1
 managing with 3-DNS Controller 4-1
 using pool type CDN 4-1
 using topology load balancing 4-1
 CDN configuration
 adding 3-DNS Controllers 4-5
 adding a topology statement 4-8
 adding data centers 4-4
 adding pool type CDN 4-7
 adding servers 4-6
 adding wide IPs and pools 4-6
 monitoring 4-9
 using a last resort pool 4-9
 CDN providers
 described 4-1
 resolving DNS queries 4-3
 CDN switching 4-1
 Change/Add Users for 3-DNS Configuration Utility
 command 6-7
 Check big3d versions command 6-5
 command line utility. See 3-DNS Maintenance menu
 command syntax, conventions 1-4
 commands
 Change/Add Users for 3-DNS Configuration
 Utility 6-7
 Check remote versions of big3d 6-5
 Configure Connection to NTP Time Server 6-8
 Configure NameSurfer 6-9
 Configure SSH communication with
 remote devices 6-6
 Dump 3dnssd Statistics 6-3
 Edit 3-DNS Configuration 6-3
 Edit big3d matrix 6-5
 Edit BIND Configuration 6-3
 Generate and Copy iQuery Encryption key 6-7
 Install and Start big3d 6-6
 Reconfigure 3-DNS Configuration Utility 6-7

- Restart 3-DNS Configuration Utility 6-7
- Restart big3d command 6-6
- Restart syncd 6-8
- Stop syncd 6-8
- Synchronize Metrics Data 6-6
- config_ssh script 6-6
- configuration planning 2-1
- configuration tools, choosing 1-1
- Configuration utility
 - about 1-2
 - adding users 6-7, 6-10
 - and supported browser versions 1-2
 - changing passwords 6-7, 6-10
 - configuring 3-DNS web server 6-7
 - creating new password file 6-11
 - updating users 6-7
 - viewing statistics 6-13
- configurations, verifying 5-3
- Configure Connection to NTP Time Server command 6-8
- Configure NameSurfer command 6-9
- Configure SSH communication with remote devices command 6-6
- content delivery network. See CDN

D

- data center servers
 - in the network configuration 2-2
- data centers
 - about 2-1
 - adding a 3-DNS Controller 5-1
 - configuring 2-12
- DNS
 - master servers 1-11
 - root servers 1-12
- DNS queries
 - delegating to CDN providers 4-2
- DNS servers
 - replacing with 3-DNS Controllers 2-7
- DNS zone files. See zone files
- documentation 1-5
- domain names, maximum supported 1-7
- Dump 3dnscd Statistics command 6-3
- Dynamic Ratio
 - about 7-5
 - configuring 7-6
 - using with QOS mode 7-5

E

- e-commerce site
 - configuring 7-10
 - configuring wide IPs 7-11
- EDGE-FX Cache
 - configuring 2-22
 - updating big3d agent 6-5
 - verifying big3d versions 6-5
- Edit 3-DNS Configuration command 6-3
- Edit big3d matrix command 6-5
- Edit BIND Configuration command 6-3
- encryption
 - and crypto 3-DNS Controllers 2-31
 - and global variables 2-31
 - and SSH communications 6-7
 - enabling 2-31

F

- F5 Networks, technical support 1-5
- fail-over
 - hardware-based 1-8
 - network-based 1-8
- features of 3-DNS Controller 1-6
- First-Time Boot utility 1-1
- FTP, configuring wide IPs 7-11

G

- Generate and Copy iQuery Encryption key command 6-7
- Global Availability mode
 - about 7-7
 - configuring 7-8
 - configuring standby data centers 7-9
- global variables
 - configuring 2-31
 - enabling encryption 2-31
- globally-distributed network
 - adding 3-DNS Controllers 3-3
 - adding BIG-IP Controllers 3-4
 - adding data centers 3-2
 - configuring 3-2
 - using Topology load balancing 3-2
- GLOBAL-SITE Controller
 - configuring 2-20
 - updating big3d agent 6-5
 - verifying big3d versions 6-5

H

- hardware-based fail-over 1-8
- help, online 1-5
- high availability 7-11
- hosts
 - and probes 2-24, 2-27
 - and supported SNMP agents 2-27
 - configuring 2-24
 - viewing statistics 2-28

I

- Install and Start big3d command 6-6
- Internet protocols 1-6
- IP addresses
 - and NameSurfer 1-2
- iQuery protocol
 - about 1-6
 - and NTP 6-8

K

- knowledge base, Ask F5 1-5

L

- last resort pool
 - using in a CDN configuration 4-9
- limits settings
 - modifying thresholds 3-7
- load balancing modes
 - Global Availability 7-8
 - Quality of Service 7-1
 - Topology 3-1
- load balancing, using pools 1-13

M

- media options 1-7
- metrics
 - and hosts 2-27
 - collecting from hosts 2-27
- metrics data
 - synchronizing new controllers 6-6
- metrics data, copying 6-6
- Microsoft Internet Explorer 1-2
- MindTerm SSH Console
 - about 6-11
 - using 6-11
- multiple services
 - configuring 7-10
 - configuring ports 7-11

