3-DNS Administrator Guide

version 4.2

MAN-0046-01

Product Version

This manual applies to version 4.2 of 3-DNS®.

Legal Notices

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

1
Introduction

2
Planning the 3-DNS Configuration

3
Setting Up the Hardware

4
Working with the Setup Utility

5
Configuring the Base Network

6
Essential Configuration Tasks

7
Configuring a Globally-Distributed Network

8
Configuring a Content Delivery Network

9
Working with Quality of Service

1

Introduction

- Getting started
- Using the Administrator Kit
- What is the 3-DNS?
- What's new in version 4.2
- Finding help and technical support resources

Getting started

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

- **Planning the 3-DNS Configuration**
  This chapter describes the network and configuration planning you need to do before you install the 3-DNS in your network.
- **Setting Up the Hardware**
  This chapter describes the physical installation of the 3-DNS system.
- **Working with the Setup Utility**
  This chapter describes the Setup utility and its functions. The Setup utility runs automatically the first time you turn on the 3-DNS.
- **Configuring the Base Network**
  This chapter describes the base network, which includes the IP addresses, VLANs, and network interfaces on the 3-DNS.
- **Essential Configuration Tasks**
  This chapter describes the software configuration 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.
- **Working with Quality of Service**
  This chapter describes the components of the Quality of Service load balancing mode.
- **Working with Global Availability Load Balancing**
  This chapter describes the components of the Global Availability load balancing mode.
- **Adding a 3-DNS to an Existing Network**
  This chapter describes the tasks you complete to configure an additional 3-DNS in a network that already contains one or more 3-DNS systems.
- **Administration and Monitoring**
  This chapter describes the administrative tasks you complete for the 3-DNS, as well as the monitoring tools that are provided with the 3-DNS.

Choosing a configuration tool

The 3-DNS provides several web-based and command line administrative tools that make for easy setup and configuration. Use the following overview to help you decide when each utility is best used.

Setup utility

The Setup 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 to the network. The Setup 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. 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. You can use NameSurfer to configure and maintain additional DNS zone files on a 3-DNS that runs as a primary DNS server. 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 restarting the 3-DNS web server. You can use the 3-DNS Maintenance menu from a console connection, from a remote shell connection, or from the MindTerm SSH Console in the Configuration utility.

Browser support

The Configuration utility, which provides web-based access to the 3-DNS 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.

- **Configuration Worksheet**
  Use the Configuration Worksheet to gather the IP addresses, default routes, administrative account, and server information you need to configure the 3-DNS. The Setup utility prompts you for this information when you configure the 3-DNS for the first time.
- **Hardware poster**
  The hardware poster is a graphical representation of the physical components of the 3-DNS.
- **3-DNS Administrator Guide**
  The ***3-DNS Administrator Guide*** provides examples of common wide-area load balancing solutions supported by the 3-DNS. 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. The Administrator Guide also covers general network administration issues, such as installing the hardware and setting up the networking configuration.
- **3-DNS Reference Guide**
  The ***3-DNS Reference Guide*** provides basic descriptions of individual 3-DNS 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, use the **BIG-IP Reference Guide** and hardware poster 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 products

We refer to all products in the BIG-IP product family as the BIG-IP. We refer to the 3-DNS Controller and the 3-DNS module as the 3-DNS. If specific configuration information relates to a specific platform, we note the platform.

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***, Chapter 2, *3-DNS Maintenance Menu*.

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 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.

Table 1.1 *Command line conventions used in this manual*

Item in text	Description
[ ]	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*

What is the 3-DNS?

A 3-DNS is a network appliance that monitors the availability and performance of global resources, and uses that information to manage network traffic patterns. The 3-DNS uses load balancing algorithms, topology-based routing, and production rules to 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.

3-DNS 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
- Ensure wide-area persistence by maintaining a mapping between an local DNS server 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 systems, EDGE-FX Caches, and other load-balancing hosts
- Monitor real-time network conditions

Internet protocol and network management support

The 3-DNS supports both the standard DNS protocol and the 3-DNS iQuery protocol (a protocol used for collecting dynamic load balancing information). The 3-DNS 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 systems), RSH, Telnet, and FTP. The Configuration utility supports HTTPS, for secure web browser connections using SSL (distributed only on crypto 3-DNS systems), as well as standard HTTP connections.

The proprietary 3-DNS SNMP agent allows you to monitor status and current traffic flow using popular network management tools. The 3-DNS SNMP agent provides detailed data such as current connections being handled by each virtual server.

Security features

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

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

Configuration scalability

The 3-DNS is a highly scalable and versatile solution. You can configure the 3-DNS to manage up to several hundred domain names, including full support of domain name aliases. The 3-DNS supports a variety of media options, including Fast Ethernet, and Gigabit Ethernet; the 3-DNS 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 sync group feature allows you to automatically synchronize configurations from one 3-DNS to any other 3-DNS in the network, simplifying administrative management. The synchronization feature offers a high degree of administrative control. For example, you can set the 3-DNS to synchronize a specific configuration file set, and you can also set which 3-DNS systems 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 platform includes the **big3d** agent, which is an integral part of 3-DNS load balancing. The **big3d** agent continually monitors the availability of the servers that the 3-DNS 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 any of the following platforms: 3-DNS, BIG-IP, EDGE-FX Cache, and GLOBAL-SITE. Each **big3d** agent broadcasts its collected data to all of the 3-DNS systems in your network, ensuring that all 3-DNS systems 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 router 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 the ***3-DNS Reference Guide***, Chapter 4, *The big3d Agent*.

Redundant system configurations

A ***redundant system*** is essentially a pair of 3-DNS units, with one operating as the active unit that responds to DNS queries, and the other one operating as the standby unit. If the active unit fails, the standby unit takes over and begins to respond to DNS queries while the other 3-DNS restarts and becomes the standby unit.

The 3-DNS 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 unit checks on the status of the active unit once 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 unit checks on the status of the active unit once every second using the Ethernet.

Note

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

Monitoring the 3-DNS and the network

The 3-DNS includes sophisticated monitoring tools to help you monitor the 3-DNS, the traffic it manages, and the Internet. The following monitoring tools are available on the 3-DNS: the Statistics screens, the Internet Weather Map, and the Network Map. All of these tools are in the Configuration utility.

Comparing a 3-DNS to a BIG-IP

A 3-DNS load balances traffic for a globally-distributed network, and a BIG-IP load balances traffic for a local area network. While both systems provide load balancing, one of the significant differences between the BIG-IP and the 3-DNS is that the 3-DNS responds to DNS requests issued by an LDNS on behalf of a client, while the BIG-IP provides connection management between a client and a back-end server.

Once the 3-DNS returns a DNS answer to an LDNS, the conversation between the LDNS and the 3-DNS ends, and the client connects to the IP address returned by the 3-DNS. Unlike the 3-DNS, the BIG-IP sits between the client and the content servers. It manages the client's entire conversation with the content server.

What's new in version 4.2

The 3-DNS, version 4.2 offers the following major new features in addition to many other enhancements.

Custom regions for Topology

When you use the Topology load balancing mode, you can now configure user-defined regions. By specifying user-defined regions, you can customize the topology statement to best meet the traffic management needs of your customers and your network. For more information, refer to *Understanding user-defined regions*, in the ***3-DNS Reference Guide***, Chapter 13, *Topology*.

Router, bridge, and node modes

The 3-DNS can run in three modes: node, bridge, and router.

- In node mode, the 3-DNS runs as it always has - as an authoritative DNS for either a domain or sub-domain - in addition to managing global traffic. In node mode only, you can use the NameSurfer application to manage your DNS zone files.
- In bridge mode, the 3-DNS intercepts DNS packets, routes requests that map to wide IPs to the best virtual server, and forwards all other DNS packets to a DNS server in the same subnet.

- In router mode, the 3-DNS functions similarly to bridge mode, with the exception that the 3-DNS interacts with two or more IP subnets.

For more information, refer to *Choosing the 3-DNS mode*, on page 2-10, and *Configuring the 3-DNS mode*, on page 4-8.

Internet Weather Map

With the Internet Weather Map, you can monitor the health of the traffic between your data centers and users requesting your site. The Internet Weather Map is provides real-time data when you use path-based, or dynamic, load balancing methods, such as Round Trip Times and Completion Rate. For more information, refer to the ***3-DNS Reference Guide***, Chapter 7, *Internet Weather Map*.

ECV search string

You can now specify a regular expression text string that you want to verify as part of an extended content verification (ECV) monitor on a wide IP. For more information, refer to the ***3-DNS Reference Guide***, Chapter 6, *Extended Content Verification (ECV)*.

Setup utility

The 3-DNS now offers a menu-driven Setup utility for all setup activities such as defining the default route, assigning IP addresses to the interfaces, and configuring remote access and administrative accounts. Several options on the Setup utility incorporate the configuration steps of the First-Time Boot utility from previous releases. The Setup utility also replaces all **config_<option>** commands. For more information, refer to Chapter 4, *Working with the Setup Utility*.

Finding help and technical support resources

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

- **Release notes**
  Release notes for the 3-DNS are available from the home screen 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 features**
  You can find help online in three different locations:

- The Configuration utility home screen has PDF versions of the guides included in the Administrator Kit. The 3-DNS software upgrades replace the guides with updated versions as appropriate.
- The Configuration utility has online help for each screen. 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 **-h** or **-help**, and the 3-DNS displays the syntax and usage associated with the command. You can also type **man <command>** to display the man page for 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, including NameSurfer.

2

Planning the 3-DNS Configuration

- Managing traffic on a global network
- Planning issues for the network setup
- Choosing the 3-DNS mode
- Planning issues for the load balancing configuration
- Using advanced traffic control features

Managing traffic on a global network

The 3-DNS is a sophisticated wide-area traffic manager. With 3-DNS, you can load balance web site traffic and distributed applications. You can also monitor the health of your network. This section provides a brief overview of how the 3-DNS works within a global network, and how it interacts with any BIG-IP, EDGE-FX Cache, GLOBAL-SITE, or host in the network. The section also illustrates how the 3-DNS 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 systems that load balance connections for a sample Internet domain, **domain.com**.

Understanding a basic 3-DNS configuration

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

Figure 2.1 illustrates the layout of the 3-DNS, BIG-IP, and host servers in the three data centers. The Los Angeles data center houses one 3-DNS and one BIG-IP, as does the New York data center. The Tokyo data center houses only one 3-DNS and one host server.

In the Los Angeles and New York data centers, the **big3d** agent runs on the 3-DNS systems and the BIG-IP systems, but in the Tokyo data center, the **big3d** agent runs only on the 3-DNS. 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 systems running in each data center, as illustrated by the green, blue, and purple lines.

◆ Note

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

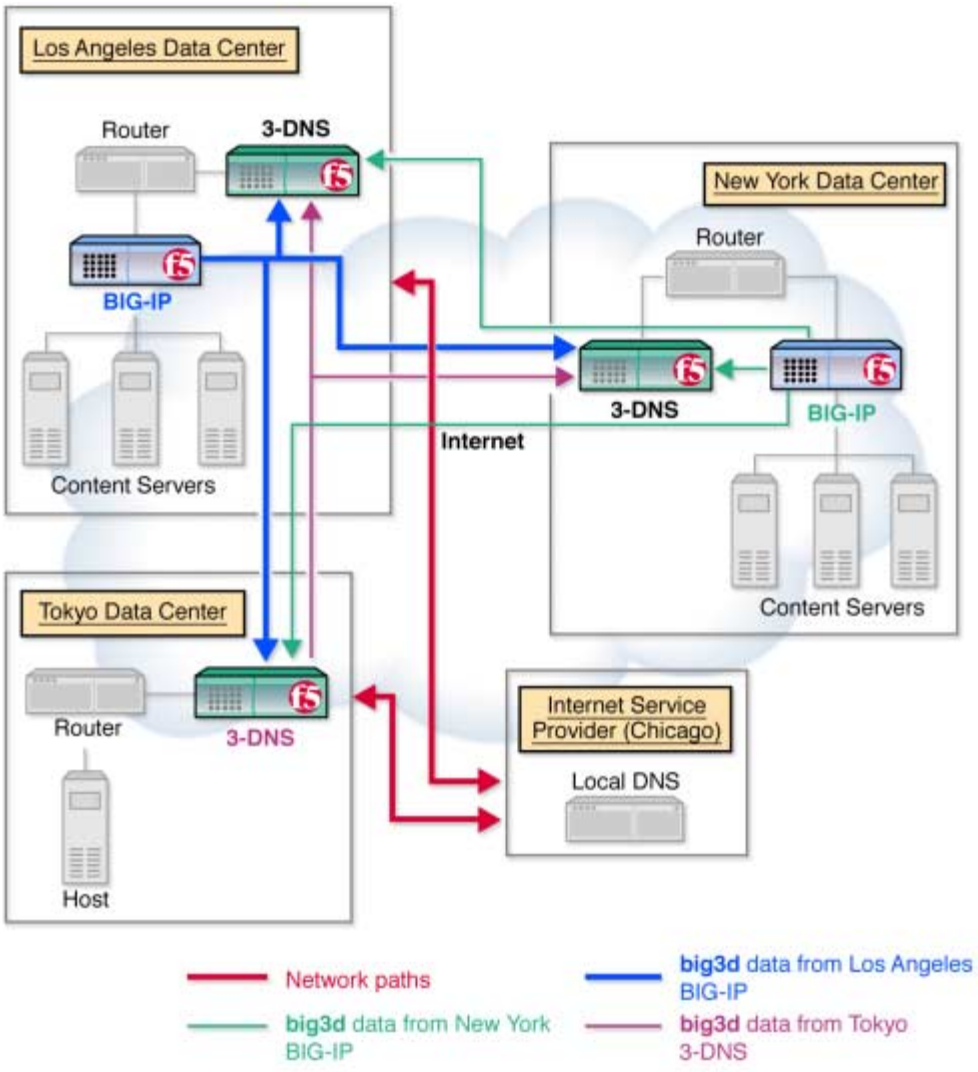

Figure 2.1 *A sample network layout showing data paths*

Synchronizing configurations and broadcasting performance metrics

3-DNS systems typically work in sync groups, where a group of systems shares load balancing configuration settings. In a sync group, any system that has new configuration changes can broadcast the changes to any other system in the sync group, allowing for easy administrative maintenance. To distribute metrics data among the systems in a sync group, the principal 3-DNS 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 systems in the network, again allowing for simple and reliable metrics distribution.

Using a 3-DNS as a standard DNS server

When a client requests a DNS resolution for a domain name, an LDNS sends the request to one of the 3-DNS systems that is authoritative for the zone. The 3-DNS 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.

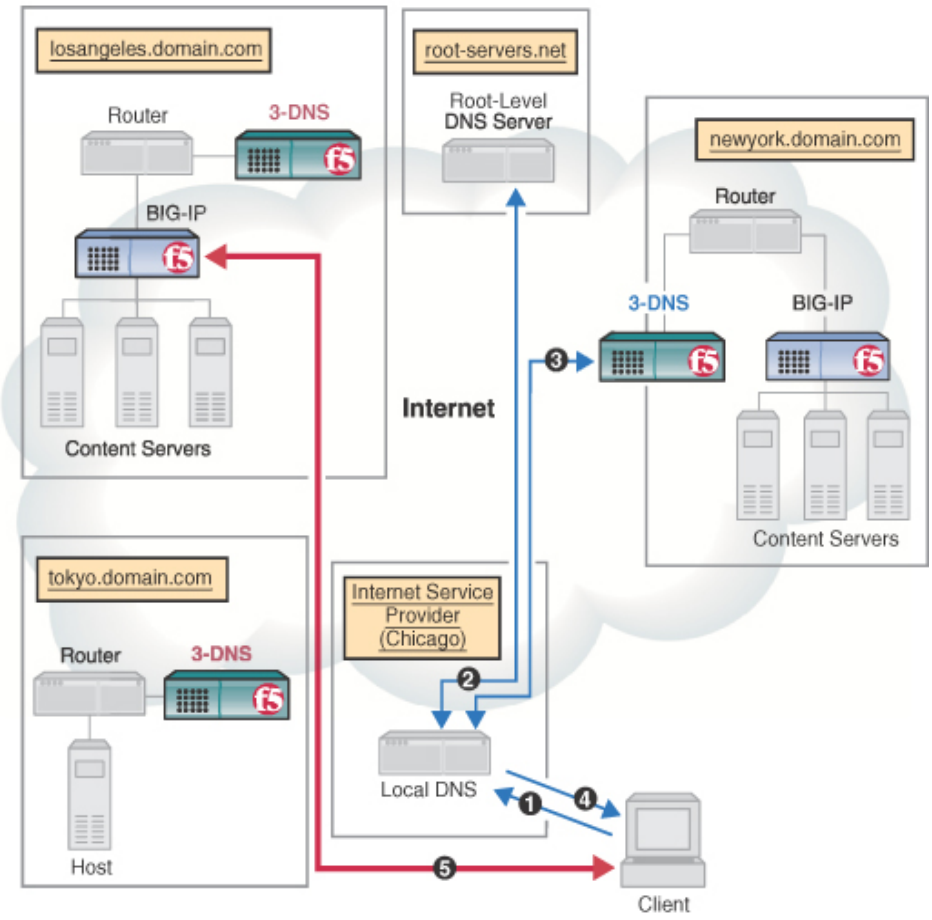

Figure 2.2 *DNS name resolution process*

Figure 2.2 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 the DNS systems associated with **www.domain.com**, which in this case runs on the 3-DNS.
3. The LDNS then connects to one of the 3-DNS systems to resolve the **www.domain.com** name. The 3-DNS 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 caches the answer from the 3-DNS, 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 load balancing modes can provide efficient load balancing for any network configuration. The 3-DNS bases load balancing on pools of virtual servers. When a client requests a DNS resolution, the 3-DNS 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 Chapter 8, *Load Balancing* in the ***3-DNS Reference Guide***. For more information on load balancing configurations, review the sample configurations in Chapter *7, Configuring a Globally-Distributed Network*, and Chapter 8, *Configuring a Content Delivery Network*. If you are unfamiliar with the 3-DNS, you may also want to review Chapter 6, *Essential Configuration Tasks*.

Working with 3-DNS systems and other products

The 3-DNS 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**
  A BIG-IP virtual server maps to a series of content servers.
- **EDGE-FX Cache**
  An EDGE-FX Cache virtual server maps to cached content that gets refreshed at frequent intervals.

- **Generic host**
  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 2.3 illustrates the hierarchy of how the 3-DNS manages virtual servers.

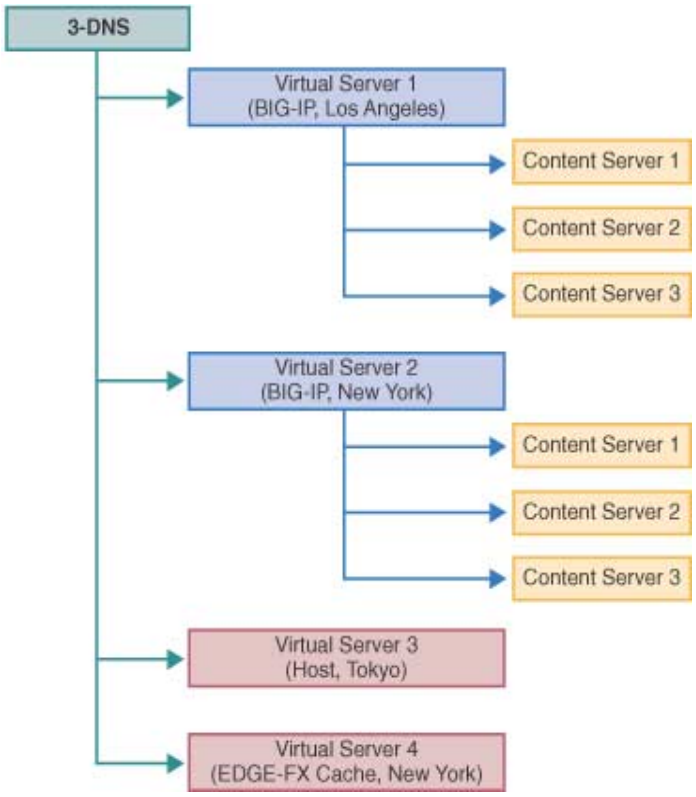

Figure 2.3 *Load balancing management on a 3-DNS*

Planning issues for the network setup

After you finish running the Setup utility, and connect each system to the network, you can set up the network and load balancing configuration on one 3-DNS, and let the sync group feature automatically broadcast the configuration to the other 3-DNS systems in the network. You do not have to configure the 3-DNS systems individually, unless you are planning an

advanced configuration that requires different configurations for different data centers, or you are configuring the 3-DNS systems from the command line.

Tip

If you are configuring additional 3-DNS systems in a network that already has a 3-DNS in it, please review Chapter 11, ***Adding a 3-DNS to an Existing Network****.*

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

- **Base network**
  The base network includes the interfaces, VLANs, and trunks for the network topology. Configuring the base network installs the 3-DNS in your physical network.
- **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, BIG-IP, EDGE-FX Cache, GLOBAL-SITE, and host systems that you use for load balancing and probing.
- **Sync group**
  A ***sync group*** defines the group of 3-DNS systems that share configuration settings.

Note

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

Configuring the base network

The 3-DNS interfaces and the related topics of self IP addresses, VLANs, and trunks are collectively referred to, in this manual, as the ***base network***. The base network, or at least an initial version of it, is configured when you run the Setup utility for the first time. The initial base network configuration also includes such things as the default route for the 3-DNS, fully qualified domain names, and certificate information that can only be configured using the Setup utility or its components. (To make changes to other base network components, such as domain names, default routes, and certificate information, refer to Chapter *4, Working with the Setup Utility,* which describes the Setup utility and its various components.)

A 3-DNS usually has two network interfaces. Each active interface must be configured with a VLAN membership, and each VLAN must have a self IP address. Note that most 3-DNS configurations require only one interface, VLAN, and self IP address. However, if you are configuring the 3-DNS in

bridge mode or router mode, you may need to configure two (or more) interfaces, depending on your network requirements. For more information on configuring the base network, refer to Chapter 5, *Configuring the Base Network*.

Defining data centers and servers

In the 3-DNS configuration, 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, BIG-IP, EDGE-FX Cache, GLOBAL-SITE, or host)
- Server IP address (or shared IP alias for redundant systems)
- Name of the data center where the server runs
- The **big3d** agent factories (on 3-DNS, BIG-IP, EDGE-FX Cache, and GLOBAL-SITE only)
- Virtual servers managed by the server (BIG-IP, EDGE-FX Cache, and host servers 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 systems in your network. See the **3-DNS Reference Guide**, Chapter 4, **The big3d Agent**, for help with determining how both of these issues affect your installation.*

Planning a sync group

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

When you define the sync group, you select the sync group members from the list of 3-DNS systems you have already defined. The sync group lists the 3-DNS systems in the order in which you selected them. The first 3-DNS in the list becomes the principal 3-DNS. The remaining 3-DNS systems in the list become receivers. If the principal 3-DNS becomes disabled, the next 3-DNS in the list becomes the principal 3-DNS until the original principal 3-DNS comes back online.

Understanding how a sync group works

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 3-DNS systems in a sync group operate as peer servers. At set intervals, the **syncd** utility compares the time stamps of the configuration files earmarked for synchronization on all of the 3-DNS systems. If the time stamp on a specific file differs between 3-DNS systems, the 3-DNS with the latest file broadcasts the file to all of the other 3-DNS systems in the group.

Understanding how the time tolerance variable affects a sync group

The time tolerance variable is a global variable that defines the number of seconds that the time setting on one 3-DNS can be ahead or behind the time setting on another 3-DNS. If the difference between the times on the systems is greater than the time tolerance, the time setting on the 3-DNS running behind is reset to match the 3-DNS with the most recent time. For example, if the time tolerance is 5 seconds, and one 3-DNS is running 10 seconds ahead of the other, the 3-DNS running behind has its time reset to match the one running 10 seconds ahead. If the second system 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 synchronization). The default setting is **10** seconds.

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

Setting up communications on a 3-DNS

There are three different communication issues that you need to resolve when you set up communication between the 3-DNS systems running in your network

- **3-DNS systems communicating with other 3-DNS systems**
  To allow 3-DNS systems to communicate with each other, you must set up **ssh** and **scp** utilities for crypto systems (that use SSH and SCP) that communicate with other crypto systems, and you must set up **rsh** and **rcp** utilities for systems that communicate with non-crypto systems (that do not use SSH and SCP).
- **3-DNS communicating with BIG-IP, EDGE-FX Cache, and GLOBAL-SITE**
  To allow 3-DNS to communicate with BIG-IP, EDGE-FX Cache, and GLOBAL-SITE, you address the same **ssh** and **rsh** issues. Crypto systems communicating with other crypto systems can use **ssh** and **scp** utilities, but systems communicating with non-crypto systems require **rsh** and **rcp** utilities.

- **3-DNS communicating with big3d agents**
  To allow communications between **big3d** agents and the 3-DNS, you need to configure iQuery ports on any 3-DNS, BIG-IP, EDGE-FX Cache, and GLOBAL-SITE systems that run the **big3d** agent.

Note

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

Setting up communication between crypto and non-crypto systems

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

If your network is a mixed environment, that is, composed of both crypto and non-crypto systems, you need to enable the **rsh** and **rcp** utilities on the crypto systems. Though the **rsh** and **rcp** utilities come pre-installed on the crypto systems, you must explicitly enable these utilities. You can enable the utilities when you run the Setup utility, or you can run the **config_rshd** script from the command line. Table 2.1 shows the ports and protocols used by 3-DNS for crypto and non-crypto communications.

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

Table 2.1 *Communications between 3-DNS systems*

Setting up data collection with the big3d agent

The **big3d** agent collects performance information from other 3-DNS, BIG-IP, GLOBAL-SITE, and EDGE-FX Cache systems on behalf of the 3-DNS you are configuring. 3-DNS 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, review Chapter 3, *The big3d Agent*, in the ***3-DNS Reference Guide***.

Choosing the 3-DNS mode

The 3-DNS can run in one of three modes: node, bridge, router. The base network configuration changes depending on which mode you choose. The following sections describe the three modes and provide basic configuration examples.

Running a 3-DNS in node mode

Node mode is the traditional way to configure the 3-DNS. The benefits of running the 3-DNS in node mode are as follows:

- You can replace your name servers with 3-DNS systems.
- You can use the 3-DNS as the authoritative DNS server for your domain.
- You can manage your DNS zone files with NameSurfer.

When you replace your DNS servers with 3-DNS, you can use the extensive wide-area traffic management capabilities of the 3-DNS in conjunction with the standard DNS protocol. When the 3-DNS receives a request that matches a wide IP, it routes that request to the best virtual server in your network. When 3-DNS receives a non-matching request, that request is handled by the BIND utility (**named**) that is running on the 3-DNS.

When you configure the 3-DNS to be authoritative for your domain, you can easily manage DNS zone files using NameSurfer, a browser-based, third-party application included on the 3-DNS. When you define wide IPs in the Configuration utility, the NameSurfer application automatically makes the appropriate additions to the zone files. The changes are then broadcast to the other 3-DNS systems in your network.

◆ Note

If you configure wide IPs from the command line, you need to make the corresponding zone file changes from the command line.

Using the 3-DNS synchronization features

If you use the advanced synchronization features of the 3-DNS, we strongly recommend that you configure each 3-DNS 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 systems in the network and have those changes automatically broadcast to all of the other systems in the network.
- Each 3-DNS 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.

Importing BIND files to NameSurfer during an initial installation

During the initial configuration, you can specify that the 3-DNS import any existing BIND files from your name server to the 3-DNS. During the initial configuration, you can also designate NameSurfer as the primary name server for your domain. This forces NameSurfer to automatically format your BIND files in the NameSurfer format. For more information, refer to the NameSurfer documentation available from the home screen in the Configuration utility.

Running a 3-DNS in bridge mode or router mode

Running the 3-DNS in bridge mode or router mode offers the following benefits:

- You gain the wide-area traffic management capabilities of the 3-DNS without disrupting your current DNS system.
- In an enterprise, you can install, configure, and test the 3-DNS before you add the system to your production environment.
- You do not use NameSurfer to manage your zone files.
- You can load balance requests across two separate IP networks.

When you configure the 3-DNS in bridge mode, you install the 3-DNS into your network so that all DNS requests are intercepted by the 3-DNS before they are sent to your name server for resolution. Based on the content of the request, the 3-DNS does one of the following:

- If the request matches a wide IP managed by the 3-DNS, the system responds to the request with the best available virtual server in your network.
- If the request does note match any wide IPs managed by the 3-DNS, the system forwards the request to the DNS server for resolution.

Planning issues for the load balancing configuration

The final phase of installing a 3-DNS 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 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 a BIG-IP, virtual servers managed by an EDGE-FX Cache, virtual servers managed by a generic host server, or they can be individual host servers themselves. Note that the 3-DNS 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 that does not require significant additional configuration steps, such as Round Robin or Hops. 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 configurations in this Administrator Guide, in Chapter 7, *Configuring a Globally-Distributed Network*, and in Chapter 8, *Configuring a Content Delivery Network*.

Using advanced traffic control features

The 3-DNS 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 7, *Configuring a Globally-Distributed Network*, and in the ***3-DNS Reference Guide***, see Chapter 13, *Topology*.
- **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 10, *Production Rules*, in the ***3-DNS Reference Guide***, for information about setting up production rules.

3

Setting Up the Hardware

- Unpacking and installing the hardware
- Addressing hardware configuration issues
- Setting up automatic DNS zone file management
- Preparing workstations for command line access
- Using a serial terminal
- Configuring Sendmail
- Shutting down the 3-DNS

Unpacking and installing the hardware

Regardless of the configuration you intend to use, you need to completely install the 3-DNS hardware. This chapter reviews the hardware requirements, introduces the hardware, notes the environmental issues, and gives procedures for installing the hardware. It also provides basic information about configuration and management issues for redundant systems, multiple network interfaces, and DNS zone files.

The two basic tasks you must complete to get the 3-DNS installed and set up are as follows:

- Connect the peripheral hardware and connect the 3-DNS to the network.
- Turn the system on and run the Setup utility.
  The Setup utility is a wizard that helps you configure basic system elements such as administrative passwords, IP addresses, and host names for both the root system and the 3-DNS web server. For more information on configuring your 3-DNS, see Chapter 4, *Working with the Setup Utility*.

Reviewing the hardware requirements

The 3-DNS comes with the hardware you need for installation and maintenance. However, you must provide standard peripheral hardware, such as a keyboard and monitor or serial terminal.

Hardware provided with the 3-DNS

When you unpack the 3-DNS, make sure the following components are included:

- One power cable
- One PC/AT-to-PS/2 keyboard adapter
- Four rack-mounting screws
- One extra fan filter
- One 3-DNS Administrator Kit, which includes the 3-DNS Software and Documentation CD-ROM, the hardware poster, and the Configuration Worksheet.

If you purchase a hardware-based redundant system, you also receive one fail-over cable to connect the two units together (network-based redundant systems do not require a fail-over cable).

Peripheral hardware that you provide

For each 3-DNS in the system, you need to provide the following peripheral hardware:

- Standard input/output hardware for direct administrative access to the 3-DNS. Either of the following options is acceptable:

  - VGA monitor and PC/AT-compatible keyboard
  - Serial terminal and a null modem cable. (See *Using a serial terminal*, on page 3-6, for serial terminal configuration information.)
- Network hubs, switches, or concentrators to connect to the 3-DNS network interfaces. The devices you select must be compatible with the network interface cards installed in the 3-DNS. The devices can support 10/100 Ethernet or Gigabit Ethernet. Note that for Ethernet, you need either a 10Mb/sec or 100 Mb/sec hub or switch.

If you plan on performing remote administration from your own PC workstation, as most users do, we recommend that you have your workstation already in place. Keep in mind that the Setup utility prompts you to enter your workstation's IP address when you set up remote administrative access.

Familiarizing yourself with the 3-DNS hardware

The 3-DNS is offered in a 2U hardware configuration. Before you begin to install the 3-DNS, you may want to quickly review the hardware poster that illustrate the controls and ports on the front and the back of a 2U 3-DNS.