N

- name resolution 1-11, 1-12
- NameSurfer
 - about 1-2
 - and 3-DNS Maintenance menu 6-1
 - configuring 6-9
 - configuring as authoritative 2-10
 - managing DNS zone files 2-7
 - maximum supported IP addresses 1-2
 - transferring BIND files 2-8
- Netscape Navigator 1-2
- network configuration
 - configuring rsh 2-4
 - configuring ssh 2-4
- network management tools 1-6
- Network Map
 - about 6-12
 - viewing 6-12
- network time protocol. See NTP
- network-based fail-over 1-8
- nslookup 5-5
- NTP
 - and iQuery protocol 6-8
 - synchronizing 3-DNS Controllers 6-8
 - synchronizing time 6-8

O

- online help 1-5

P

- passwords, changing 6-9
- PDF versions, Administrator Kit 1-5
- pools 1-13
- port list
 - configuring 7-10
- principal 3-DNS Controller 1-10
 - about 2-29
 - adding another controller 5-2
 - planning sync groups 2-3
- probers
 - and hosts 2-24, 2-27
- production rules 2-6

Q

- QOS coefficients
 - about 7-2
 - and wide IPs 7-4
 - configuring 7-3
 - considerations 7-2

- QOS equation
 - modifying 7-3
 - syntax 7-4
- Quality of Service mode
 - about 7-1
 - and default settings 7-1
 - understanding QOS coefficients 7-2
 - using Dynamic Ratio 7-5
- R**
- receiver 3-DNS Controller
 - about 2-29
 - planning sync groups 2-3
- Reconfigure 3-DNS Configuration Utility command 6-7
- redundant systems 1-8
- release notes 1-5
- remote administration 2-2, 6-7
- resource thresholds
 - setting limits 3-7
- Restart 3-DNS Configuration Utility command 6-7
- Restart big3d command 6-6
- Restart syncd command 6-8
- rsh utilities 2-4
- S**
- sample 3-DNS Controller configuration 1-9
- sample configuration
 - big3d agent communications 1-9
- scalability 1-7
- security features 1-6
- server performance
 - monitoring 3-8
- servers
 - defining 2-2
 - defining 3-DNS Controllers 2-15
 - defining additional 3-DNS Controllers 5-1
 - defining BIG-IP Controllers 2-17
 - defining in the configuration 2-15
 - See also data center servers
- SMTP 1-6
- SNMP 1-6
 - and host prober 2-27
 - host prober 2-24
- SNMP agents
 - and supported hosts 2-27
- SNMP MIB 1-2
- SSH
 - and remote administration 6-7
 - configuring 6-6
 - MindTerm SSH console 1-6
- ssh utilities 2-4
- SSL 1-7
- Statistics screens
 - described 6-13
 - in Configuration utility 6-14
 - viewing 6-13
- statistics, viewing in 3-DNS Maintenance menu 6-3
- Stop syncd command 6-8
- stylistic conventions 1-3
- sub-domains 2-6
- sync group
 - about 1-7, 2-3
 - and 3dns_add script 5-1
 - and time tolerance variable 2-3
 - and zone files 2-7
 - broadcasting configurations 2-1
 - configuring 2-29
 - defined 2-3
 - planning 2-2
 - planning configurations 2-3
 - sample configuration 1-10
- sync groups
 - and additional controllers 5-1
- syncd
 - stopping or restarting 6-8
 - working with 6-8
- syncd_start script 6-8
- syncd_stop script 6-8
- Synchronize Metrics Data command 6-6
- synchronized files
 - and time tolerance variable 2-3
 - and zone files 2-7
 - archiving 6-6
 - copying metrics 6-6
 - using syncd 6-8
- system resources
 - about 3-7
 - setting limits 3-7
- T**
- Technical Support web site 1-5
- time synchronization 6-8
- time tolerance variable 2-30
 - about 2-3
 - and sync groups 2-3
- Topology load balancing
 - about 2-6
 - using in a CDN 4-8
 - using in a global network 3-2
- topology records
 - configuring 3-6

topology statement
 configuring topology records 3-6
 using in a CDN 4-8

U

user administration
 adding users 6-10
 changing user settings 6-10
 configuring 6-7
 setting access levels 6-10

utilities

 3-DNS Maintenance menu 1-2
 Configuration 1-2
 First-Time Boot 1-1

V

view statistics 6-3

virtual servers

 availability settings 3-8
 defining 2-2

W

web server. See Configuration utility

wide IP sub-domains 2-7, 2-9

wide IPs

 and DNS zone files 2-7
 and QOS coefficients 7-4
 configuring 6-3
 verifying configuration 5-5

wideip.conf file

 editing 6-3

Z

zone file management

 using NameSurfer 1-2

zone files

 and 3-DNS Maintenance menu 6-1
 configuring 6-3
 managing 6-9
 managing with NameSurfer 6-9
 planning management of 2-6
 synchronizing 3-DNS Controllers 2-7
 transferring to 3-DNS 2-7