Environmental requirements and usage guidelines

A 3-DNS is an industrial network appliance, designed to be mounted in a standard 19-inch rack. To ensure safe installation and operation of the unit:

- Install the rack according to the manufacturer's instructions, and check the rack for stability before placing equipment in it.
- Build and position the rack so that once you install the 3-DNS, the power supply and the vents on both the front and back of the unit remain unobstructed. The 3-DNS must have adequate ventilation around the unit at all times.
- Do not allow the air temperature in the room to exceed 40° C (104° F).
- Do not plug the unit into a branch circuit shared by more electronic equipment than the circuit is designed to manage safely at one time.
- Verify that the voltage selector is set appropriately before connecting the power cable to the unit.

Guidelines for DC-powered equipment

A DC-powered installation must meet the following requirements:

- Install the unit using a 20 Amp external branch circuit protection device.
- For permanently connected equipment, incorporate a readily- accessible disconnect in the fixed wiring.
- Use only copper conductors.

Installing and connecting the hardware

There are six basic steps to installing the hardware. You simply need to install the system in the rack, connect the peripheral hardware and the external and internal interfaces, and then connect the fail-over and power cables. If you have a unit with three or more network interface cards (NICs), be sure to review step 3.

WARNING

Do not turn on a 3-DNS until all peripheral hardware is connected to the unit.

To install the hardware

1. Mount the 3-DNS on the rack and secure it using the four rack-mounting screws that are provided.
2. Connect the hardware that you have chosen to use for input/output:
   - If you are using a VGA monitor and keyboard, connect the monitor connector cable to the video port and connect the keyboard connector cable to the keyboard port. Note that a PC/AT-to-PS/2 keyboard adapter is included with each 3-DNS (see the component list on page 3-1).
   - Optionally, if you are using a serial terminal as the console, connect the serial cable to the serial terminal port.
3. Connect the external interface to the network from which the 3-DNS receives connection requests.

   If you have purchased a unit with three or more network interface cards (NICs), be sure to note or write down how you connect the cables to the internal and external interfaces. When you run the Setup utility, it automatically detects the number of interfaces that are installed and prompts you to configure more external interfaces, if you want. It is important to select the correct external interface based on the way you have connected the cables to the back of the unit.
4. If you have a hardware-based redundant system, connect the fail-over cable to the fail-over port on each unit.
5. Connect the power cable to the 3-DNS, and then connect it to the power source.

WARNING

Before connecting the power cable to a power supply, customers outside the US should make sure that the voltage selector is set appropriately. This check is necessary only if the 3-DNS has an external voltage selector.

Addressing hardware configuration issues

Before you start the hardware setup, you may want to review the following items which address configuration and management issues for redundant systems, systems that use more than one network interface, and DNS zone file management.

Setting up a stand-alone unit or a redundant system

If you are setting up a stand-alone unit, you need one IP address and host name for each of the interfaces you plan to connect to the network. If you are setting up a redundant system, you need the actual IP address for each interface in each unit. If you are connecting the redundant system to more than one network, you also need a shared IP alias for each interface.

Setting up fail-over for a redundant system

Hardware-based fail-over is a redundant system that connects two 3-DNS units directly to each other using a fail-over serial cable. ***Network-based fail-over*** is a redundant system where two units are connected to each other either directly using an Ethernet cable, or indirectly via an Ethernet network. Of the two units in a redundant system, one runs as the ***active unit***, managing all DNS resolution requests, and the other runs as the ***standby unit***, waiting to take over in case the active unit fails and reboots. The communication between the units, such as fail-over notification, runs across either the fail-over cable in the hardware-based redundant system, or the network in the network-based redundant system.

When you run the Setup utility, it prompts you to enter the IP address of the other unit in the redundant system.

Triggering a fail-over in a redundant system

The 3-DNS tracks two key aspects of the system to validate system performance. In a redundant system, there are two events that indicate a system failure, and trigger a fail-over.

- If the **3dnsd** daemon becomes unresponsive, or if you manually stop the daemon using the **3ndc stop** or **3ndc restart** commands, the 3-DNS treats this as a system failure and initiates a fail-over.
- If the 3-DNS fails to detect any traffic on its network interfaces, it attempts to create traffic to test the integrity of the interface. If the test fails, the 3-DNS treats this as a system failure and initiates a fail-over.

Using redundant systems with the sync group feature

If you include a redundant system in a sync group, you specify the redundant system's shared IP address when you define the sync group.

Using more than one network interface

The Setup utility automatically detects the number of interfaces installed in the 3-DNS. In most instances, you need to configure only one of the interfaces. If you want to configure an additional interface, you simply enter the same type of information that you entered for the first interface.

The 3-DNS now runs in three modes: node, bridge, and router. If you are running the 3-DNS in node mode, you only need to configure one interface. If you are running the 3-DNS in bridge mode, you use the additional interface to connect the 3-DNS to the authoritative DNS using either a cross-over cable, or through a separate switch or hub. In bridge mode, you do not need to configure the information in the Setup utility for the additional network interface. In router mode, you must configure two (or more) interfaces, on different subnets, in the Setup utility.

◆ Note

For more information about the 3-DNS modes, refer to ***Configuring the 3-DNS mode****, on page 4-8.*

Setting up automatic DNS zone file management

If you choose to run the 3-DNS in node mode (that is, as the primary name server for your domain), the Setup utility asks you if you want to use the NameSurfer application as the primary name server for DNS zone files. We recommend that you always run NameSurfer as the primary name server for DNS zone files. When you define or modify wide IPs in the Configuration utility, NameSurfer automatically makes the corresponding changes to the DNS zone files. The NameSurfer application also provides you with easy management of high-level domain zone files unrelated to the wide IP configuration.

If you plan on transferring existing BIND files from a primary DNS server to the 3-DNS, refer to *Importing BIND files to NameSurfer during an initial installation*, on page 2-11.

◆ Note

If you run the 3-DNS in router or bridge mode, you do not configure the NameSurfer application because the 3-DNS is not the authoritative DNS for your domain.

Preparing workstations for command line access

The type of system you have determines the options you have for remote command line administration:

- Crypto 3-DNS systems support secure shell (SSH) command line access. Note that if you have a Windows-based PC workstation, you can also use the Mindbright Mindterm SSH client to run an **ssh** session from a web browser. If you have a UNIX workstation, you can use a standard **ssh** client.
- Non-crypto 3-DNS systems support command line access using a standard **rsh** shell.

Note

If you are working with a crypto 3-DNS, you can access the Mindterm SSH client through the web-based Configuration utility.

Using a serial terminal

If you want to use a serial terminal (in addition to a standard console) with the 3-DNS, you need only ensure that the serial terminal settings are as follows:

- 9600 baud
- 8 bits
- 1 stop bit
- No parity

Configuring Sendmail

You can configure the 3-DNS to send email notifications to you, or to other administrators, using the Sendmail utility. The 3-DNS includes a sample Sendmail configuration file that you can use to start with, but you must customize the Sendmail setup for your network environment before you can use it.

Before you begin setting up Sendmail, you may need to look up the name of the mail exchanger for your domain. If you already know the name of the mail exchanger, refer to *Setting up Sendmail*, on page 3-7, for details about setting up the **sendmail** utility itself.

Finding the mail exchanger for your domain

You can use the **nslookup** command on any workstation that is configured for lookup. Once you find the primary IP address for your domain, you can find the mail exchanger for your domain.

To find the mail exchanger for your domain

1. Identify the default server name for your domain. From a workstation capable of name resolution, type the following on the command line:

   ```
   nslookup
   ```

2. The command returns a default server name and corresponding IP address:

   ```
   Default Server: <server name>
   Address:  <server>
   ```

3. Use the domain name to query for the mail exchanger:

   ```
   set q=mx
   <domain name>
   ```

The returned information includes the name of the mail exchanger. For example, the sample information shown in Figure 3.1 lists **bigip.net** as the preferred mail exchanger.

```
bigip.net   preference = 10, mail exchanger = mail.domain.com
bigip.net   nameserver = ns1.bigip.net
bigip.net   nameserver = ns2.bigip.net
bigip.net   internet address = 192.168.112.1
ns1.bigip.net       internet address = 192.168.112.2
ns2.bigip.net       internet address = 192.168.112.3
```

Figure 3.1 *Sample mail exchanger information*

Setting up Sendmail

When you set up Sendmail, you must edit three configuration files. Since the 3-DNS does not accept email messages, you can use the **crontab** utility to purge unsent or returned messages and send them to yourself or another administrator.

To set up and start Sendmail

1. From the command line, open the **/etc/rc.conf** file. Add the following line to the file:

   ```
   sendmail_enable="YES"
   ```

2. Save and close the **/etc/rc.conf** file.

3. To set the name of your mail exchange server, open the **/etc/mail/sendmail.cf** file and set the **DS** variable to the name of your mail exchanger. The syntax for this entry is:

   ```
   DS<MAILHUB_OR_RELAY>
   ```

4. Save and close the **/etc/mail/sendmail.cf** file.

5. To allow Sendmail to purge outgoing messages that cannot be delivered immediately from the queue containing mail, open the **/etc/crontab** file, and change the last line of the file to read:

```
0,15,30,45 * * * * root /usr/sbin/sendmail -q > /dev/null 2>&1
```

6. Save and close the **/etc/crontab** file.
7. To prevent returned or undeliverable email from going unnoticed, open the **/etc/aliases** file and create an entry so that **root** points to you or another administrator at your site.

```
root: networkadmin@domain.com
```

8. Save and close the **/etc/aliases** file.
9. Run the **/usr/sbin/newaliases** command to generate a new aliases database that incorporates the information you added to the **/etc/aliases** file.
10. To turn Sendmail on, either reboot the system, or type the following command:

```
/usr/sbin/sendmail -bd -q30m
```

Note

The 3-DNS supports only outgoing mail for Sendmail servers.

Shutting down the 3-DNS

When you need to turn the 3-DNS completely off, you need to complete two tasks. The first task is to shut down the 3-DNS software. After you shut down the 3-DNS software, you can turn off the power to the system.

To shut down the BIG-IP software from the command line

1. To shut down the BIG-IP software, type the following command:

```
halt
```

2. When you see the following message, it is safe to turn off the power to the system:

```
System is halted, hit reset, turn power off, or press
return to reboot
```

WARNING

Do not remove the power supply from the power source to turn off the 3-DNS. Doing so may result in irrevocable damage to the system.

4

Working with the Setup Utility

- Creating the initial configuration with the Setup utility
- Connecting to the 3-DNS for the first time
- Using the Setup utility for the first time
- Running the Setup utility after creating the initial configuration

Creating the initial configuration with the Setup utility

Once you install and connect the 3-DNS hardware, the next step in the installation process is to turn the system on and run the Setup utility. The Setup utility defines the initial configuration settings required to install the 3-DNS into the network. You can run the Setup utility remotely from a web browser, or from an SSH or Telnet client, or you can run it directly from the console.

Before you connect to the 3-DNS, we recommend that you gather the list of information outlined in the configuration worksheet provided with the system. Note that the screens you see are tailored to the specific hardware and software configuration that you have. For example, if you have a single system, the Setup utility skips the redundant system screens.

◆ Note

If you are configuring the 3-DNS module on a BIG-IP, refer to the BIG-IP documentation for this part of the installation process.

Connecting to the 3-DNS for the first time

The Setup utility prompts you to enter the same information, whether you run the utility from a web browser or from the command line. When the utility completes, we recommend that you reboot the system. This automatically removes the default IP address and root password provided specifically for the purposes of running the Setup utility remotely. The 3-DNS replaces the default IP address and root password with the password and IP addresses that you define when you run the utility for the first time.

Running the utility from a console or serial terminal

Before you can run the Setup utility from either a console or a serial terminal, you must first log in. Use the following default user name and password to log in.

User name: **root**

Password: **default**

After you log in, you can start the utility directly from the console or serial terminal by typing the command **config**. Once you complete the utility, we recommend that you reboot the 3-DNS.

◆ Note

If you want to set up a terminal connection directly to the 3-DNS, see ***Using a serial terminal****, on page 3-6.*

Running the Setup utility remotely

You can run the Setup utility remotely only from a workstation that is on the same LAN as the unit. To allow remote connections for the Setup utility, the 3-DNS comes with two pre-defined IP addresses, and a pre-defined root password. The default root password is **default**, and the preferred default IP address is **192.168.1.245**. If this IP address is unsuitable for your network, the 3-DNS uses an alternate IP address, **192.168.245.245**. However, if you define an IP alias on an administrative workstation in the same IP network as the 3-DNS, the unit detects the network of the alias and uses the corresponding default IP address.

Once the utility finishes and the system reboots, these default IP addresses and the root password are replaced by the information that you entered in the Setup utility.

Setting up an IP alias for the default IP address before you turn on the system

You must set up an IP alias for your remote workstation before you turn on the system and start the Setup utility. The remote workstation must be on the same IP network as the system. If you add this alias prior to booting up the 3-DNS, the system detects the alias and uses the corresponding address.

To set up an IP alias for the alternate IP address

The IP alias must be in the same network as the default IP address you want the 3-DNS to use. For example, on a UNIX workstation, you might create one of the following aliases:

- If you want the unit to use the default IP address **192.168.1.245**, then add an IP alias to the machine you want to use to connect to the system using the following command:

  ```
  ifconfig exp0 add 192.168.1.1
  ```

- If you want to use the default IP address **192.168.245.245**, then add an IP alias such as:

  ```
  ifconfig exp0 add 192.168.245.1
  ```

WARNING

On Microsoft Windows® or Windows NT® machines, you must use a static IP address, not DHCP. Within the network configuration, add an IP alias in the same network as the IP in use on the unit. For information about adding a static IP address to a Microsoft Windows operating system, please refer to your vendor's documentation.

Determining which default IP address is in use

After you configure an IP alias on the administrative workstation in the same IP network as the 3-DNS and you turn the system on, the 3-DNS sends ARPs on the internal VLAN to see if the preferred **192.168.1.245** IP address is in use. If the address is appropriate for your network and is currently available, the 3-DNS assigns it to the internal VLAN. You can immediately use it to connect to the unit and start the Setup utility.

If the alternate network is present on the LAN, **192.168.245.0/24**, or if the node address **192.168.1.245** is in use, then the 3-DNS assigns the alternate IP address **192.168.245.245** to the internal VLAN instead.

Starting the Setup utility from a web browser

When you start the utility from a web browser, you use the selected default IP address as the application URL.

To start the Setup utility in a web browser

1. Open a web browser on a workstation connected to the same IP network as the internal VLAN of the system.
2. Type the following URL, where **<default IP>** is the IP address in use on the 3-DNS internal VLAN.
   https://<default IP>
3. At the login prompt, type **root** for the user name, and **default** for the password.
   The Configuration Status screen opens.
4. On the Configuration Status screen, click **Start Wizard**.
5. Fill out each screen using the information from the Setup utility configuration list. After you complete the Setup utility, the 3-DNS reboots and uses the new settings you defined.

◆ Note

You can rerun the Setup utility from a web browser at any time by clicking the Setup utility link on the welcome screen.

Starting the Setup utility from the command line

You can run the command line version of the Setup utility from a remote SSH client or from a Telnet client.

To start the Setup utility from the command line

1. Start an SSH client on a workstation connected to the same IP network as the internal VLAN of the 3-DNS.
2. Type the following command, where **<default IP>** is the IP address in use on the 3-DNS internal VLAN.
   ssh <default IP>
3. At the login prompt, type **root** for the user name, and **default** for the password.
4. At the 3-DNS prompt, type the following command to start the command-line based Setup utility.
   config

5. Fill out each screen using the information from the Setup utility configuration list. After you complete the Setup utility, the 3-DNS reboots and uses the new settings you defined.

Note

*You can rerun the Setup utility at any time using the **config** command.*

Using the Setup utility for the first time

The following sections provide detailed information about the settings that you define in the Setup utility when you run the utility for the first time.

Setting the keyboard type

Select the type of keyboard you want to use with the 3-DNS. The following options are available:

- Belgian
- Bulgarian MIK
- French
- German
- Japanese - 106 key
- Norwegian
- Spanish
- Swedish
- US + Cyrillic
- US - Standard 101 key (the default)
- United Kingdom

Defining the root password

A root password allows you command line administrative access to the 3-DNS system. The password must contain a minimum of 6 characters, but no more than 32 characters. Passwords are case-sensitive, and we recommend that your password contain a combination of upper- and lower-case characters, as well as numbers and punctuation characters. Once you enter a password, the Setup utility prompts you to confirm your root

password by typing it again. If the two passwords match, your password is immediately saved. If the two passwords do not match, the Setup utility provides an error message and prompts you to re-enter your password.

WARNING

*When you run the Setup utility for the first time, you must change the root password from **default** to something else. See Chapter 12, **Administration and Monitoring**, if you later decide you want to change the root password again.*

Defining the system host name

The host name identifies the 3-DNS itself. Host names must be fully qualified domain names (FQDNs). The host portion of the name can start with a letter or digit, and must be at least two characters. The entire host name must be less than 255 characters, and each label (between dots) must be less than 63 characters.

Configuring a default gateway pool

On this screen, if you enter two or more default route addresses, the 3-DNS creates a default gateway pool. If a 3-DNS does not have a predefined route for network traffic, the unit automatically sends traffic to the pool that you define as the default gateway pool. You can think of the default gateway pool as a pool of default routes. Typically, a default gateway pool is set to zero or more gateway IP addresses. If you type more than one default gateway IP address, the additional gateways provide high availability for administrative connections. If a gateway in the default gateway pool becomes inactive, existing connections through the inactive gateway are routed through another gateway in the default gateway pool.

WARNING

All default gateway IP addresses that you add to the default gateway pool must be in the same IP network as the 3-DNS.

Configuring a redundant system's settings

There are two types of settings you need to define for redundant systems: unit IDs and fail-over IP addresses.

Unit IDs

The default unit ID number is **1**. If this is the first unit in the redundant system, use the default. When you configure the second unit in the redundant system, type **2**.

Choosing a fail-over IP address

A fail-over IP address is the IP address of the unit that will take over if the active unit in the redundant system fails.

Setting the interface media type

The media type options for each interface depend on the network interface card included in your hardware configuration. The Setup utility prompts you with the settings that apply to the interfaces installed in the system. The 3-DNS supports the following media types:

- auto (automatically detects the media type)
- 10baseT
- 10baseT, FDX
- 100baseTX
- 100baseTX, FDX
- Gigabit Ethernet

For the best results, choose the **auto** setting for each interface. In some cases, systems configured using the **auto** media setting are incompatible, and the proper duplex setting will not be negotiated. In these cases, you may need to set the media type to the same speed and duplex on this system, and on the corresponding switch or host. Check your switch or hub documentation for this information.

WARNING

The Setup utility lists only the network interfaces that it detects during system boot. If the utility lists only one interface device, a network adapter may have come loose during shipping. Check the LED indicators on the network adapters to ensure that they are working and are connected.

Configuring VLANs and IP addresses

You can create a new VLAN, or use the default VLANs, **internal** and **external**, to create the 3-DNS base network configuration. Note that in general, you need only one configured VLAN for the 3-DNS. You may want to review Chapter 5, *Configuring the Base Network*, before you configure any VLANs other than the defaults.

Determine whether you want to have security turned on or off for each VLAN. Then, type the IP address settings for the VLAN. The IP address settings include:

- Security settings
- IP address, netmask, and broadcast address
- Floating self IP address, netmask, and broadcast (for redundant systems only)

Assigning interfaces to VLANs

After you configure the VLANs that you want to use on the 3-DNS, you can assign interfaces to the VLANs. If you use the default VLANS, **internal** and **external**, we recommend that you assign at least one interface to **external**, and at least one interface to **internal**. In a typical configuration, the external VLAN is the one on which the 3-DNS receives connection requests. Note that the VLAN **internal** is optional. If you plan on running the 3-DNS in bridge or router mode, you can configure a second VLAN for a particular IP subnet. For more information on the bridge and router modes, see *Configuring the 3-DNS mode*, on page 4-8.

Associating a primary IP address and VLAN with the system host name

If you have defined more than one VLAN, you have assigned interfaces to them, you can choose one VLAN/IP address combination as the primary IP address to associate with the system's host name.

Configuring remote web server access

The 3-DNS web server provides the ability to set up remote web access on each VLAN. When you set up web access on a VLAN, you can connect to the web-based Configuration utility through the VLAN. To enable web access, specify a fully qualified domain name (FQDN) for each VLAN. The 3-DNS web server configuration also requires that you define a user name and password. If SSL is available, the configuration also generates authentication certificates.

The Setup utility guides you through a series of screens to set up remote web access.

- The first screen prompts you to select the VLAN you want to configure for web access. After you select an interface to configure, the utility prompts you to type a fully qualified domain name (FQDN) for the interface. You can configure web access on one or more interfaces.
- After you configure the interface, the utility prompts you for a user name and password. After you type a user name and password, the utility prompts you for a vendor support account. The vendor support account is not required.
- The certification screen prompts you for country, state, city, company, and division.

WARNING

If you ever change the IP addresses or host names on the 3-DNS interfaces, you must use the Setup utility to reconfigure the 3-DNS web server and the portal to reflect your new settings.

You can also add users to the existing password file, change a password for an existing user, or recreate the password file, without actually repeating the remote web server configuration process. Refer to *Managing users on the 3-DNS*, in Chapter 12, *Administration and Monitoring*.

WARNING

If you have modified the remote web server configuration outside of the Configuration utility, be aware that some changes may be lost when you run the ***Configure web servers*** *option in the Setup utility. This utility overwrites the* ***httpd.conf*** *file and* ***openssl.conf****, but does not warn you before doing so.*

Setting the time zone

Next, you need to specify the time zone for the region that the 3-DNS is in. This ensures that the clock for the 3-DNS is set correctly, and that dates and times recorded in log files correspond to the time zone of the system administrator. Scroll through the list to find the time zone at your location. Note that one option may appear with multiple names. Select the time zone you want to use, and press the Enter key to continue.

Configuring the 3-DNS mode

The 3-DNS can now run in three different modes: node, bridge, and router.

- **Node mode**
  The ***node mode*** is the traditional installation of the 3-DNS. The 3-DNS replaces a DNS server in a network and uses the DNS server's IP address. All DNS traffic is directed at the 3-DNS because it is registered with InterNIC as authoritative for the domain. In node mode, you usually run BIND on the system to manage DNS zone files. In node mode, you may also use the NameSurfer application available to manage your zone files.
- **Bridge mode**
  In ***bridge mode***, the 3-DNS acts as an IP bridging device by forwarding packets between two LAN segments (usually on the same IP subnet). The system usually has one IP address, and is installed between the router or switch and the authoritative DNS server. The 3-DNS does not replace the authoritative DNS server. The 3-DNS filters all DNS packets that match wide IPs, and forwards the remaining packets to the authoritative DNS server for resolution. Note that this may be the preferred method of using the 3-DNS because you do not have to replace the authoritative DNS server, and you can perform out-of-band testing before you deploy 3-DNS software upgrades.
- **Router mode**
  In ***router mode***, the 3-DNS acts as a router by forwarding packets between two different IP subnets. You can put the 3-DNS anywhere in the network topology so that packets destined for the authoritative DNS server have to pass through it. Router mode requires at least two IP

addresses and two VLANs. Router mode is probably most useful for Internet service providers (ISPs) that want to redirect traffic to local content servers. For example, by using the 3-DNS in router mode, an ISP can redirect requests for **ads.mydomain.net** to a local ad server.

Configuring remote administrative access

After you configure remote web access, the Setup utility prompts you to configure remote command line access. On most 3-DNS units, the first screen you see is the Configure SSH screen, which prompts you to type an IP address for SSH command line access. If SSH is not available, you are prompted to configure access through RSH instead.

When you configure remote command line access, the Setup utility prompts you to create a support account for that method. You can use this support account to provide a support engineer access to the 3-DNS.

When the Setup utility prompts you to enter an IP address for administration, you can type a single IP address or a list of IP addresses, from which the 3-DNS will accept administrative connections (either remote shell connections, or connections to the web server on the 3-DNS). To specify a range of IP addresses, you can use the asterisk (*) as a wildcard character in the IP addresses.

The following example allows remote administration from all hosts on the **192.168.2.0/24** network:

```
192.168.2.*
```

Note

For administration purposes, you can connect to the 3-DNS floating self IP address, which always connects you to the active unit in an active/standby redundant system. To connect to a specific unit, connect directly to the IP address of that 3-DNS.

Configuring SSH

Use this option to configure secure shell server (**ssh**) on a 3-DNS. This utility prompts you for an IP address from which administrators may access the 3-DNS with SSH. You can use wildcard characters (*) to include all addresses from a specific part of the network. This utility also prompts you to create a support account for access by technical support.

If the service port for SSH is closed, this utility opens the service port to permit SSH connections to the 3-DNS.

Configuring RSH

Use this option to configure the remote shell (**rsh**) server on a 3-DNS. This utility prompts you for an IP address from which administrators may access the 3-DNS. You can use wildcard characters (*) to include all addresses from a specific part of the network. This utility also prompts you to create a support account for access by technical support.

If **inetd** is not currently configured, this utility configures **inetd** for the remote shell server (**rshd**). If the service port for **rsh** is closed, this utility opens the service port to permit **rsh** connections to the 3-DNS.

Initializing the iControl portal

Select this option to configure the CORBA ports (IIOP and FSSL). This option prompts you for a list of IP addresses or host names you want to embed as objects in the Portal object reference.

This option prompts you to set the Portal to use IP addresses instead of DNS names. If the Portal is set to use IP addresses, the 3-DNS does not have to do a DNS lookup.

In addition to these settings, you can change the following iControl portal settings:

- You can set the security mode of the portal. You can allow the portal to handle non-secure requests.
- You can change the name of the Portal object reference file.
- You can specify the Portal PID file name.

Configuring NTP support

You can synchronize the time on the 3-DNS to a public time server by using Network Time Protocol (NTP). NTP is built on top of UDP and assures accurate, local timekeeping with reference to clocks located on the Internet. The NTP protocol is capable of synchronizing distributed clocks, within milliseconds, over long periods of time. If you choose to enable NTP, make sure UDP port **123** is open in both directions when the 3-DNS is behind a firewall.

Configuring NameSurfer for zone file management

In the final series of the Setup utility screens, you choose whether to have NameSurfer handle DNS zone file management on the current 3-DNS. If you configure the 3-DNS in node mode, we strongly recommend that you configure NameSurfer to handle zone file management. If you designate NameSurfer as the primary name server, NameSurfer converts the DNS zone files on the system, becomes the authoritative DNS, and automatically processes changes and updates to the zone files. (You can access the NameSurfer application directly from the Configuration utility).

To open the NameSurfer application

1. In the navigation pane, click **NameSurfer**.
   The NameSurfer home screen opens.

2. Edit the zone file information as required.
   For help with the NameSurfer application, click **Help** in the NameSurfer navigation pane.

◆ **Note**

Remember that if you run the 3-DNS in bridge or router mode, the system is not authoritative for any domains, so the NameSurfer application is not available to manage any zone files.

Running the Setup utility after creating the initial configuration

You can also use the Setup utility to change existing settings at any time. After you complete the initial configuration, the Setup utility presents a menu of individual configuration options. There is a section of required configuration options and a section of optional configuration options.

To run the Setup utility from the command line, type in the following command:

`config`

Figure 4.1 shows the Setup utility menu.

```
lqq I N I T I A L   S E T U P   M E N U qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x                                                                               x
x                                                                               x
x    Choose the desired configuration function from the list below.             x
x                                                                               x
x                                                                               x
x    (A) All configuration steps        (R) Steps for redundant systems         x
x                                                                               x
x    REQUIRED                                                                   x
x    (E) Set default gateway pool       (V) Configure VLANs & networking        x
x    (H) Set host name                  (W) Configure web servers               x
x    (P) Set root password                                                      x
x                                                                               x
x    OPTIONAL                                                                   x
x    (D) Configure DNS                  (O) Configure remote access             x
x    (F) Configure FTP                  (S) Configure SSH                       x
x    (I) Initialize iControl portal     (T) Configure Telnetd                   x
x    (K) Set keyboard type              (U) Configure RSH                       x
x    (M) Define time servers            (Z) Set time zone                       x
x    (N) Configure NameSurfer           (Q) Quit                                x
x                                                                               x
x    Enter Choice:                                                              x
x                                                                               x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

Figure 4.1 *The Setup utility menu*

Additional configuration options in the Setup utility

The following Setup utility options are available after you have configured the 3-DNS for the first time. Note that while these options are available as part of the platform, you may not want to enable them for security reasons.

Configuring FTP

Use this utility to configure FTP on the 3-DNS. This utility prompts you for an IP address from which administrators may access the 3-DNS with FTP. You can use wildcard characters (*) to include all addresses from a specific part of the network. This utility also prompts you to create a support account for access by technical support.

If the service port for FTP is closed, this utility opens the service port to permit FTP connections to the 3-DNS.

Configuring Telnet

Use this option to configure Telnet on the 3-DNS. The utility prompts you for a configuration address for each service from which administrators may access the 3-DNS. You can use wildcard characters (*) to include all addresses from a specific part of the network. This utility also prompts you to create a support account for access by technical support.

If **inetd** is not currently configured, this utility configures **inetd** for the requested services. If the ports for Telnet or FTP are closed, this utility opens the ports to permit Telnet or FTP connections to the 3-DNS.

WARNING

Although you can configure FTP and Telnet on a 3-DNS, we recommend that you leave these services disabled, for security reasons.

5

Configuring the Base Network

- Introduction
- Configuring the interfaces
- Configuring a self IP address
- Configuring trunks
- Working with VLANs

Introduction

This chapter describes the 3-DNS interfaces and the related topics of self IP addresses, VLANs, and trunks. ***Interfaces*** are the network interface cards installed in the 3-DNS, and are designated by a number that specifies their physical position in the 3-DNS. A ***VLAN*** is a logical grouping of network interfaces. You can use a VLAN to logically group devices that are on different network segments. ***Self IP addresses*** are the IP addresses owned by the 3-DNS. A ***trunk*** is a group of interfaces associated for link aggregation and fail-over. Collectively, these objects are referred to in this manual as the ***base network***.

The base network is what you configure when you run the Setup utility for the first time. This initial base network configuration also includes such things as the default gateway pool for the 3-DNS, fully qualified domain names, remote communications, and certificate information that can only be configured using the Setup utility. This chapter focuses on the VLAN and networking components of the Setup utility as you would configure them once the initial base network is in place. This chapter also discusses trunks and VLAN grouping, which you can configure only after you configure the initial base network for the first time. (To make changes to other base network components, such as remote access, default routes, and certificate information, refer to Chapter 4, *Working with the Setup Utility*.)

Each active interface on the 3-DNS must be configured with a VLAN membership, and each VLAN must have a self IP address. (Each interface can have one or more additional, floating self IP addresses as required.) You can change the self IP addresses or create any number of additional ones for a VLAN in floating form.

The configuration options for VLANs include ***tagging*** (which allows multiple VLANs to be configured on a single interface), creating new VLANS for additional interfaces, and associating a single VLAN with multiple interfaces. In addition, you can group separate VLANs for the purpose of sharing packets between them. This is known as ***VLAN grouping***.

Trunks are aggregated links. In link aggregation, interfaces can be combined into a trunk to increase bandwidth in an additive manner. The other benefit of link aggregation is link fail-over. If one link in a trunk goes down, traffic is simply redistributed over the remaining links.

Configuring the interfaces

Typically, a 3-DNS has two network interfaces. The following sections describe the naming convention, displaying the status, setting the media type, and setting the duplex mode for the interfaces in the 3-DNS.

Understanding the interface naming convention

By convention, the Ethernet interfaces on a 3-DNS take the name **<s>.<p>** where **s** is the slot number of the NIC, and **p** is the port number on the NIC. For the 2U platform, slot numbering is top-to-bottom and port numbering is left-to-right as shown in Figure 5.1.

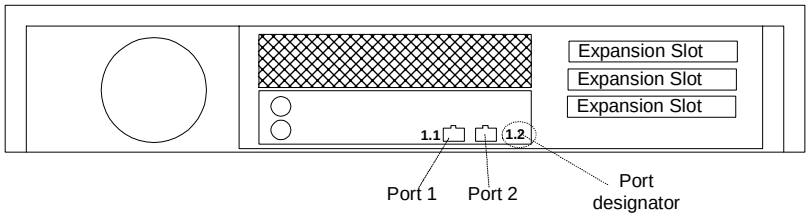

Figure 5.1 *Rear view of a 3-DNS with two interface ports*

Displaying status for interfaces

Use the following syntax to display the current status and the settings for the installed interface cards:

```
b interface show
```

Figure 5.2 is an example of the output you see when you issue this command.

```
interface  speed   pkts   pkts   pkts   pkts   bits   bits errors trunk STP
            Mb/s     in    out   drop   coll     in    out
  1.1 UP  100 HD      0    213      0      0      0  74.2K      0
  2.1 UP  100 HD     20     25      0      0  28.6K  33.9K      0
```

Figure 5.2 *The **bigpipe interface show** command output*

Use the following syntax to display the current status and the setting for a specific interface.

```
b interface <if_name> show
```

Setting the media type

You can set the media type to the specific media type for the interface card or to **auto** for auto detection. If the media type is set to **auto** and the card does not support auto detection, the default type for that interface is used, for example **100BaseTX**.

Use the following syntax to set the media type:

```
b interface <if_name> media <media_type> | auto
```

(Default media type is **auto**.)

Note

*If the 3-DNS is inter-operating with an external switch, the media setting should match that of the switch. To accomplish this, it is best to specify the setting explicitly, and not rely on automatic detection using **auto**.*

Setting the duplex mode

You can set duplex mode to full or half duplex. If the media type does not allow duplex mode to be set, this is indicated by an onscreen message. If media type is set to **auto**, or if setting duplex mode is not supported for the interface, the duplex setting is not saved to **bigip.conf**.

Use the following syntax to set the duplex mode:

```
b interface <if_name> duplex  full | half | auto
```

(Default mode is **auto**.)

Note

*If the 3-DNS is inter-operating with an external switch, the media setting should match that of the switch. To accomplish this, it is best to specify the setting explicitly, and not rely on automatic detection using **auto**.*

Configuring a self IP address

A self IP address is an IP address mapping to one or more VLANs and their associated interfaces on a 3-DNS. You assign a self IP address to each interface on the unit as part of the initial configuration, and you also assign a floating (shared) alias for units in a redundant system. You can create additional self IP addresses for health checking, gateway failsafe, routing, or other purposes. You create additional self IP addresses using the **self** command in the **bigpipe** utility. (See the ***3-DNS Reference Guide***, Appendix C, *bigpipe Command Reference*, for more information.)

To add a self IP address to a VLAN using the Configuration utility

1. In the navigation pane, click **Network**.
   The VLANs screen opens.
2. In the VLANs screen, click the Self IP Addresses tab.
   The Self IP Addresses screen opens.
3. On the Self IP Addresses screen, click the **Add** button.
   The Add Self IP Address screen opens.
4. In the **IP Address** box, type the self IP address to be assigned.
5. In the **Netmask** box, type an optional netmask.

6. In the **Broadcast** box, type an optional broadcast address.
7. If you want to configure the self IP address as a floating address, click a check in the **Floating** box.
8. In the **VLAN** box, type the name of the VLAN to which you want to assign the self IP address.
9. Click the **Done** button.

To add a self IP address to a VLAN from the command line

Assigning a self IP address to a VLAN automatically maps it to the VLAN's interfaces. Use the following syntax:

```
b self <addr> vlan <vlan_name> [ netmask <ip_mask> ][ broadcast <broadcast_addr>] [unit
    <id>]
```

You can add any number of additional self IP addresses to a VLAN to create aliases. For example:

```
b self 11.11.11.4 vlan external
b self 11.11.11.5 vlan external
b self 11.11.11.6 vlan external
b self 11.11.11.7 vlan external
```

Also, any one self IP address can have **floating** enabled to create a ***floating alias*** that is shared by both units of a 3-DNS redundant pair:

```
b self 11.11.11.8 floating enable
```

Configuring trunks

Link aggregation is the grouping of links (individual physical interfaces) to form a ***trunk***. Link aggregation increases the bandwidth of the individual links in an additive manner. Thus, four fast Ethernet links, if aggregated, create a single 400 Mbps link. The other advantage of link aggregation is link fail-over. If one link in a trunk goes down, traffic is simply redistributed over the remaining links.

A trunk must have a controlling link, and it acquires all the attributes of that controlling link from layer 2 and above. The trunk automatically acquires the VLAN membership of the controlling link, but does not acquire its media type and speed. Outbound packets to the controlling link are load balanced across all of the known-good links in the trunk. Inbound packets from any link in the trunk are treated as if they came from the controlling link.

You can create a trunk with a maximum of eight links. For optimal performance, links should be aggregated in powers of two. Thus, you ideally will aggregate two, four, or eight links.

To configure a trunk using the Configuration utility

1. In the navigation pane, click **Network**.
   The Network screen opens.
2. Click the **Trunks** tab.
   The Trunks screen opens.
3. On the Trunks screen, click the **Add** button.
   The Add Trunk screen opens.
4. From the Available Interfaces list, select the link that is to be the controlling link, and click **controlling >>**.
   The interface appears at the top of the Aggregated Interfaces list.
5. From the Available Interfaces list, select the remaining link(s) and click **aggregated >>**.
   The interface(s) appears in the Aggregated Interfaces list below the controlling link.
6. Click **Done**.

To configure a trunk from the command line

Use the following syntax to configure a trunk from the command line:

```
b trunk <controlling_if> define <if_list>
```

Interfaces are specified using the **s.p** naming convention, where **s** is slot number and **p** is port number. An **<if_list>** is one or more such interfaces, with multiple interfaces separated by spaces.

For more information on interface naming, refer to *Understanding the interface naming convention*, on page 5-2.

Working with VLANs

A VLAN, or virtual local area network, is a grouping of separate networks that causes them to behave as if they were a single local area network, whether or not there is a direct Ethernet connection between them. A VLAN can be associated with one or more interfaces on one or more systems. VLANs are configured using software rather than hardware, which offers a great degree of flexibility. VLAN segmentation localizes broadcast traffic and also provides security.

Acting as a layer 2 switch, the 3-DNS supports two types of VLANs: interface-group (untagged), and tagged. The difference is in the method by which traffic is passed among the interfaces that are members of the VLAN. An interface group VLAN allows untagged traffic onto a member interface based on a table of member MAC addresses. A tagged VLAN allows tagged traffic onto a member interface based on the interface having a tag ID matching that of the packets.

A 3-DNS interface can belong to only one untagged VLAN, but can belong to multiple tagged VLANS. Tagging therefore becomes a way of accepting traffic from multiple VLANs onto one 3-DNS interface.

Note

You should use VLAN tagging only if you are running the 3-DNS in bridge mode.

Interface group VLANs and the default VLAN mapping

By default, the Setup utility configures each interface on the 3-DNS as an untagged member of an interface-group VLAN. The 3-DNS identifies the lowest-numbered interface in that group a member of the VLAN **external,** and makes the remaining interface a member of the VLAN **internal**. In most 3-DNS configurations, you only use one VLAN, **external**. This creates the mapping shown in Figure 5.3.

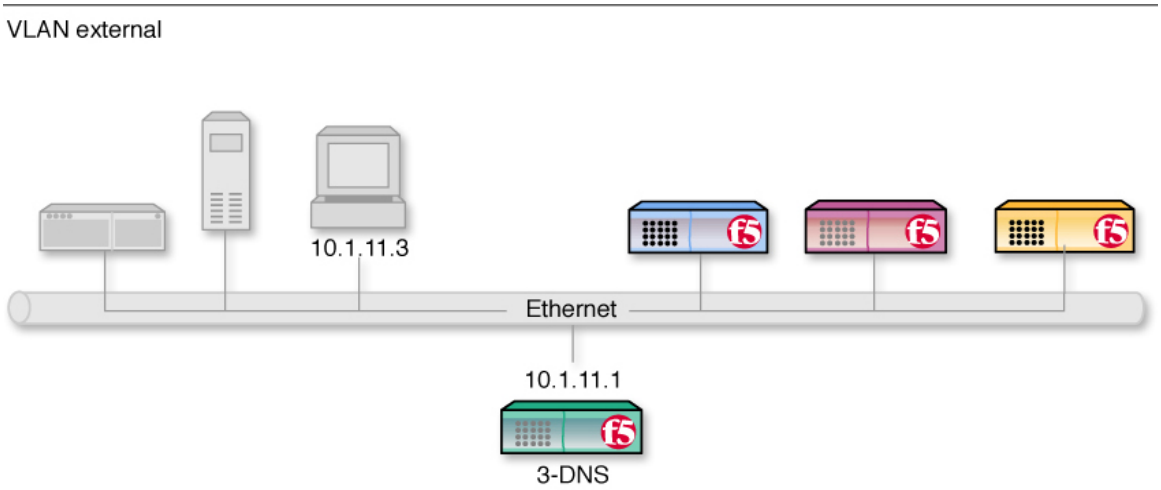

Figure 5.3 *VLAN on a 3-DNS*

VLAN flexibility is such that separate IP networks can belong to a single VLAN, while a single IP network can be split among multiple VLANs. The latter case allows the 3-DNS (when running in bridge mode) to be inserted into an existing LAN without reconfiguring the existing DNS server.

Working with the VLAN commands

You can create, rename, or delete tagged and untagged VLANs using the Configuration utility, or from the command line. Table 5.1 summarizes the VLAN command options.

Option	Description
Default VLAN configuration	The Setup utility provides a default VLAN configuration. On a typical unit with two interfaces, you create an internal and external VLAN.
Create VLAN	Create, rename, or delete a VLAN. Typically, one untagged VLAN is assigned to one interface.
Tag VLANs	You can tag VLANs and associate a single interface to multiple tagged VLANs.
Set VLAN security	You can set port lockdown by VLAN.
Set fail-safe timeouts	You can set a fail-safe timeout on a VLAN. You can use a fail-safe timeout to trigger fail-over in a redundant system.
Self IP addresses	You can set one or more self IP addresses for VLANs.
MAC masquerade	You can use this attribute to set up a media access control (MAC) address that is shared by a redundant system. If you use a redundant system in a network that has secure hubs, or you want to run a redundant system in bridge mode, you should configure the MAC masquerade address.

Table 5.1 *Configuration properties of VLANs*

Creating, renaming, and deleting VLANs

Typically, if you use the default configuration, one VLAN is assigned to each interface in the system. However, if you need to change your network configuration, or if the default VLANs are not adequate for a network configuration, you can create new VLANs, rename existing VLANs, or delete a VLAN.

To create a VLAN using the Configuration utility

1. In the navigation pane, click **Network**.
   The VLANs screen opens.
2. Click the **Add** button to start the Add VLAN wizard.
3. In the Add VLAN screen, type the attributes for the VLAN. For more information about VLANs, click the **Help** button.

To rename or delete a VLAN using the Configuration utility

1. In the navigation pane, click **Network**.
   The VLANs screen opens.
2. In the VLANs screen, use one of the following options:
   - To rename a VLAN, click the VLAN name you want to change. The VLAN properties screen opens. Type the new name in the **VLAN name** box.
   - To delete a VLAN, click the **Delete** button for the VLAN you want to delete.

To create, rename, or delete a VLAN from the command line

To create a VLAN from the command line, use the following syntax:

```
b vlan <vlan name> interfaces add <if name> <if name>
```

For example, if you want to create a VLAN named **my_vlan** that contains the interfaces **1.1** and **1.2**, type the following command:

```
b vlan my_vlan interfaces add 1.1 1.2
```

To rename an existing VLAN, use the following syntax:

```
b vlan <vlan name> rename <new vlan name>
```

For example, if you want to rename the VLAN **my_vlan** to **your_vlan**, type the following command:

```
b vlan my_vlan rename your_vlan
```

To delete a VLAN, use the following syntax:

```
b vlan <vlan name> delete
```

For example, to delete the VLAN named **your_vlan**, type the following command:

```
b vlan your_vlan delete
```

Configuring VLAN groups

A VLAN group is a grouping of two or more VLANs belonging to the same IP network for the purpose of allowing layer 2 packet forwarding, also known as L2 forwarding, between those VLANs.

For a VLAN group to use layer 2 forwarding, you must configure the following 3-DNS features:

- The VLANs between which the packets are to be passed must be on the same IP network.
- The VLANs between which the packets are to be passed must be grouped.
- Layer 2 forwarding must be enabled for the VLAN group.

- A self IP address must be assigned to the VLAN group for routing purposes.

To create a VLAN group from the command line

You can define a VLAN group from the command line using the **vlangroup** command. For example:

```
b vlangroup network11 vlans add internal external
```

To assign the self IP address to the VLAN group, use the following syntax:

```
b self <ip address> vlan <vlangroup name>
```

You must enable layer 2 forwarding for the VLAN group using the **vlan proxy_forward** attribute. This attribute is enabled by default when the VLAN group is enabled. To verify that proxy forwarding is enabled, type the following command:

```
b vlans show
```

Check the output of the VLAN group for **proxy_forward enable**.

Configuring tagged VLANs

A tagged VLAN has a tag number associated with it. Any 3-DNS interface that is explicitly added to the tagged VLAN can send traffic tagged with that number, and can accept traffic that is similarly tagged (meaning the traffic originated from another member interface). Although you add the interface to the VLAN, in practice we usually use tagging to associate multiple VLANs with a single interface.

You can create VLANs with or without specified tags. If you do not specify a tag, 3-DNS automatically assigns one to the VLAN. Therefore, a VLAN always has a tag; whether it functions as a tagged VLAN depends on whether it actually has tagged members.

Tagging a VLAN

You can create tagged VLANs, tag existing VLANs, and add multiple tagged VLANs to a single interface. There are three steps to creating multiple tagged VLANs on one interface.

- Create the VLANs for which you want to tag the interface.
- Mark the interface as tagged.
- Add the tagged VLANs to the tagged interface.

To create a tagged VLAN using the Configuration utility

1. In the navigation pane, click **Network**.
   The VLAN screen opens.
2. Click the **Add** button.
   The Add VLAN screen opens.

3. On the Add VLAN screen, enter the VLAN name and specify the tagged interfaces by selecting them from the **Resources** list and clicking **tagged >>**.
4. Configure the other VLAN options as needed, and click the **Done** button. (It is not necessary to fill in a VLAN tag number. This is done automatically.)

To tag an existing VLAN using the Configuration utility

1. In the navigation pane, click **Network**.
   The VLAN screen opens.
2. Click the VLAN name in the list.
   The properties screen for that VLAN opens.
3. On the screen, specify the tagged interfaces by selecting them from the **Resources** list and clicking **tagged >>**. (It is not necessary to fill in a VLAN tag number. This is done automatically.)

To create a tagged VLAN from the command line

You create a new tagged VLAN using the **bigpipe vlan tag** command, specifying a tag number. For example:

```
b vlan my_vlan tag 1209
```

A tagged VLAN is mapped to an interface or interfaces (or an untagged VLAN is tagged and mapped an interface or interfaces) using the **tagged** flag. For example:

```
b vlan external interfaces add tagged 4.1 5.1 5.2
```

The effect of the command is to place a tag on interfaces **4.1**.and **5.1,** which in turn makes **external** a tagged VLAN. (However, it remains an untagged VLAN for interfaces which are part of it but not tagged.)

An interface can have more than one tag, for example, it can be a member of more than one tagged VLAN:

```
b vlan external interfaces add tagged 4.1
b vlan internal interfaces add tagged 4.1
```

Setting up security for VLANs

You can lock down a VLAN to prevent direct connection to the 3-DNS through that VLAN. This lockdown can be overridden for specific services by enabling the corresponding global variable for that service. For example:

```
b global open_ssh_port enable
```

To enable or disable port lockdown using the Configuration utility

1. In the navigation pane, click **Network**.
   The VLAN screen opens.
2. Click the VLAN name in the list.
   The properties screen for that VLAN opens.
3. To enable port lockdown, check the **Port Lockdown** box.
   To disable port lockdown, clear the **Port Lockdown** check box.

To enable or disable port lockdown from the command line

To enable port lockdown, type:

```
b vlan <vlan_name> port_lockdown enable
```

To disable port lockdown, type:

```
b vlan <vlan_name> port_lockdown disable
```

Setting fail-safe timeouts for VLANs

For redundant 3-DNS systems, the machine fails-over when it detects the loss of traffic on a VLAN, and the traffic is not restored during the fail-over timeout period for that VLAN. You can enable a fail-safe mechanism to attempt to generate traffic when half the timeout has elapsed. If the attempt is successful, the fail-over is stopped.

To set the fail-over timeout and arm the fail-safe using the Configuration utility

1. In the navigation pane, click **Network**.
   The VLAN screen opens.
2. Click the VLAN name in the list.
   The properties screen for that VLAN opens.
3. Check the **Arm Failsafe** box, and specify the timeout in seconds in the **Timeout** box.

To set the fail-over timeout and arm the fail-safe from the command line

Using the **vlan** command, you can set the timeout period and also arm or disarm the fail-safe.

To set the timeout, type:

```
b vlan <vlan_name> timeout <timeout_in_seconds>
```

To arm the fail-safe, type:

```
b vlan <vlan_name> failsafe arm
```

To disarm the fail-safe, type:

```
b vlan <vlan_name> failsafe disarm
```

Setting the MAC masquerade address

You can share the media access control (MAC) masquerade address between 3-DNS units in a redundant system. This has the following advantages:

- Increased reliability and failover speed
- Inter-operability with switches that are slow to respond to network changes
- Inter-operability with switches that are configured to ignore network changes

The MAC address for a VLAN is the MAC address of the first interface to be mapped to the VLAN, typically 1.1 for **external** and 1.2 for **internal**. You can view the interfaces mapped to a VLAN using the following command:

```
b vlan show
```

You can view the MAC addresses for the interfaces on the 3-DNS using the following command:

```
b interface show verbose
```

Use the following syntax to set the MAC masquerade address that will be shared by both 3-DNS units in the redundant system.

```
b vlan <vlan_name> mac_masq <MAC_addr>
```

WARNING

*You must specify a default route before using the **mac_masq** command. You specify the default route in the **/etc/hosts** and **/etc/netstart** files.*

Find the MAC address on both the active and standby units, and choose one that is similar but unique. A safe technique for choosing the shared MAC address follows.

Suppose you want to set up **mac_masq** on the external interfaces. Using the **b interface show** command on the active and standby units, you note that their MAC addresses are:

```
Active: 1.1 = 0:0:0:ac:4c:a2
Standby: 1.1 = 0:0:0:ad:4d:f3
```

In order to avoid packet collisions, you now must choose a unique MAC address as the MAC masquerade address. The safest way to do this is to select one of the addresses and logically **OR** the first byte with **0x40**. This makes the MAC address a locally administered MAC address.

In this example, either **40:0:0:ac:4c:a2** or **40:0:0:ad:4d:f3** would be a suitable shared MAC address to use on both 3-DNS units in the redundant system. The shared MAC address is used only when the 3-DNS is in active mode. When the unit is in standby mode, the original MAC address of the network card is used.

If you do not configure **mac_masq**, on startup, or when transitioning from standby mode to active mode, the 3-DNS sends gratuitous ARP requests to notify the default router and other systems on the local Ethernet segment that its MAC address has changed. See RFC 826 for more details on ARP.

Note

*The MAC masquerade information is stored in the **bigip_base.conf** file.*

6

Essential Configuration Tasks

- Reviewing the configuration tasks
- 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 Setup utility, you set up the network and load balancing aspects of the 3-DNS. The 3-DNS has three essential configuration tasks that all users must complete, regardless of the chosen load balancing solution.

The 3-DNS 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 3-DNS and other servers
  - 3-DNS synchronization (if you have more than one 3-DNS 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

Setting up a basic configuration

Each 3-DNS in the network setup must have information regarding which data center houses specific servers, and with which other 3-DNS systems 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, 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 systems, BIG-IP systems, EDGE-FX Caches, and hosts) that reside at that location.

  A data center can contain any type of server. For example, in Figure 6.1 on page 6-3, the Tokyo data center contains a 3-DNS and a host, while the New York and Los Angeles data centers contain 3-DNS systems and BIG-IP systems.

  For information about configuring data centers, see *Setting up a data center*, on page 6-2.

- **Servers**
  The data center servers that you define in the network setup include 3-DNS systems, BIG-IP systems, GLOBAL-SITE systems, EDGE-FX Caches, and host machines. You define the 3-DNS systems that manage load balancing to the BIG-IP systems, 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 6-5.

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

  For information about configuring sync groups, see *Working with sync groups*, on page 6-19.

- **Wide IPs**
  After you define virtual servers for your BIG-IP systems, 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 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 8, *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 6-22.

Setting up a data center

The first step in configuring your 3-DNS network is to create data centers. A ***data center*** defines the group of 3-DNS, BIG-IP, GLOBAL-SITE, EDGE-FX Cache, and host systems that reside in a single physical location. Figure 6.1 on page 6-3 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 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 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 configuration.

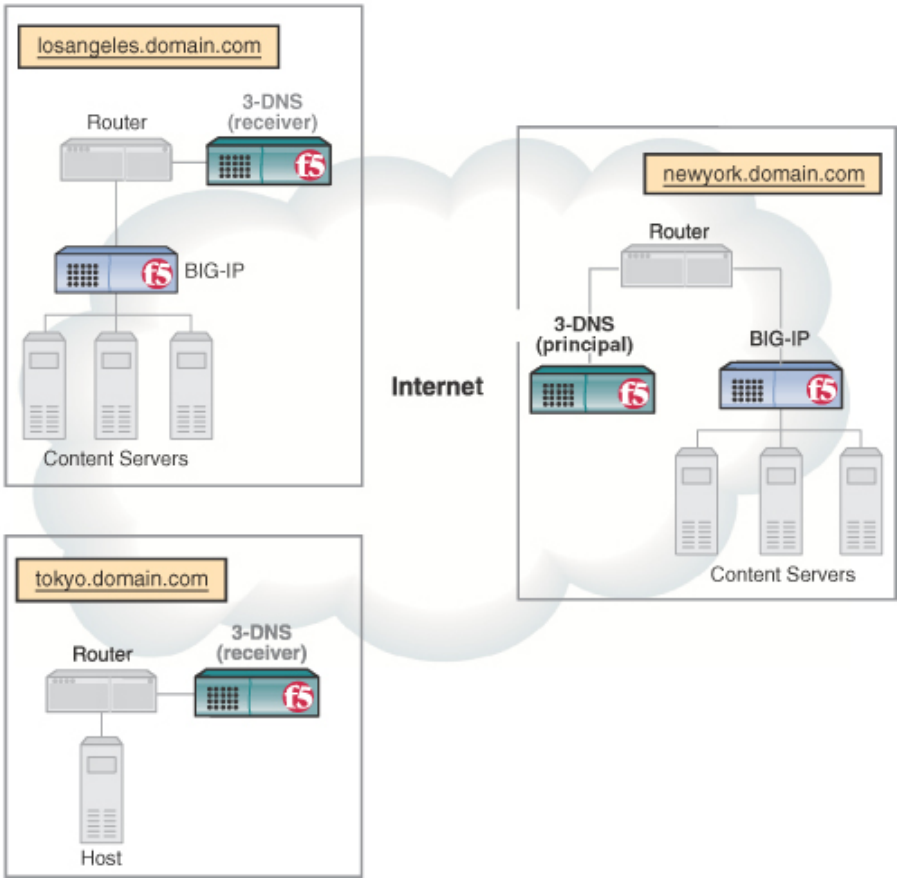

Figure 6.1 *Example data center setup*

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 6.2.
5. Type the server type and IP address for each server that is part of the specified data center.

Figure 6.2 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 6.2 *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 6.3 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 6.3 *Sample data center definition*

Setting up servers

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

This section describes how to set up each server type—3-DNS, BIG-IP, EDGE-FX Cache, GLOBAL-SITE, and host—that makes up your network. The setup procedures here assume that the 3-DNS, BIG-IP, EDGE-FX Cache, GLOBAL-SITE, and host systems are up and running, and that they already have virtual servers defined. (Note that 3-DNS and GLOBAL-SITE systems do not manage virtual servers.)

Defining 3-DNS systems in the configuration

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

◆ Note

*Please review Chapter 11, **Adding a 3-DNS to an Existing Network**, if you are configuring more than one 3-DNS in your network.*

To define a 3-DNS using the Configuration utility

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

Repeat this procedure for each 3-DNS you need to add.

To define a 3-DNS 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 6.4 to define a 3-DNS.

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>
    snmp <number>
    hops <number>
    ecv <number>
    } ]
  }
```

Figure 6.4 *Syntax for defining a 3-DNS*

Figure 6.5 shows a sample **server** statement that defines a 3-DNS.

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

Figure 6.5 *Sample 3-DNS definition*

Defining BIG-IP systems

Before you define BIG-IP systems in the configuration, 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
- The IP address of the BIG-IP itself

To define a BIG-IP using the Configuration utility

1. In the navigation pane, expand the **Servers** item, and then click **BIG-IP**.
2. On the toolbar, click **Add BIG-IP** .
   The Add New BIG-IP screen opens.
3. Add the new BIG-IP settings. (For help on defining BIG-IP systems, click **Help** on the toolbar.)
   The BIG-IP 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**.
2. In the table, find the BIG-IP 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.

To define a BIG-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. Use the syntax shown in Figure 6.6 to define a BIG-IP.

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. When you include the **translate** keyword, the iQuery utility includes translated IP

addresses in the packets sent to the specific BIG-IP. For more information on configuring the **big3d** agent and iQuery, see Chapter 4, *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>
      snmp <number>
      hops <number>
      ecv <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 6.6 *Syntax for defining a BIG-IP in the* ***wideip.conf*** *file*

Figure 6.7 shows a sample **server** statement that defines a BIG-IP.

```
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 6.7 *Sample BIG-IP definition*

Defining a BIG-IP with the 3-DNS module in the configuration

In the 3-DNS configuration, you treat the BIG-IP platform and the 3-DNS module as if they were separate devices. You can add the two server types either by using the Configuration utility or by editing the **wideip.conf** file. The following instructions describe how to add a BIG-IP with the 3-DNS module, with the name **combo.domain.net** and the IP address **192.168.100.100**, to the configuration.

Before you define a BIG-IP with the 3-DNS module in the 3-DNS configuration, you should have the following information:

- The name and IP address of the BIG-IP
- The name and IP address of the 3-DNS

To add a BIG-IP with the 3-DNS module using the Configuration utility

1. In the navigation pane, expand the **Servers** item, and then click **BIG-IP**.
   The BIG-IP List screen opens.
2. On the toolbar, click **Add BIG-IP**.
   The Add BIG-IP screen opens.
3. In the **BIG-IP Name** box, type **combo.domain.net**.
4. In the **BIG-IP IP Address** box, type **192.168.100.100**.
5. Add the rest of the settings as needed.

   When you have finished defining the BIG-IP, you can add the 3-DNS module to the configuration.
6. In the navigation pane, expand the **Servers** item, and then click **3-DNS**.
   The 3-DNS List screen opens.
7. On the toolbar, click **Add 3-DNS**.
   The Add 3-DNS screen opens.
8. In the **3-DNS Name** box, type **combo.domain.net**.
9. In the **3-DNS IP Address** box, type **192.168.100.100**.
10. Add the rest of the settings as needed.

Note that both server types use the same name and IP address, as shown in Figure 6.8. If you are configuring a redundant system, you use the shared IP address. For assistance, contact technical support.

To add a BIG-IP with the 3-DNS module from the command line

1. At the command line, type **3dnsmaint**.
   The 3-DNS Maintenance menu opens.
2. Using the arrow keys, choose **Edit 3-DNS Configuration**.
3. Add the server definitions for both the BIG-IP and the 3-DNS to the **wideip.conf** file. Use the syntax in Figure 6.8 as an example.

```
server { // datacenter=DC1, #VS=1
  type bigip
  address 192.168.100.68
  name "birch.win.net"
  limit { /* none */ }
  iquery_protocol udp
  remote {
    secure yes
    user "root"
  }
  factories {
    snmp 1
  }
  prober 127.0.0.1
}

server { // datacenter=DC1, #VS=0
  type 3dns
  address 192.168.100.68
  name "birch.win.net"
  limit { /* none */ }
  iquery_protocol udp
  remote {
    secure yes
    user "root"
  }
  factories {
    snmp 1
  }
}
```

Figure 6.8 *Sample definition of a BIG-IP with the 3-DNS module*

Defining a GLOBAL-SITE in the configuration

The 3-DNS uses the GLOBAL-SITE for path probing and metrics collection only. The GLOBAL-SITE does not manage any virtual servers. Before you define a GLOBAL-SITE in the 3-DNS configuration, you should have the following information:

- The name of the GLOBAL-SITE
- The IP address of the GLOBAL-SITE

To define a GLOBAL-SITE using the Configuration utility

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

To define a GLOBAL-SITE 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 6.9 to define a GLOBAL-SITE.

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

Figure 6.9 *Syntax for defining a GLOBAL-SITE*

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

Figure 6.10 shows a sample **server** statement that defines a GLOBAL-SITE.

```
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 6.10 *Sample GLOBAL-SITE 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 6.11 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>
    snmp <number>  //minimum of 1 to collect metrics
    hops <number>
    ecv <number>
  }]
  vs {
    address <virtual server IP address>
    port <port number> | service <"service name">
  [ depends_on {
      address <IP address>
      address <IP address>
    } ]
  }
}
```

Figure 6.11 *Syntax for defining an EDGE-FX Cache*

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 4, *The big3d Agent,* of the ***3-DNS Reference Guide***.

Figure 6.12 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 6.12 *Sample EDGE-FX Cache server definition*

Defining host servers

A ***host*** is an individual network server or server array controller other than a 3-DNS, BIG-IP, EDGE-FX Cache, or GLOBAL-SITE. 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 6-18.

◆ Note

*To fully configure host probing, you must configure the SNMP agent settings in the host definition as previously described, set up the **big3d** agents to run SNMP factories, and configure the SNMP agents on the hosts themselves. For details, please refer to Chapter 4, **The big3d Agent**, and Chapter 12, **SNMP**, in the **3-DNS Reference Guide**.*

To define a host using the Configuration utility

1. In the navigation pane, expand the **Servers** item, and then click **Host**.

2. On the toolbar, click **Add Host**.
   The Add New Host 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**.
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 6.13 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 | 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 6.13 *Syntax for defining a host*

Figure 6.14 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  dns_rev
   port            53
   snmp {
      agent        ucd
      community    "public"
      version      1
   }
   vs {
      address         192.168.104.50:25
   }
   vs {
      address         192.168.104.50:80
   }
}
```

Figure 6.14 *Sample host 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, BIG-IP, EDGE-FX Cache, or GLOBAL-SITE that runs the **big3d** agent and is in the same data center as the host.

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 uses this performance information for dynamic load balancing modes, such as Packet Rate, Quality of Service, and Kilobytes/Second.

Table 6.1 shows the host SNMP agents supported by the 3-DNS.

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 distributed with Microsoft® Windows NT® Server 4.0.
Win2KServ	This SNMP matrix agent is distributed with Microsoft Windows 2000 Server.
Cisco LDV2	This SNMP agent is distributed with the Cisco® LocalDirector, version 2.X.
Cisco LDV3	This SNMP agent is distributed with the Cisco LocalDirector, version 3.X.
ArrowPoint	This SNMP agent is distributed with the Cisco/ArrowPoint CSS series.
Alteon	This SNMP agent is distributed with the Alteon® WebSystems ACEdirector.
Foundry	This SNMP agent is distributed with the Foundry® ServerIron.
CacheFlow	This SNMP agent is distributed with the CacheFlow® appliances.

Table 6.1 *Supported SNMP agents*

Viewing host performance metrics

The Configuration utility displays the host metrics in the Host Statistics screen. The 3-DNS bases the advanced load balancing decisions on packet rate, kilobytes per second, and current connections metrics, but the Host Statistics 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 4, *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 configuration. First, when you define a 3-DNS or BIG-IP, 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, review Chapter 12, *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 systems that synchronize their configuration settings and metrics data. A sync group contains a principal system and one or more receiver systems. The ***principal*** system is the 3-DNS from which the ***receiver*** systems obtain their metrics and server statistics information. You configure a sync group from the principal 3-DNS. First list the IP address of the principal itself. Then list the receiver 3-DNS systems in the order that they should become principals if previously listed 3-DNS systems fail.

Each 3-DNS in your network must be included in a sync group. There may be cases where you do not want a 3-DNS to share its configuration with other systems. In this case, you can create a separate sync group for each 3-DNS. 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 6.15 *Sample non-syncing* ***sync groups*** *statements*

◆ Note

To implement such a configuration, you must modify each 3-DNS system'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 systems, first select the 3-DNS that you want to be the principal system. Then check the box next to each 3-DNS 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 6.16 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 6.16 *Syntax for setting up a sync group*

Figure 6.17 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 6.17 *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 system's time setting is allowed to be out of sync with another 3-DNS system'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 systems.

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, choose **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 6.18 shows the correct syntax for enabling encryption.

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

Figure 6.18 *Syntax for enabling encryption*

7

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 to distribute requests in an efficient and seamless manner using Topology load balancing. When you use Topology load balancing, the 3-DNS compares the location information derived from the DNS query message to the topology records in the topology statement. The system then distributes the request according to the topology record that best matches the location information.

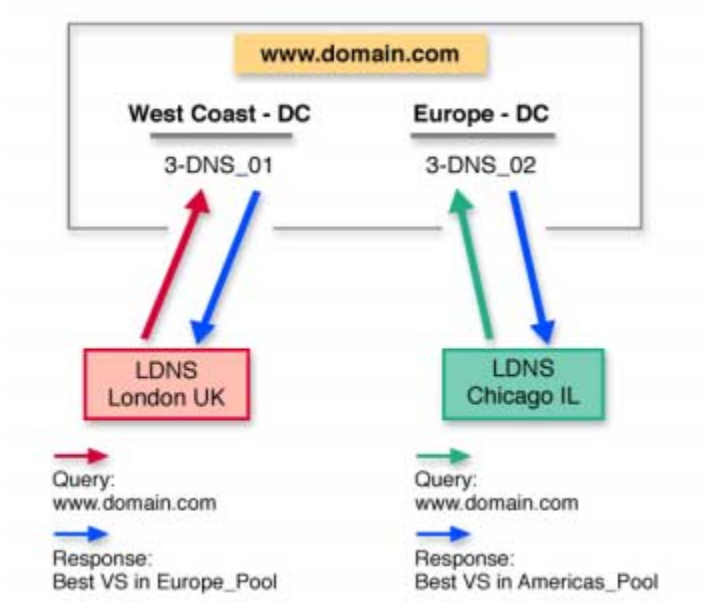

Figure 7.1 *Topology load balancing in a globally-distributed network*

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 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 contains a classifier that maps IP addresses to geographic locations. With this classifier, the 3-DNS resolves DNS requests to the geographically closest LDNS server at either the country or the continent level. The system 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 7.1, 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 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 in each data center.
- You have BIG-IP systems, 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 8, *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 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 7.1, on page 7-1, we have added two data centers labeled ***West Coast - DC*** *and* ***Europe - DC****.*

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

Once you have added all of your data centers to the 3-DNS configuration, you are ready to notify the 3-DNS that you are configuring about the 3-DNS systems in your network, including the 3-DNS you are configuring.

◆ Note

Please note that when you are working with more than one 3-DNS, you create your entire configuration on one system and then add the second system using the ***3dns_add*** *script. The* ***3dns_add*** *script copies the entire configuration from the first (or existing) system onto the second (new) system, and synchronizes all of the settings. For details on configuring additional 3-DNS systems in existing networks, using the* ***3dns_add*** *script, see Chapter* 11, ***Adding a 3-DNS to an Existing Network****.*

To add 3-DNS systems using the Configuration utility

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

Configuration notes

For the globally-distributed network configuration shown in Figure 7.1, on page 7-1, we have a 3-DNS in each data center, ***West Coast - DC*** *and* ***Europe - DC****. The system we are configuring is labeled* ***3-DNS_01****, and is in the* ***West Coast - DC*** *data center. The additional system is in the* ***Europe - DC*** *data center, and is labeled* ***3-DNS_02****.*

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

Now you are ready to let the 3-DNS know about any BIG-IP systems, or other servers, that you have in your network. Remember that the 3-DNS load balances requests to the virtual servers managed by the BIG-IP systems, EDGE-FX Caches, or host servers in your network. In this example

configuration, we set up BIG-IP systems. For information on adding EDGE-FX Caches or host servers to your network, please refer to *Setting up servers*, on page 6-5.

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

To add BIG-IP systems using the Configuration utility

1. In the navigation pane, expand the **Servers** item, then click **BIG-IP**. The BIG-IP List screen opens.
2. Click **Add BIG-IP** on the toolbar.
   The Add New BIG-IP screen opens.
3. Add the BIG-IP 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 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, 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, you can repeat the previous steps to add all of the additional BIG-IP systems to the 3-DNS 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 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 to load balance DNS requests, and click **Finish**.
   The 3-DNS 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 procedure 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 7.1, on page 7-1, we have set up one wide IP, labeled **www.domain.com**, and we added two pools to the wide IP, **americas_pool** and **europe_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 topology records before the 3-DNS 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 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 uses the topology records, and how to configure topology in the **wideip.conf** file, please review Chapter 13, *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 7.1, on page 7-1, we added topology records, as shown in Figure 7.2:

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

***Figure 7.2** 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 can detect when a managed server or virtual server is low on system resources, and can 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 systems

1. In the navigation pane, expand the **Servers** item and click **BIG-IP**.
2. In the Limits Settings column of the BIG-IP 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. 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 12, *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 9, *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.)

8

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 in a CDN

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

- **CDN switching**
  CDN switching is the functionality of the 3-DNS that allows a user to delegate global traffic to a third-party network. The two features of the 3-DNS that make CDN switching possible are:
  - **Geographic redirection**
    The 3-DNS 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 3-DNS delegates DNS queries either to a data center, by responding with **A** records, or to a CDN provider, by responding with a **CNAME** record.
  - **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 **CNAME** on the 3-DNS so that the 3-DNS redirects requests to a CDN provider's name servers rather than to a grouping of virtual servers. For a list of our partner CDN providers, click **CDN Providers** on the 3-DNS home screen.
- **Resource monitoring, limits, and thresholds**
  The 3-DNS 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. In the example, the content provider for **www.download.domain.com** has two data centers, one in San Jose, California (see Figure 8.1), and one in Washington, DC (see

Figure 8.2 on page 8-3). The 3-DNS systems (in the two data centers) use the Topology load balancing mode to direct the DNS queries to the geographically closest virtual servers.

In Figure 8.1, 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 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).

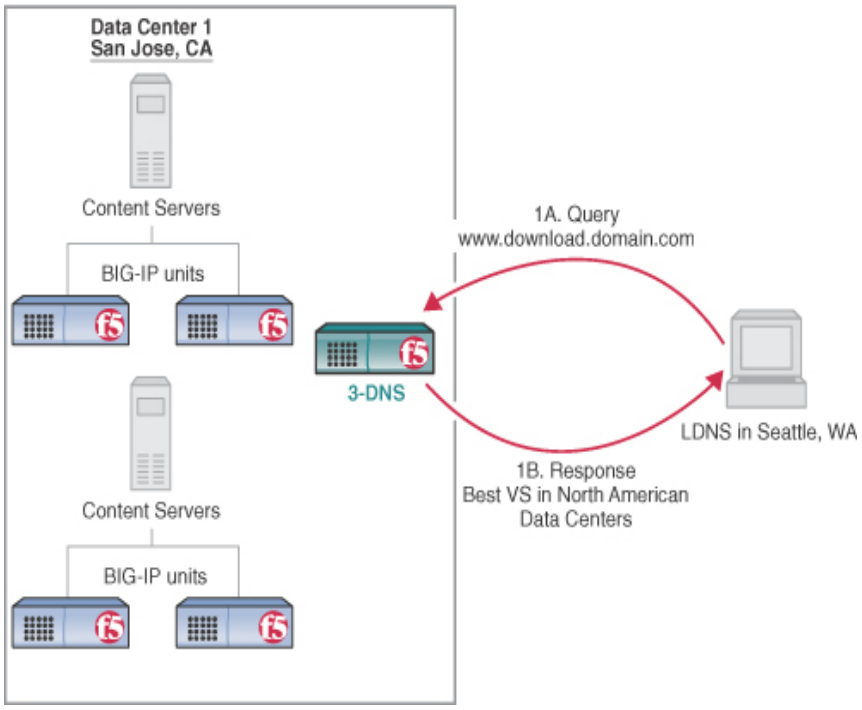

Figure 8.1 *DNS query resolution based on Topology load balancing mode*

In Figure 8.2, 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 in the content provider's North American data center responds to the London LDNS with delegation information (a **CNAME** record) 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**).

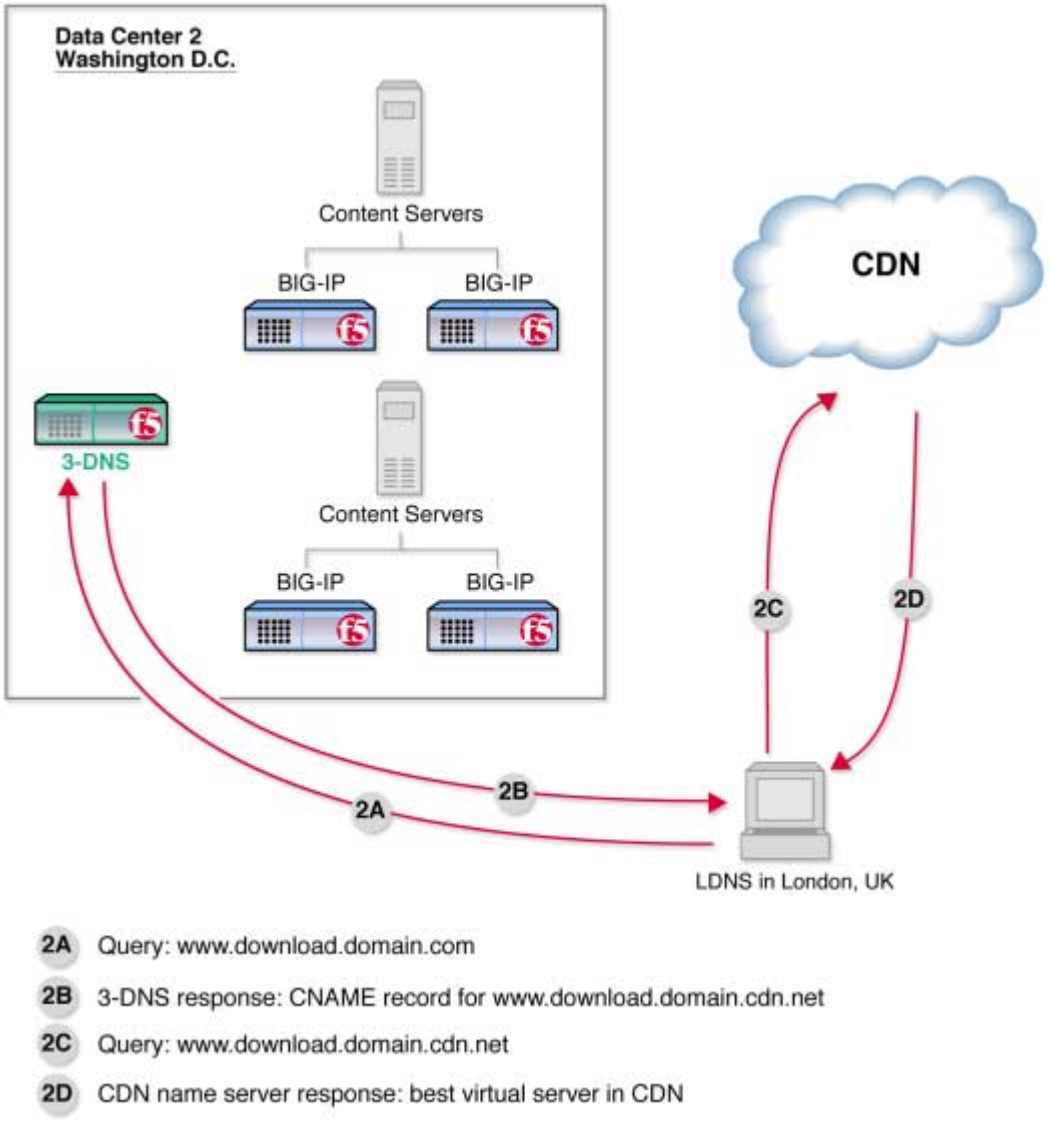

Figure 8.2 *DNS query resolution to content delivery network provider*

Deciding to use a CDN provider

The 3-DNS 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 at **news.domain.cdn.net**, while they serve their stock quotes content with **quote.domain.com** from their corporate data center.
- The CDN provider sets its billing rates based on megabits 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 8-1. The tasks are as follows:

- Adding data centers
- Adding 3-DNS systems
- Adding load balancing 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.

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 systems

Once you have added all of your data centers to the 3-DNS configuration, you are ready to advise the 3-DNS you are configuring about other 3-DNS systems in your network.

To add 3-DNS systems using the Configuration utility

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

Configuration note

*Please note that when you are working with more than one 3-DNS, you create your entire configuration on one system and then add the second system using the **3dns_add** script. The **3dns_add** script copies the entire configuration from the first system onto the second system, and synchronizes all of the settings. For details on configuring additional 3-DNS systems in existing networks, using the **3dns_add** script, see Chapter 11, **Adding a 3-DNS to an Existing Network**.*

Adding load balancing servers

Now you are ready to let the 3-DNS know about any BIG-IP systems, 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 load balance your origin site content. For specific information on configuring any of these server types, please review *Setting up servers*, on page 6-5.

Adding wide IPs and pools

Once you have added all the physical elements to the 3-DNS 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 8.1 and 8.2.

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 to load balance DNS requests, and click **Finish**.
   The 3-DNS 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 **Dynamic Delegation, Type** list, select **CNAME**.
   d) In the **Dynamic Delegation, Canonical Name** box, type the canonical name that you want the 3-DNS to deliver in the **CNAME** record when it redirects traffic to the CDN provider. For our example, the canonical name is **www.download.domain.cdn.net**. Note that the canonical name for the CDN pool type automatically becomes an alias for the wide IP.
5. Click **Next**.
   The Wide IP List screen opens.

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 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, see Chapter 13, **Topology**, in the **3-DNS Reference Guide**. For information on setting up globally-distributed network with Topology load balancing, see Chapter 7, **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 can successfully load balance DNS queries based on the location information derived from the DNS query message. For our example, using the topology statement you just created, the 3-DNS would direct queries for **www.download.domain.com** that originated in North America to the **origin** pool for resolution. Requests that did not originate in North America would be directed to the CDN provider using the **cdn_ pool**.

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 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 8, *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.
- **ECV monitor**
  With an extended content verification (ECV) monitor, you can verify that a specific file is available on the content servers for a wide IP. For more information on ECV monitors, refer to the ***3-DNS Reference Guide***, Chapter 6, *Extended Content Verification (ECV)*.

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 in the ***3-DNS Reference Guide***.

9

Working with Quality of Service

- Overview of Quality of Service
- Understanding QOS coefficients
- Customizing the QOS equation
- Using the Dynamic Ratio option

Overview of Quality of Service

The Quality of Service mode is a dynamic load balancing 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 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 Quality of Service, 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 9.1 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	Default value	Example upper limit	Higher or lower?
Packet rate	Packets per second	1	700	Lower
Round trip time	Microseconds	50	2,000,000	Lower
Completion rate	Percentage of successfully transferred packets (0-100%)	5	100%	Higher
Topology	Score that defines network proximity by comparing server and LDNS IP addresses (0-2^{32})	0	100	Higher
Hops	Number of intermediate systems transitions (hops)	0	64	Lower
VS capacity	Number of nodes ***up***	0	20	Higher
Kilobytes/second	Kilobytes per second throughput	3	15000	Lower

Table 9.1 *QOS coefficients: Default values, 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 normalizes the raw metrics to values in the range of 0 to10. 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 9.1, you are putting the most emphasis on completion rate.

```
globals {
         qos_coeff_rtt 50
         qos_coeff_completion_rate 100
         qos_coeff_packet_rate 1
         qos_coeff_topology 0
         qos_coeff_hops 0
         qos_coeff_vs_capacity 0
         qos_coeff_kbps 0
}
```

Figure 9.1 *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, choose **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 9.2 to define a global QOS equation.

```
globals {
         qos_coeff_rtt 50
         qos_coeff_completion_rate 5
         qos_coeff_packet_rate 1
         qos_coeff_topology 0
         qos_coeff_hops 0
         qos_coeff_vs_capacity 0
         qos_coeff_kbps 0
}
```

Figure 9.2 *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, choose **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 9.3 to define a wide IP's QOS equation.

Figure 9.3 displays a wide IP definition that overrides the global QOS equation settings shown in Figure 9.2.

```
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 9.3 *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 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 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 9.4) 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 9.4 *Enabling dynamic ratio in a pool configuration*

10

Working with Global Availability Load Balancing

- Overview of the Global Availability load balancing mode
- Configuring the Global Availability mode

Overview of the Global Availability load balancing mode

You can use the Global Availability mode in one of two ways: either to load balance among wide IP pools, or to load balance within a wide IP pool. When you use the Global Availability mode to load balance among pools, the 3-DNS continually sends requests to the first pool in the wide IP. When all the virtual servers in the pool become unavailable, the pool is marked unavailable and the 3-DNS starts sending requests to the next pool listed in the wide IP. When the first pool is available again, the 3-DNS stops sending requests to the second pool, and starts sending them to the first pool again. If you have an origin site and an overflow network, such as a CDN, you can use Global Availability to load balance between the two networks.

When you use the Global Availability mode to load balance virtual servers within a pool, the load balancing works in much the same way. The 3-DNS repeatedly selects the first available virtual server in the wide IP pool to respond to requests. If that virtual server becomes unavailable, subsequent connections go to the next available virtual server listed in the pool. When the first listed virtual server becomes available again, the 3-DNS distributes requests to it again.

Figure 10.1 shows the 3-DNS using the Global Availability load balancing mode.

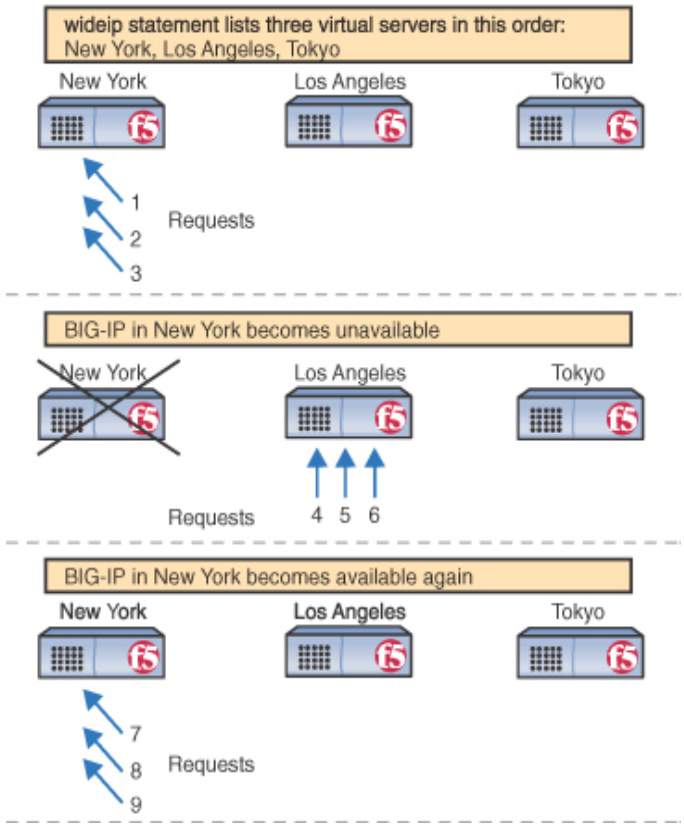

Figure 10.1 *Global Availability mode*

Configuring the Global Availability mode

The following sections describe how to configure the Global Availability load balancing mode to load balance among pools and to load balance within a pool.

To configure the Global Availability load balancing mode among pools 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. In the **Pool LB Mode** box, select **Global Availability**.
4. Click **Update**.
5. A popup screen appears, indicating that with the Global Availability load balancing mode you must order the pools. Click **OK**.
   The Modify Virtual Servers screen opens.
6. In the Order column, specify the order in which you want to list the pools for Global Availability.
7. Click **Update**.

To configure the Global Availability load balancing mode among pools 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 **pool_lbmode**.
5. List the pools in the wide IP in descending order of preference.

To configure the Global Availability load balancing mode within a pool 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 within a pool 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 within the pool that you want to modify.
5. List the virtual servers in the wide IP in descending order of preference. See Figure 10.2 on page 10-4 for an example of the syntax.

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 10.2 shows a sample **wideip** definition, in the **wideip.conf** file, where Global Availability is the preferred load balancing mode.

```
// Global availability
wideip {
   address           192.168.101.50
   port              80 // http
   name              "cgi.wip.domain.com"
   pool {
      name           "mypool"
      preferred      ga
      address       192.168.101.60 //New York data center
      address       192.168.102.60 //Los Angeles data center
      address       192.168.103.60 //Tokyo data center
   }
}
```

Figure 10.2 *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 sends resolution requests to the second listed virtual server until the first listed virtual server becomes available again.

11

Adding a 3-DNS to an Existing Network

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

Working with more than one 3-DNS in the network

When you are working with more than one 3-DNS in your network, and you want the systems to load balance to the same virtual servers, you can create your entire configuration on one system and then add the second system using the **3dns_add** script. The **3dns_add** script copies the entire configuration from the first system onto the second system, and synchronizes all of the settings between the systems. When you are finished, the first system acts as the principal system in the sync group, and the second system becomes a receiver system. (For more information about sync groups, see *Working with sync groups*, on page 6-19.)

The following sections of this chapter describe the procedures you follow to add a 3-DNS into a network that already has at least one 3-DNS configured and working properly. If you are adding the first 3-DNS to your network, refer to Chapter 6, *Essential Configuration Tasks*.

Note

*If you are adding a second 3-DNS to your network but do not want it to be in the same sync group as your first system, or you want the second 3-DNS 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 to your network

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

- Physically install the second 3-DNS in its data center. (For more information on hardware installation, see Chapter 3, *Setting Up the Hardware*)
- Run the Setup utility on the second system. (For more information on the Setup utility, see Chapter 4, *Working with the Setup Utility*, or if you are running the 3-DNS module on the BIG-IP, refer to the ***BIG-IP Reference Guide***.)
- Make the existing 3-DNS aware of the IP address, fully-qualified domain name, and data center location of the second 3-DNS. (See *Making the existing 3-DNS aware of the additional system*, on page 11-2.)
- Add the new 3-DNS to the sync group of the existing 3-DNS.

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

WARNING

*We strongly recommend that you run the **3dns_add** script to add additional 3-DNS systems to your network if you are using a sync group. If you do not use the script, you risk overwriting your current configuration.*

Installing the hardware and running the Setup utility

You can find detailed instructions on installing the 3-DNS hardware in Chapter 3, *Setting Up the Hardware*. Chapter 4, *Working with the Setup Utility*, includes detailed instructions on running the Setup utility. When you have finished this part of the setup for the second system, do not make any other changes to the configuration.

Note

If you are working with the 3-DNS module on the BIG-IP, please refer to the BIG-IP Administrator Kit for information on installing the hardware and running the Setup utility.

Making the existing 3-DNS aware of the additional system

Once you have installed the hardware and run the Setup utility on the new system, you add its configuration information to the existing 3-DNS (the 3-DNS that is already installed in your network). The existing system becomes the principal system in the sync group once you run the **3dns_add** script on the new system.

To add the new system to the existing system'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 system, and click **Update**.
2. Add the second 3-DNS to the configuration.
   a) In the navigation pane, expand the **Servers** item, and click **3-DNS**.
   The 3-DNS List screen opens.
   b) Click **Add 3-DNS** on the toolbar.
   The Add New 3-DNS screen opens.
   c) Add the information for the new system and click **Update**.
3. Add the new system to the existing system'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 3-DNS you just defined and click **Add**.
The new system becomes a receiver in the sync group of the existing system.

You have now successfully added the new 3-DNS to the existing system's configuration and sync group. 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 either by using a remote secure shell session, or by using a monitor and keyboard connected directly to the 3-DNS.

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 Setup utility.
3. To run the script, type **3dns_add** at the command line.
The script copies the entire configuration of the existing 3-DNS to the new system.

Verifying the configuration

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

- Verify that each 3-DNS 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 systems 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 systems have time to synchronize with each other.

To verify that each 3-DNS 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. In the Server and Big3d columns, make sure the status is **up**, which is indicated by a small green ball.
3. In the E/D column, make sure the systems are enabled.
4. If the status of any of your systems is **down**, **unknown**, or **unavailable**, wait a few minutes and click **Refresh**. If status of the systems 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. In the Server column, make sure that the status of each server is **up**, which is indicated by a small green ball.
3. If the status of any of your servers is **down**, **unknown**, or **unavailable**, wait a few minutes and click **Refresh**. 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. 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.
3. If the status of any of your virtual servers is **down**, **unknown**, or **unavailable**, wait a few minutes and click **Refresh**. 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 systems, 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 systems. 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.*

12

Administration and Monitoring

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

Monitoring and administration utilities provided on the 3-DNS

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

The 3-DNS 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. The Configuration utility supports Netscape Navigator, version 4.5 or later, and Internet Explorer, version 4.02 or later.
- **Setup utility**
  The Setup utility is a menu-driven command line utility that you can use to configure many of the platform settings for the 3-DNS. You can also use the browser-based version of the Setup utility for the initial configuration of the 3-DNS. If you are using the Setup utility to make changes to your existing configuration, we recommend that you use the command line version of the utility. To access the Setup utility from the command line, type **config**.
- **3-DNS Maintenance menu**
  The 3-DNS Maintenance menu is a command line utility you can use to configure the 3-DNS. Use the 3-DNS Maintenance menu to simplify certain tasks such as updating the **big3d** agent and editing the **wideip.conf** file. To access the 3-DNS Maintenance menu from the command line, type **3dnsmaint**.
- **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, the servers and the virtual servers it manages, and the load balancing it performs.
- **3dpipe utility**
  Using the **3dpipe** utility, you can perform the following tasks, at the command line:
  - View lists of configured data centers, servers, virtual servers, wide IPs, and pools
  - View the status (enabled or disabled) of configured data centers, servers, virtual servers, wide IPs, and pools

- Enable configured data centers, server types, virtual servers, wide IPs, and pools
- Disable, for a specific time period, configured data centers, servers, virtual servers, wide IPs, and pools
- View summary statistics for the 3-DNS itself

Managing users on the 3-DNS

The Setup utility prompts you to define a password that allows remote access to the 3-DNS, 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 itself, at the command line.

To change the root password for command line access

1. At the 3-DNS 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 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 from the Configuration utility. The crypto 3-DNS 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 3-DNS as you normally would.

Note

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

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 itself.
Globals	This statistics screen provides information on the global settings for the 3-DNS.
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 systems that are in the same sync group as the 3-DNS 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	This statistics screen provides information on the 3-DNS systems you have configured.
BIG-IP	This statistics screen provides information on the BIG-IP systems you have configured.
EDGE-FX Caches	This statistics screen provides information on the EDGE-FX Caches you have configured.

Table 12.1 *Configuration utility Statistics screens*

Statistics Item	Description
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.
Internet Weather Map	This statistics screen provides information on the average round trip times, average completion rates, and average router hops between the data centers you have configured and local DNS servers.
Paths	This statistics screen provides information on the paths created by the 3-DNS 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 database.

Table 12.1 *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.

Working with command line utilities

The 3-DNS includes several command line utilities. These utilities allow you to configure various features of the 3-DNS from the command line. For additional 3-DNS configuration options, you may also want to review the following chapters in the ***3-DNS Reference Guide***: Chapter 2, *3-DNS Maintenance Menu*, and Chapter 11, *Scripts*. For information on working with the Setup utility, see Chapter 4, *Working with the Setup Utility*, in this guide.

Viewing command line utilities documentation

You can access the most current documentation on 3-DNS utilities by using the Configuration utility or by using the command line. You can view all the documentation for the 3-DNS from the main screen of the Configuration utility, including the man pages for the utilities that are shipped with the system.

To view 3-DNS man pages using the Configuration utility

1. Log on to the Configuration utility.
2. From the Online Documentation section of the 3-DNS home screen, click **3-DNS Man Pages**.
   A screen containing an index of 3-DNS man pages opens.

To display a list of utilities that fall into a particular category

To display a list of utilities that fall into a particular category, type the following command:

```
man -k <category>
```

For example, to get a list of utilities that pertain to DNS, type the following command, and a list of utilities that pertain to DNS appears.

```
man -k dns
```

To display documentation for a specific 3-DNS utility

To display the man page for a specific utility, type the following command:

```
man <utility>
```

For example, if you type the following command, the **3dparse** man page appears:

```
man 3dparse
```

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 most often referred to as the 3-DNS.

3-DNS Maintenance menu

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

3-DNS web server

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

A record

The **A** record is the ADDRESS resource record that a 3-DNS 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 or hops queries.

active unit

In a redundant system, an active unit is a 3-DNS 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 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 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**.

CDN switching

CDN switching is the functionality of the 3-DNS 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 that make CDN switching possible are geographic redirection and the pool type CDN.

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.

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.

data center

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

data center server

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

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, 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 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 uses to load balance a resolution request. The 3-DNS 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.

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 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 3-DNS systems and BIG-IP systems.

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 systems, BIG-IP systems, EDGE-FX Caches, and GLOBAL-SITE systems. 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 uses three load balancing modes. The preferred method specifies the first load balancing mode that the 3-DNS 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 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, 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 systems, EDGE-FX Caches or GLOBAL-SITE systems, 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 systems 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 systems that automatically manages DNS zone files, synchronizing them with the configuration on the 3-DNS. 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, 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 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, an EDGE-FX Cache, or a host. The 3-DNS 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 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 uses to load balance a resolution request. See also *alternate method, fallback method*.

principal 3-DNS

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

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 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. Prober factories can run on BIG-IP systems, EDGE-FX Caches, and GLOBAL-SITE systems.

production rule

A production rule, on the 3-DNS, 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.

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.

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.

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

A receiver 3-DNS is a system, 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*.

redundant system

A redundant system is a pair of systems that are configured for fail-over. In a redundant system, one system runs as the active unit and the other system 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 system 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 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.

Setup utility

The Setup utility is a utility that takes you through the initial system configuration process. The Setup utility runs automatically when you turn on a 3-DNS for the first time.

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 system 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 systems that share system configurations and path metrics for data center servers and virtual servers. Sync groups have one principal 3-DNS, and may contain one or more receiver systems. The receiver systems obtain their configuration information from the principal system. See also *principal 3-DNS, receiver 3-DNS*.

time tolerance value

The time tolerance value is the number of seconds that one 3-DNS system's clock is allowed to differ in comparison to another 3-DNS system'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 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 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 and does not yet have metrics information, the 3-DNS marks its status as **unknown**. The 3-DNS can use unknown servers for load balancing, but if the load balancing mode is dynamic, the 3-DNS 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, EDGE-FX Cache, or host server.

watchdog timer card

The watchdog timer card is a hardware device that monitors the 3-DNS 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 systems, EDGE-FX Caches, or by host servers. The 3-DNS 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

A

B

C

D

E

F

G

H

Q

R

S